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, VA 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.
17/952,176	27-JUN-23	11687741

Rimon Law, P.C. - SMC Steven Colby
423 Washington Street, Suite 600
San Francisco, CA 94111

EGRANT NOTIFICATION

Your electronic patent grant (eGrant) is now available, which can be accessed via Patent Center at https://patentcenter.uspto.gov

The electronic patent grant is the official patent grant under 35 U.S.C. 153. For more information, please visit https://www.uspto.gov/electronicgrants

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/952,176	06/27/2023	11687741	SMC-83-C12C3	8353

43198 7590 06/07/2023

Rimon Law, P.C. - SMC
Steven Colby
423 Washington Street, Suite 600
San Francisco, CA 94111

ISSUE NOTIFICATION

The projected patent number and issue date are specified above. The patent will issue electronically. The electronically issued patent is the official patent grant pursuant to 35 U.S.C. § 153. The patent may be accessed on or after the issue date through Patent Center at https://patentcenter.uspto.gov/. The patent will be available in both the public and the private sides of Patent Center. Further assistance in electronically accessing the patent, or about Patent Center, is available by calling the Patent Electronic Business Center at 1-888-217-9197.

The USPTO is implementing electronic patent issuance with a transition period, during which period the USPTO will mail a ceremonial paper copy of the electronic patent grant to the correspondence address of record. Additional copies of the patent (i.e., certified and presentation copies) may be ordered for a fee from the USPTO's Certified Copy Center at https://certifiedcopycenter.uspto.gov/index.html. The Certified Copy Center may be reached at (800)972-6382.

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

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

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

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

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Patents Stakeholder Experience (OPSE), Stakeholder Support Division (SSD) at (571)-272-4200.

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

Steven Michael Colby, Verdi, NV;

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

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

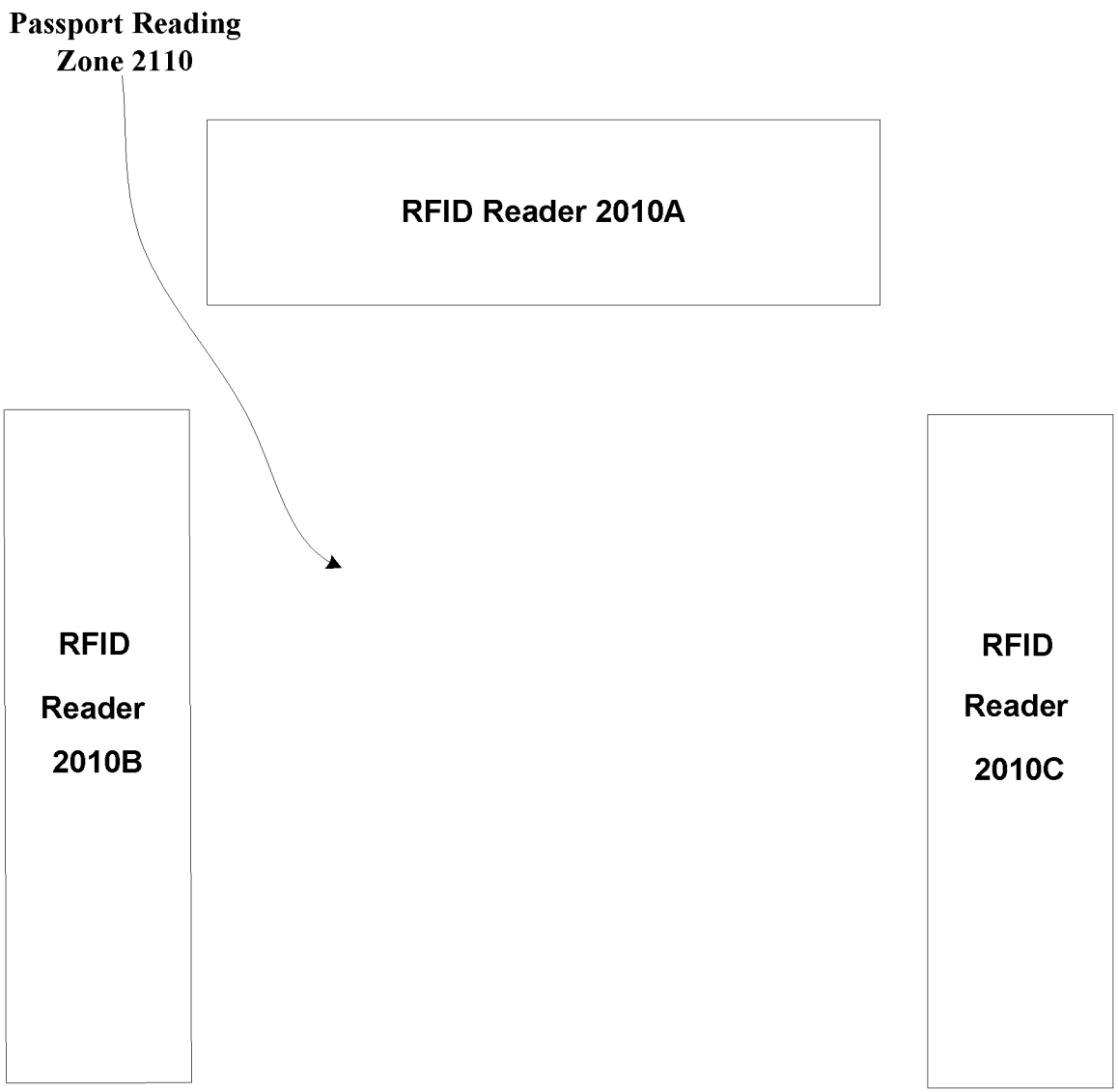

Passport Reading
Zone 2110
RFID Reader 2010A
RFID
Reader
2010B
RFID
Reader
2010C

FIG. 21

IN THE UNITED STATES

PATENT AND TRADEMARK OFFICE

APPLICANT:	Mynette Technologies, Inc.
APPLICATION NO.:	17/952,176
CONFIRMATION NO.:	8353
FILING DATE:	23-SEP-2022
TITLE:	Methods of Using a Cellular Telephone
EXAMINER:	Jamara Franklin
ART UNIT:	2876
ATTY. DKT. NO.:	SMC-83-C12C3

Response to Notice to File Corrected Application Papers

In response to the notice mailed May 26, 2023, please find submitted wherewith a corrected drawing sheet 15/39 including FIG. 21 having text in compliance with 37 CFR 1.84 (p)(1).

No new matter is introduced with this submission.

Respectfully submitted,

Date: ___May 26, 2023__ ___/Steven M. Colby 50,250/____

Dr. Steven M. Colby, JD, Ph.D.
(Reg. No. 50,250)
Partner, Rimon PC
CEO, Mynette Technologies, Inc.

Electronic Acknowledgement Receipt

EFS ID:	48065753
Application Number:	17952176
International Application Number:	
Confirmation Number:	8353
Title of Invention:	Methods of Using a Cellular Telephone
First Named Inventor/Applicant Name:	Steven Michael Colby
Customer Number:	43198
Filer:	Steven M. Colby
Filer Authorized By:	
Attorney Docket Number:	SMC-83-C12C3
Receipt Date:	26-MAY-2023
Filing Date:	23-SEP-2022
Time Stamp:	16:06:46
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Drawings-only black and white line drawings	CorrectedFIG-21.pdf	91933 969bf19d84337330ebaaed356facb8dc385f06a6	no	1

Warnings:

Information:					
2	Post Allowance Communication - Incoming	SMC-83-C12C3-NoticeResponse-filing.pdf	74068 e9b9c77a45b3dd2d9a6b91a95dcc151c3e5303cf	no	1
Warnings:					
Information:					
			Total Files Size (in bytes):	166001	

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.
17/952,176	09/23 2022	Steven Michael Colby	SMC-83-C12C3	8353

43198 7590 05/26/2023
Rimon Law, P.C. - SMC
Steven Colby
423 Washington Street, Suite 600
San Francisco, CA 94111

EXAMINER
FRANKLIN, JAMARA ALZAIDA

ART UNIT	PAPER NUMBER
2876	

NOTIFICATION DATE	DELIVERY MODE
05/26/2023	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.rimonlaw@clarivate.com
karen.hagerman@rimonlaw.com
steven.colby@rimonlaw.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

Application No. : 17952176
Applicant : Colby
Filing Date : 09/23/2022
Date Mailed : 05/26/2023

NOTICE TO FILE CORRECTED APPLICATION PAPERS

Notice of Allowance Mailed

This application has been accorded an Allowance Date and is being prepared for issuance. The application, however, is incomplete for the reasons below.

Applicant is given two (2) months from the mail date of this Notice within which to respond. This time period for reply is extendable under 37 CFR 1.136(a) for only TWO additional MONTHS.

The informalities requiring correction are indicated in the attachment(s). If the informality pertains to the abstract, specification (including claims) or drawings, the informality must be corrected with an amendment in compliance with 37 CFR 1.121 (or, if the application is a reissue application, 37 CFR 1.173). Such an amendment may be filed after payment of the issue fee if limited to correction of informalities noted herein. See Waiver of 37 CFR 1.312 for Documents Required by the Office of Patent Publication, 1280 Off. Gaz. Patent Office 918 (March 23, 2004). In addition, if the informality is not corrected until after payment of the issue fee, for purposes of 35 U.S.C. 154(b)(1)(iv), "all outstanding requirements" will be considered to have been satisfied when the informality has been corrected. A failure to respond within the above-identified time period will result in the application being ABANDONED.

See attachment(s).

A copy of this notice MUST be returned with the reply. Please address response to "Mail Stop Issue Fee, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450".

/Quang Nguyen/
Publication Branch
Office of Data Management
(571) 272-4200

Application No. 17952176 **Drawings filed: 09/23/2022**

IDENTIFICATION OF DRAWING DEFICIENCIES

- [ ] There is a hole or the image thereof within the illustration. FIG(s)
- [ ] The illustration is penetrated or traversed by a solid or broken line that is not intended to be part of the drawing, such as a dark line caused by a flaw in the copying process. FIG(s)
- [ ] An ink stamp or the image thereof obscures part of the illustration. FIG(s)
- [ ] The drawing is marred by black smudges, obliterations, or fax/copier marks (for example, speckles or dots in a substantial portion of the drawing). FIG(s)
- [ ] Figure numbers are duplicated or missing. FIG(s)
- [ ] Drawing sheet or figure is missing. FIG(s)
- [ ] Numbers, letters, or reference characters in the drawing have been crossed out or are illegibly handwritten. FIG(s)
- [ ] The character of the lines, numbers, and letters is poor. FIG(s)
- [ ] The drawing's background shows that the original drawing was made on graph paper or other paper with a pattern or decoration. FIG(s)
- [ ] The FIG. number label is placed in a location that causes the drawing to be read upside down. FIG(s)
- [ ] Data, a reference number, or part of the drawing is truncated or missing, or a lead line has no reference number. FIG(s)
- [ ] The drawing and/or the FIG. label contain(s) foreign language. FIG(s)
- [ ] This utility application contains a photograph of a view that is capable of being illustrated as a line drawing. FIG(s)
- [ ] A petition under 37 CFR 1.84(a)(2) to accept color drawings has been granted, but the brief description of the drawings in the specification does not contain (or has not been amended to contain) the paragraph required by 37 CFR 1.84(a)(2)(iii).
- [ ] This reissue application contains added and/or amended drawings that are not labeled as “New” or “Amended” or “Canceled” as required by 37 CFR 1.173(b)(3). FIG(s)
- [ ] This Design reissue application contains a drawing that is labeled as “Canceled” but is not surrounded by brackets, or a drawing that is surrounded by brackets but is not labeled as “Canceled.” See 37 CFR 1.173(b)(3). FIG(s)
- [X] OTHER: See Comment Below
- [X] COMMENTS:
  FIG. 21 contains figure reference numbers "2010B", "2010C" which are not oriented in the same direction as the figure. See 37 CFR 1.84 (p)(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 NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/952,176	09/23/2022	Steven Michael Colby	SMC-83-C12C3	8353

43198 7590 05/17/2023
Rimon Law, P.C. - SMC
Steven Colby
423 Washington Street, Suite 600
San Francisco, CA 94111

EXAMINER
FRANKLIN, JAMARA ALZAIDA

ART UNIT	PAPER NUMBER
2876	

NOTIFICATION DATE	DELIVERY MODE
05/17/2023	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.rimonlaw@clarivate.com
karen.hagerman@rimonlaw.com
steven.colby@rimonlaw.com

Corrected ***Notice of Allowability***	**Application No.** 17/952,176	**Applicant(s)** Colby, Steven Michael	
	Examiner JAMARA A FRANKLIN	**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 the amendment filed on 3/16/23.
   ☐ 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 See Continuation Sheet . 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 _____.
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 _____.

/JAMARA A FRANKLIN/
Primary Examiner, Art Unit 2876

Continuation of 3. The allowed claim(s) is/are: 1,3-13,15-21,23-27 and 29-34

DETAILED ACTION

Acknowledgment is made of the amendment filed on 3/16/23. Claims 1, 3-13, 15-21, 23-27, and 29-34 are currently pending.

Notice of Pre-AIA or AIA Status

The present application is being examined under the pre-AIA first to invent provisions.

Terminal Disclaimer

The terminal disclaimer filed on 2/03/23 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of any patent granted on **U.S. Patent Application No. 17/697,923** has been reviewed and is accepted. The terminal disclaimer has been recorded.

Allowable Subject Matter

Claims 1, 3-13, 15-21, 23-27, and 29-34 are allowed.

The following is an examiner's statement of reasons for allowance: the prior art of record fails to teach or fairly suggest either alone or in combination thereof:

Regarding claim 1, a method of performing a financial transaction using a cellular telephone, the method comprising:

placing the cellular telephone within reading range of a wireless communication device, the cellular telephone being configured to communicate wirelessly using an inductive coupling and an RF antenna, wherein communication by the cellular telephone is responsive to a circuit including an

electronic switch configured to change a state of the circuit, the circuit being configured to communicate responsive to the state of the circuit;

activating the electronic switch within the cellular telephone to change the state of the circuit, activation of the electronic switch being responsive to a biometric sensor included in the cellular telephone; and

communicating financial account information from the cellular telephone to the wireless communication device responsive to the state of the circuit to facilitate the financial transaction, the communication of the financial account information using the inductive coupling or the RF antenna;

regarding claim 19, a method of performing a financial transaction using a cellular telephone, the method comprising:

placing the cellular telephone within reading range of a wireless communication device, the cellular telephone being configured to communicate wirelessly using an RF antenna, wherein the RF antenna is responsive to a circuit including an electronic switch configured to change a state of the circuit, the circuit being configured to communicate via the RF antenna responsive to the state of the circuit;

activating the electronic switch within the cellular telephone to change the state of the circuit, activation of the electronic switch being responsive to entry of a personal identification number; and

communicating financial account information from the cellular telephone to the wireless communication device responsive to the state of the circuit to facilitate the financial transaction, the communication of the financial account information using the RF antenna.

Furthermore claims are allowable in view of the timely filing of the proper terminal disclaimer on 2/03/23.

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

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JAMARA ALZAIDA FRANKLIN whose telephone number is (571)272-2389. The examiner can normally be reached **Monday-Friday, 9:00am-4:30pm**.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **Michael G. Lee** can be reached on **571-272-2398**. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: https://patentcenter.uspto.gov. Visit https://www.uspto.gov/patents/apply/patent-center for more information about Patent Center and https://www.uspto.gov/patents/docx for information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

May 12, 2023

JAF

/JAMARA A FRANKLIN/
Primary Examiner, Art Unit 2876

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/952,176	Colby, Steven Michael
	Examiner	Art Unit
	JAMARA A FRANKLIN	2876

CPC - Searched*		
Symbol	**Date**	**Examiner**
G06K7/10158; G06K7/10316; G06K19/07709; G06K19/07758; G06Q20/227; G06Q20/3278; G06Q20/4012	12/20/2022	JAF
updated search	04/07/2023	JAF

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**
assignee and inventor search	12/20/2022	JAF
considered parent application no. 17/728,412	12/20/2022	JAF
G06K7/10158; G06K7/10316; G06K19/07709; G06K19/07758; G06Q20/227; G06Q20/3278; G06Q20/4012	12/20/2022	JAF
similarity search	12/20/2022	JAF
updated search	04/07/2023	JAF

/JAMARA A FRANKLIN/ Primary Examiner, Art Unit 2876	

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/952,176	Colby, Steven Michael
	Examiner	**Art Unit**
	JAMARA A FRANKLIN	2876

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**
G06K7/10158; G06K7/10316; G06K19/07709 ; G06K19/ 07758; G06Q20/227; G06Q20/3278; G06Q20/4012		04/07/2023	JAF

/JAMARA A FRANKLIN/ Primary Examiner, Art Unit 2876	

SAMSUNG EXHIBIT 1010, Page 19

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/952,176	Colby, Steven Michael
	Examiner	**Art Unit**
	JAMARA A FRANKLIN	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	12/20/2022	04/07/2023	05/12/2023						
1	1	✓	=	=						
-	2	✓	-	-						
2	3	✓	=	=						
3	4	✓	=	=						
4	5	✓	=	=						
5	6	✓	=	=						
6	7	✓	=	=						
7	8	✓	=	=						
8	9	✓	=	=						
9	10	✓	=	=						
10	11	✓	=	=						
11	12	✓	=	=						
12	13	✓	=	=						
-	14	✓	-	-						
13	15	✓	=	=						
14	16	✓	=	=						
15	17	✓	=	=						
16	18	✓	=	=						
19	19	✓	=	=						
20	20	✓	=	=						
21	21	✓	=	=						
-	22	✓	-	-						
22	23	✓	=	=						
24	24	✓	=	=						
25	25	✓	=	=						
26	26	✓	=	=						
27	27	✓	=	=						
-	28	✓	-	-						
28	29	✓	=	=						
29	30	✓	=	=						
19	31		=	=						
20	32		=	=						
30	33		=	=						
23	34		=	=						

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/952,176	Colby, Steven Michael
	Examiner	**Art Unit**
	JAMARA A FRANKLIN	2876

CPC						
Symbol					**Type**	**Version**
G06K	/	7	/	10158	F	2013-01-01
G06Q	/	20	/	4012	I	2013-01-01
G06K	/	19	/	07709	I	2013-01-01
G06Q	/	20	/	3278	I	2013-01-01
G07G	/	1	/	009	I	2013-01-01
G06K	/	7	/	10316	I	2013-01-01
G06Q	/	20	/	227	I	2013-01-01
G06Q	/	20	/	352	I	2013-01-01
G06K	/	19	/	07758	I	2013-01-01

CPC Combination Sets								
Symbol					**Type**	**Set**	**Ranking**	**Version**
	/		/					

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 30	
/JAMARA A FRANKLIN/ Primary Examiner, Art Unit 2876 (Primary Examiner)	12 May 2023 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 31

U.S. Patent and Trademark Office

Part of Paper No.: 20230512

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/952,176	Colby, Steven Michael
	Examiner	**Art Unit**
	JAMARA A FRANKLIN	2876

INTERNATIONAL CLASSIFICATION				
CLAIMED				
G06Q	/	20	/	22

NON-CLAIMED				
	/		/	

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**
235	379

CROSS REFERENCES(S)						
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**					

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 30	
/JAMARA A FRANKLIN/ Primary Examiner, Art Unit 2876 (Primary Examiner)	12 May 2023 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 31

U.S. Patent and Trademark Office

Part of Paper No.: 20230512

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/952,176	Colby, Steven Michael
	Examiner	**Art Unit**
	JAMARA A FRANKLIN	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	9	10	19	19	-	28								
-	2	10	11	20	20	28	29								
2	3	11	12	21	21	29	30								
3	4	12	13	-	22	17	31								
4	5	-	14	22	23	18	32								
5	6	13	15	24	24	30	33								
6	7	14	16	25	25	23	34								
7	8	15	17	26	26										
8	9	16	18	27	27										

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 30	
/JAMARA A FRANKLIN/ Primary Examiner, Art Unit 2876 (Primary Examiner)	12 May 2023 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 31

U.S. Patent and Trademark Office

Part of Paper No.: 20230512

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 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. **Because electronic patent issuance may occur shortly after issue fee payment, any desired continuing application should preferably be filed prior to payment of this issue fee in order not to jeopardize copendency.**

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

43198 7590 04/13/2023
Rimon Law, P.C. - SMC
Steven Colby
423 Washington Street, Suite 600
San Francisco, CA 94111

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.
17/952,176	09/23/2022	Steven Michael Colby	SMC-83-C12C3	8353

TITLE OF INVENTION: Methods of Using a Cellular Telephone

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0.00	$0.00	$480	07/13/2023

EXAMINER	ART UNIT	CLASS-SUBCLASS
FRANKLIN, JAMARA ALZAIDA	2876	705-072000

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/AIA/122 or PTO/SB/122) attached.

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

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

1 _____
2 _____
3 _____

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

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document 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)

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

☑ Electronic Payment via Patent Center or 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

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.

☐ Applicant asserting small entity status. See 37 CFR 1.27

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

☐ Applicant changing to regular undiscounted fee status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: 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 4/13/2023

Typed or printed name Steven Colby Registration No. 50,250

PTOL-85 Part B (08-18) Approved for use through 01/31/2020 OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

SAMSUNG EXHIBIT 1010, Page 24

Electronic Patent Application Fee Transmittal

Application Number:	17952176
Filing Date:	23-Sep-2022
Title of Invention:	Methods of Using a Cellular Telephone
First Named Inventor/Applicant Name:	Steven Michael Colby
Filer:	Steven M. Colby
Attorney Docket Number:	SMC-83-C12C3

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:				
UTILITY APPL ISSUE FEE	2501	1	480	480

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**480**

Electronic Acknowledgement Receipt

EFS ID:	47840674
Application Number:	17952176
International Application Number:	
Confirmation Number:	8353
Title of Invention:	Methods of Using a Cellular Telephone
First Named Inventor/Applicant Name:	Steven Michael Colby
Customer Number:	43198
Filer:	Steven M. Colby
Filer Authorized By:	
Attorney Docket Number:	SMC-83-C12C3
Receipt Date:	13-APR-2023
Filing Date:	23-SEP-2022
Time Stamp:	18:01:00
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$480
RAM confirmation Number	E20234CI01578319
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	Issue Fee Payment (PTO-85B)	FeeTransmittleFiled.pdf	1040768 da37b18cdecf60810d7c61b8008b840fcac39d27	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	37825 5bf879c81c46a84e1373d7f4240aa186d3f03580	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1078593		

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

43198 7590 04/13/2023
Rimon Law, P.C. - SMC
Steven Colby
423 Washington Street, Suite 600
San Francisco, CA 94111

EXAMINER
FRANKLIN, JAMARA ALZAIDA

ART UNIT	PAPER NUMBER
2876	

DATE MAILED: 04/13/2023

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/952,176	09/23/2022	Steven Michael Colby	SMC-83-C12C3	8353

TITLE OF INVENTION: Methods of Using a Cellular Telephone

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0.00	$0.00	$480	07/13/2023

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 40% the amount of undiscounted fees, and micro entity fees are 20% the amount of undiscounted 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. 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.

SAMSUNG EXHIBIT 1010, Page 29

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 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. **Because electronic patent issuance may occur shortly after issue fee payment, any desired continuing application should preferably be filed prior to payment of this issue fee in order not to jeopardize copendency.**

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

43198 7590 04/13/2023
Rimon Law, P.C. - SMC
Steven Colby
423 Washington Street, Suite 600
San Francisco, CA 94111

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.
17/952,176	09/23/2022	Steven Michael Colby	SMC-83-C12C3	8353

TITLE OF INVENTION: Methods of Using a Cellular Telephone

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0.00	$0.00	$480	07/13/2023

EXAMINER	ART UNIT	CLASS-SUBCLASS
FRANKLIN, JAMARA ALZAIDA	2876	705-072000

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/AIA/122 or PTO/SB/122) attached.

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

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

1_____
2_____
3_____

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

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document 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)

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

❑ Electronic Payment via Patent Center or 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

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.

❑ Applicant asserting small entity status. See 37 CFR 1.27

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

❑ Applicant changing to regular undiscounted fee status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: 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 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.
17/952,176	09/23/2022	Steven Michael Colby	SMC-83-C12C3	8353

43198 7590 04/13/2023
Rimon Law, P.C. - SMC
Steven Colby
423 Washington Street, Suite 600
San Francisco, CA 94111

EXAMINER
FRANKLIN, JAMARA ALZAIDA

ART UNIT	PAPER NUMBER
2876	

DATE MAILED: 04/13/2023

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.

SAMSUNG EXHIBIT 1010, Page 31

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. 17/952,176	Applicant(s) Colby, Steven Michael	
	Examiner JAMARA A FRANKLIN	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 the amendment and response filed on 3/16/23.
   ☐ 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 See Continuation Sheet . 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 12/26/22; 12/26/22; 2/02/23;.
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 _____.

/JAMARA A FRANKLIN/
Primary Examiner, Art Unit 2876

Continuation of 3. The allowed claim(s) is/are: 1,3-13,15-21,23-27 and 29-34

DETAILED ACTION

Acknowledgment is made of the amendment filed on 3/16/23. Claims 1, 3-13, 15-21, 23-27, and 29-34 are currently pending.

Notice of Pre-AIA or AIA Status

The present application is being examined under the pre-AIA first to invent provisions.

Terminal Disclaimer

The terminal disclaimer filed on 2/03/23 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of any patent granted on **U.S. Patent Application No. 17/697,923** has been reviewed and is accepted. The terminal disclaimer has been recorded.

Allowable Subject Matter

Claims 1, 3-13, 15-21, 23-27, and 29-34 are allowed.

The following is an examiner's statement of reasons for allowance: the prior art of record fails to teach or fairly suggest either alone or in combination thereof:

Regarding claim 1, a method of performing a financial transaction using a cellular telephone, the method comprising:

placing the cellular telephone within reading range of a wireless communication device, the cellular telephone being configured to communicate wirelessly using an inductive coupling and an RF antenna, wherein communication by the cellular telephone is responsive to a circuit including an

electronic switch configured to change a state of the circuit, the circuit being configured to communicate responsive to the state of the circuit;

activating the electronic switch within the cellular telephone to change the state of the circuit, activation of the electronic switch being responsive to a biometric sensor included in the cellular telephone; and

communicating financial account information from the cellular telephone to the wireless communication device responsive to the state of the circuit to facilitate the financial transaction, the communication of the financial account information using the inductive coupling or the RF antenna;

regarding claim 19, a method of performing a financial transaction using a cellular telephone, the method comprising:

placing the cellular telephone within reading range of a wireless communication device, the cellular telephone being configured to communicate wirelessly using an RF antenna, wherein the RF antenna is responsive to a circuit including an electronic switch configured to change a state of the circuit, the circuit being configured to communicate via the RF antenna responsive to the state of the circuit;

activating the electronic switch within the cellular telephone to change the state of the circuit, activation of the electronic switch being responsive to entry of a personal identification number; and

communicating financial account information from the cellular telephone to the wireless communication device responsive to the state of the circuit to facilitate the financial transaction, the communication of the financial account information using the RF antenna.

Furthermore claims are allowable in view of the timely filing of the proper terminal disclaimer on 2/03/23.

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

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JAMARA ALZAIDA FRANKLIN whose telephone number is (571)272-2389. The examiner can normally be reached **Monday-Friday, 9:00am-4:30pm**.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **Michael G. Lee** can be reached on **571-272-2398**. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: https://patentcenter.uspto.gov. Visit https://www.uspto.gov/patents/apply/patent-center for more information about Patent Center and https://www.uspto.gov/patents/docx for information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

April 07, 2023

JAF

/JAMARA A FRANKLIN/
Primary Examiner, Art Unit 2876

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/952,176	Colby, Steven Michael
	Examiner	**Art Unit**
	JAMARA A FRANKLIN	2876

CPC - Searched*		
Symbol	**Date**	**Examiner**
G06K7/10158; G06K7/10316; G06K19/07709; G06K19/07758; G06Q20/227; G06Q20/3278; G06Q20/4012	12/20/2022	JAF
updated search	04/07/2023	JAF

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**
assignee and inventor search	12/20/2022	JAF
considered parent application no. 17/728,412	12/20/2022	JAF
G06K7/10158; G06K7/10316; G06K19/07709; G06K19/07758; G06Q20/227; G06Q20/3278; G06Q20/4012	12/20/2022	JAF
similarity search	12/20/2022	JAF
updated search	04/07/2023	JAF

/JAMARA A FRANKLIN/ Primary Examiner, Art Unit 2876	

SAMSUNG EXHIBIT 1010, Page 39

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/952,176	Colby, Steven Michael
	Examiner	**Art Unit**
	JAMARA A FRANKLIN	2876

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**
G06K7/10158; G06K7/10316; G06K19/07709 ; G06K19/ 07758; G06Q20/227; G06Q20/3278; G06Q20/4012		04/07/2023	JAF

/JAMARA A FRANKLIN/ Primary Examiner, Art Unit 2876	

SAMSUNG EXHIBIT 1010, Page 40

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/952,176	Colby, Steven Michael
	Examiner	**Art Unit**
	JAMARA A FRANKLIN	2876

CPC

Symbol					Type	Version
G06K	/	7	/	10158	F	2013-01-01
G06Q	/	20	/	4012	I	2013-01-01
G06K	/	19	/	07709	I	2013-01-01
G06Q	/	20	/	3278	I	2013-01-01
G07G	/	1	/	009	I	2013-01-01
G06K	/	7	/	10316	I	2013-01-01
G06Q	/	20	/	227	I	2013-01-01
G06Q	/	20	/	352	I	2013-01-01
G06K	/	19	/	07758	I	2013-01-01

CPC Combination Sets

Symbol					Type	Set	Ranking	Version
	/		/					

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 30	
/JAMARA A FRANKLIN/ Primary Examiner, Art Unit 2876 (Primary Examiner)	07 April 2023 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 31

U.S. Patent and Trademark Office

Part of Paper No.: 20230407

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/952,176	Colby, Steven Michael
	Examiner	**Art Unit**
	JAMARA A FRANKLIN	2876

INTERNATIONAL CLASSIFICATION				
CLAIMED				
G06Q	/	20	/	22

NON-CLAIMED				
	/		/	

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**
235	379

CROSS REFERENCES(S)						
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**					

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 30	
/JAMARA A FRANKLIN/ Primary Examiner, Art Unit 2876 (Primary Examiner)	07 April 2023 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 31

U.S. Patent and Trademark Office

Part of Paper No.: 20230407

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/952,176	Colby, Steven Michael
	Examiner	**Art Unit**
	JAMARA A FRANKLIN	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	9	10	21	19	-	28								
-	2	10	11	22	20	28	29								
2	3	11	12	23	21	29	30								
3	4	12	13	-	22	19	31								
4	5	-	14	17	23	20	32								
5	6	13	15	24	24	30	33								
6	7	14	16	25	25	18	34								
7	8	15	17	26	26										
8	9	16	18	27	27										

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 30	
/JAMARA A FRANKLIN/ Primary Examiner, Art Unit 2876 (Primary Examiner)	07 April 2023 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 31

U.S. Patent and Trademark Office

Part of Paper No.: 20230407

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/952,176	Colby, Steven Michael
	Examiner	**Art Unit**
	JAMARA A FRANKLIN	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	12/20/2022	04/07/2023							
1	1	✓	=							
-	2	✓	-							
2	3	✓	=							
3	4	✓	=							
4	5	✓	=							
5	6	✓	=							
6	7	✓	=							
7	8	✓	=							
8	9	✓	=							
9	10	✓	=							
10	11	✓	=							
11	12	✓	=							
12	13	✓	=							
-	14	✓	-							
13	15	✓	=							
14	16	✓	=							
15	17	✓	=							
16	18	✓	=							
21	19	✓	=							
22	20	✓	=							
23	21	✓	=							
-	22	✓	-							
17	23	✓	=							
24	24	✓	=							
25	25	✓	=							
26	26	✓	=							
27	27	✓	=							
-	28	✓	-							
28	29	✓	=							
29	30	✓	=							
19	31		=							
20	32		=							
30	33		=							
18	34		=							

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	17952176
Filing Date	2022-09-23
First Named Inventor	Colby
Art Unit	2876
Examiner Name	Jamara Alzaida Franklin
Attorney Docket Number	SMC-83-C12C3

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					

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]
	1							

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]

CONSIDERED: /J.A.F/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17952176
Filing Date	2022-09-23
First Named Inventor	Colby
Art Unit	2876
Examiner Name	Jamara Alzaida Franklin
Attorney Docket Number	SMC-83-C12C3

/J.A.F/	1	"Pantech GI100 - Full Phone Specifications" in GSMArena, June 2004, accessed at https://www.gsmarena.com/pantech_gi100-806.php, 2 pages, last accessed February 2, 2023.
/J.A.F/	2	"Counterclockwise: the fingerprint reader goes back, front, back, and side to side" in GSMArena, November 26, 2017, accessed at https://www.gsmarena.com/counterclockwise_the_fingerprint_reader-news-28418.php, 3 pages, last accessed February 2, 2023.
/J.A.F/	3	"Pantech GI100 Fingerprint Scanning Handset - Download Scientific Diagram," March 2008, accessed at https://www.researchgate.net/figure/Pantech-GI100-fingerprint-scanning-handset_fig11_227059965, 1 page, last accessed February 2, 2023.
/J.A.F/	4	"Fujitsu F505i - the world's first fingerprint scanning phone" from The Flipside Story, February 22, 2021, accessed at https://www.youtube.com/watch?v=gWFy3rsK5dg and https://www.theflipside.info/f505i.php (2 pages), last accessed February 2, 2023.

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

EXAMINER SIGNATURE

Examiner Signature	/JAMARA A FRANKLIN/	Date Considered	04/07/2023

*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.

CONSIDERED: /J.A.F/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

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	/Steve Colby, Reg. No. 50,250/	Date (YYYY-MM-DD)	2023-02-02
Name/Print	Steve Colby	Registration Number	50250

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.

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	17952176
Filing Date	2022-09-23
First Named Inventor	Colby
Art Unit	2876
Examiner Name	Jamara Alzaida Franklin
Attorney Docket Number	SMC-83-C12C3

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	5528222	A	1996-06-18	Moskowitz et al.	
	2	6111506	A	2000-08-29	Yap et al.	
	3	6785405	B2	2004-08-31	Tuttle et al.	
	4	7243840	B2	2007-07-17	Bason et al.	
	5	7837119	B2	2010-11-23	Graf et al.	
	6	4774148	A	1988-09-27	Goto	
	7	7336184	B2	2008-02-23	Smith et al.	
	8	6863220	B2	2005-03-08	Selker	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A.F/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

	9	6972662	B1	2005-12-06	Ohkawa et al.	
	10	4068232	A	1978-01-10	Meyers et al.	
	11	4880683	A	1989-11-14	Stow	
	12	7083083	B2	2006-08-01	Droz	
	13	6041412	A	2000-03-21	Timson et al.	
	14	6121544	A	2000-09-19	Petsinger	
	15	6424029	B1	2002-07-23	Giesler	
	16	5869412	A	1999-02-09	Yenni et al.	
	17	6135503	A	2000-10-24	Lob et al.	
	18	7040981	B2	2006-05-09	Iliescu et al.	
	19	6213702	B1	2001-04-10	Wesselink	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

	20	7375631	B2	2008-05-20	Moskowitz et al.	
	21	5815190	A	1998-09-29	Ohshima	
	22	5627544	A	1997-05-06	Snodgrass	
	23	7246754	B2	2007-07-24	Siuta et al.	
	24	6344155	B1	2002-02-05	Kitahara et al.	
	25	7336184	B2	2008-02-26	Smith et al.	
	26	6863220	B2	2005-03-08	Selker	
	27	5606313	A	1997-02-25	Allen et al.	
	28	5815190	A	1998-09-29	Ohshima et al.	
	29	6262364	A	2001-07-17	Yoshikawa et al.	
	30	6097292	A	2000-08-01	Kelly et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A.F/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

	31	7701408	B2	2010-04-20	Bombay et al.	
	32	5963144	A	1999-10-05	Kruest	
	33	6008727	A	1999-12-28	Want et al.	
	34	6025783	A	2000-02-15	Steffens, Jr.	
	35	6380845	B2	2002-04-30	Tuttle	
	36	8487828	B2	2013-07-16	Bombay et al.	
	37	7479882	B2	2009-01-20	Mahaffey	
	38	7924156	B2	2011-04-12	Colby	
	39	7719425	B2	2010-05-18	Colby	
	40	9524485	B2	2016-12-20	Colby	
	41	9569777	B2	2017-02-14	Colby	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A.F/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

	42	8744359	B2	2014-06-03	Ramsten et al.	
	43	7042332	B2	2006-05-09	Takamura et al.	
	44	7466216	B2	2008-12-16	Kawamura et al.	
	45	7346061	B2	2008-03-18	Takayama et al.	
	46	6859650	B1	2005-02-22	Ritter	

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	20060065714	A1	2006-03-30	Jesme	
	2	20060044206	A1	2006-03-02	Moskowitz et al.	
	3	20060261171	A1	2006-11-23	Buursma et al.	
	4	20050188167	A1	2005-08-25	Squibbs et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A.F/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

	5	20050141256	A1	2005-06-30	Yamakazi et al.	
	6	20050140495	A1	2005-06-30	Yamakazi et al.	
	7	20040064698	A1	2004-04-01	Zhang	
	8	20050240778	A1	2005-10-27	Saito	
	9	20020108704	A1	2002-08-15	Umezawa et al.	
	10	20030168514	A1	2003-09-11	Rancien et al.	
	11	20030057286	A1	2003-03-27	Yamagishi et al.	

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	0383059	EP	A1	1990-08-22	Dordevic		
	2	2397272	GB	A	2004-07-21	Lawrence et al.		

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A.F/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

	3	2004/038644	WO	A2	2004-05-06	Powell et al.		
	4	1075781	EP	B1	2001-02-14	Yenni et al.		
	5	11-348471	JP	A	1999-12-12	Funaki et al.		

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	SCHNEE, Thomas, "In Hanau, the portable bus ticket plays at the right price", Berlin, 01nel.com, 5/2/2005.	
	2	DELEURENCE, Guillaume, "Caen, the city where you pay and get information by taking out your mobile phone", J1nel.com, 10/20/2005.	
	3	~~Microsoft NFC Blog~~	
	4	"Identification cards- Contactless integrated circuit(s) cards- proximity cards Part 2: Radio Frequency power and signal interface" - ISO/IEC 14443-2, July 1, 2001.	
	5	"Technical Report - PKI for Machine Readable Travel Documents offering ICC Read-Only access", ICAO PKI, October 1, 2004.	
	6	"Identification cards- Contactless integrated circuit(s) cards- proximity cards Part 3: Initialization and anticollision" - ISO/IEC 14443-3, February 1, 2001.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A.F/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

	7	ELLIS, "Use of Contaclless Integrated Circuits in Machine Readable Travel Documents". ICAO/NTWG, April 16, 2003.	
	8	"Technical Report - Development and Specification of Globally Interoperable Biometric Standards for Machine Assisted Identity Confirmation using Machine Readable Travel Documents", ICAO/NTWG, version 2.0, May 21, 2004.	
	9	FINKENZELLER, "RFID Handbook - Fundamentals and Applications in Contactless Smart Cards and Identification", Second Edition, 2003, John Wiley & Sons Lid.	
	10	JUELS, et al., "Squealing Euros: Privacy Protection in RFID-Enabled Banknotes", Conference Paper in Lecture Notes in Computer Science, January 27-30 2003.	
	11	mifare Data Sheet, Functional Specification, Revision 3.1, Phillips Semiconductors, October 2002.	
	12	"Machine Readable Passports, Specifications for Discretionary Expansion of Data Storage Capacity and Globally nteroperable Biometric Identification", ICAO, Second Draft, Part 1 Volume 2, November 18, 2004.	
	13	"Technical Report - Development of a Logical Data Structure - LOS for Optional Capacity Expansion Technologies", CAO, Revision 1.7, May 18, 2004.	
	14	RANKI, et al., "Smart Card Handbook", Third Edition, 2003, John Wiley & Sons Lid.	
	15	"Annex I - Use of Contactless Integrated Circuits in Machine Readable Travel Documents offering ICC read-only access", ICAO, Version 1.1, October 1, 2004.	
	16	Invalidity of U.S. Patent No. 7,924,156 in view of Mi Fare® Functional Product Specification, Revision 3.1, Published October 2002.	
	17	Invalidity of U.S. Patent No. 7,924,156 in view of RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, Second Edition ("RFID Handbook"), 2003.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A.F/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

	18	Invalidity of U.S. Patent No. 7,924,156 in view of Smart Card Handbook, Third Edition ("Smart Card Handbook"), 2003.
	19	Invalidity of U.S. Patent No. 7,924,156 in view of "Squealing Euros: Privacy Protection in RFID-Enabled Banknotes" ("Juels"), published January 27-30, 2003.
	20	Invalidity of U.S. Patent No. 7,924,156 in view of Juels et al., Security and Privacy Issues in E-Passports ("Juels-2"), No later than April 26, 2005.
	21	Invalidity of U.S. Patent No. 7,924,156 in view of Knospe - RFID Security (2004) ("Knospe")
	22	Invalidity of U.S. Patent No. 7,924,156 in view of Gao et al., An Approach to Security and Privacy of RFID System for Supply Chain ("Gao"), September 2004.
	23	Invalidity of U.S. Patent No. 7,924,156 in view of Weis - Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems (2004).
	24	Invalidity of U.S. Patent No. 7,924,156 in view of EPC Global Specification for RFID Protocols ("EPC Global"), January 2005.
	25	Invalidity of U.S. Patent No. 7,924,156 in view of ICAO 2003 "Use of Contactless Integrated Circuits in MRTDs" APRIL J003 {"ICAO 2003"), April 16, 2003.
	26	Invalidity of U.S. Patent No. 7,924,156 in view of Morgantown ePassports Interoperability Test Sessions, July 27-29, J004.
	27	Invalidity of U.S. Patent No. 7,719,425 in view of "ANNEX I - Use of Contaclless ICs in MRTDs" {"Annex I"), May 5, 2004.
	28	KINNEGING, "Technical Report - PKI for Machine Readable Travel Documents Offering ICC Read-Only Access" {Version 1.1, October 1, 2004). {"ICAO PKI").

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

	29	Technical Report - PKI for Machine Readable Travel Documents Offering ICC Read-Only Access {Version V0.43, April 2, 2004).	
	30	ISO/IEC 14443-1, Identification cards - Contactless integrated circuit{s) cards - Proximity cards Part 1: Physical Characteristics, April 15, 2000.	
	31	ISO/IEC 14443-2, Identification cards - Contactless integrated circuit{s) cards - Proximity cards Part 2: Radio frequency power and signal interface, July 1, 2001.	
	32	ISO/IEC 14443-3, Identification cards - Contactless integrated circuit{s) cards - Proximity cards Part 3: Initialization and anticollision, February 1, 2001.	
	33	TECHNICAL REPORT: DEVELOPMENT OF A LOGICAL DATA STRUCTURE - LDS For OPTIONAL CAPACITY EXPANSION TECHNOLOGIES, ICAO, Revision 1.7, May 18, 2004.	
	34	Technical Report: Development and Specification of Globally Interoperable Biometric Standards for Machine Assisted Identity Confirmation using Machine Readable Travel Documents, ICAO-NTWG, Version 2.0, May 21, 2004.	
	35	Specifications for discretionary expansion of Data Storage Capacity and Globally Interoperable Biometric Identification, CAO, Part 1, Volume 2, November 18, 2004.	
	36	Securing (biometric) data stored in a contaclless chip, ICAO-NTWG, Version 0.7, September 15, 2003.	
	37	In the United States Court of Federal Claims, Case 16-cv-01647-RTH, Defentants' February 19, 2021 PRCFC 6-7 Invalidity Contentions, Filed 2/19/21, 105 pages.	
	38	KUKLINSKI, "Automated Authentication of Current Identity", 2004 IEEE Conference on Technologies for Homeland Security, Cambridge, MA, April 21 22, 2004	
	39	"Denmark to Launch First Country-wide Scheme", Smart Card News Ltd., Brighton England, 1992.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

	40	"Post Office Plans £19.5m Terminal Network in UK", Smart Card News, April 1993, Vol. 2, No. 4.	
	41	"P&O Passengers Enjoy Cashless Cruising", Smart Card News, April 1994.	
	42	"Smart Card Payphones on Channel Tunnel Trains", Smart Card News, August 1994.	
	43	"Japan and USA to Push Smart Card Technology", Smart Card News, August 1993.	
	44	"NatWest Launch Mondex Global Electronic Cash", Smart Card News, December 1993.	
	45	"British Govt Launches Smart Card Initiative", Smart Card News, December 1997, Vol. 6, No. 12.	
	46	"Gaudi Multiservice Smart Card Trials in Dublin", Smart Card News, February 1994.	
	47	"Austria Starts Trials for National Electronic Purse", Smart Card News, February 1995.	
	48	"Smart Card Being Used in Swiss Ski Resorts", Smart Card News, January 1993, Vol. 2, No. 1.	
	49	"Shell Loyalty Scheme Launched in Scotland", Smart Card News, July 1994.	
	50	"Major Stored Value Card Plan in Australia", Smart Card News, June 1993.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

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

EXAMINER SIGNATURE

Examiner Signature	/JAMARA A FRANKLIN/	Date Considered	04/07/2023

*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.

CONSIDERED: /J.A.F/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

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	/Steve Colby, Reg. No. 50,250/	Date (YYYY-MM-DD)	2022-12-26
Name/Print	Steve Colby	Registration Number	50250

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.

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	17952176
Filing Date	2022-09-23
First Named Inventor	Colby
Art Unit	2876
Examiner Name	Jamara Alzaida Franklin
Attorney Docket Number	SMC-83-C12C3

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					

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]
	1							

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]

CONSIDERED: /J.A.F/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

/J.A.F/	1	"Mobile Credit Card from Barclaycard and Mercury", Smart Card News, June 1994.	
/J.A.F/	2	"Lufthansa AirPlus Card for Frequent Flyers", Smart Card News, March 1993, Vol. 2, No. 2.	
/J.A.F/	3	"Portugal to Lead Europe with Electronic Purse", Smart Card News, May 1993, Vol. 2, No. 5.	
/J.A.F/	4	"Patient Smart Card Trials in Portugal and UK", Smart Card News, May 1994	
/J.A.F/	5	"Sun Launches Java Card API for Smart Cards", Smart Card News, November 1996, Vol. 5, No. 11.	
/J.A.F/	6	"Social Security Card Pilot in Spain to Prevent Fraud", Smart Card News, November 1994.	
/J.A.F/	7	"Russian Banks to Introduce Smart Card Technology", Smart Card News, November 1993.	
/J.A.F/	8	"Spanish Banks to Launch Electronic Purse Scheme", Smart Card News, October 1993.	
/J.A.F/	9	"British Gas Leads with UK National Network", Smart Card News, September 1992, Vol. 1, No. 1.	
/J.A.F/	10	"Bank Passbook and Purse in Indonesia", Smart Card News, September 1993.	
/J.A.F/	11	"Mikcon Austria Bid for World Ticket Card", Smart Card News, September 1994.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

/J.A.F/	12	"Rabobank Success in Electronic Banking", Smart Card News, February 1993, Vol. 2, No. 2.	
/J.A.F/	13	"Emergency Health Card Trials to Start in Ireland", Smart Card News, March 1995.	
	14	Passport Statistics, Travel.State.Gov, hllps://travel.state.gov/content/travel/en/passports/after/passport-statistics.html.	
/J.A.F/	15	In the United States Court of Federal Claims, Case 1:16-cv-01647-SGB, Document 68, Filed 8/17/18, 43 pages.	
/J.A.F/	16	International Standard ISO/IEC FEDIS 14443-1: Final Draft. Identification cards- Contactless Integrated circuit(s) cards - Proximity Cards Parts 1: Physical characteristics. ISO/IEC 2000, 1/11/2000.	
/J.A.F/	17	ISO/IEC JTC1/SC-17. Identification cards- Contactless integrated circuit(s) cards- Proximity cards - Part 2: Radio frequency power and signal interface, 10/8/2003.	
/J.A.F/	18	ISO/IEC JTC 1/SC 17. Identification cards m Contactless integrated circuit(s) cards - Proximity cards - Part 3: Initialization and anticollision, 7/27/2000.	
/J.A.F/	19	ISO/IEC JTC 1/SC 17, Identification cards m Contactless integrated circuit(s) cards - Proximity cards - Part 4: Transmission protocol, 12/4/2000.	
/J.A.F/	20	Biometrics Deployment of Machine Readable Travel Documents, ICAO NTWG Biometrics TR v2-0 final TAG 15 7/6/2004.	
/J.A.F/	21	Machine Readable Travel Documents. Development of A Logical Data Structure - LOS for Optional Capacity Expansion Technologies, LOS-technical report -Version 1.7 Approved 6/4/2004.	
/J.A.F/	22	Machine Readable Travel Documents. Supplement to 6th Edition. Part 1.Doc 9303.Release_ 4.June2006 6/19/2006.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

/J.A.F/	23	Machine Readable Travel Documents Technical Report, PKI for Machine Readable Travel Documents offering ICC Read-Only Access. TR-PKI for MRTDs offering ICC Read-Only Access VI. 1. 10/4/2004.	
/J.A.F/	24	International Standard ISO/IEC 7816, Information Technology. Identification cards. Integrated circuit{s) cards with contacts.Part 4: Interindustry commands for interchange. 5/18/2001.	
/J.A.F/	25	International Standard ISO/IEC 7816, Information Technology. Identification cards. Integrated circuit{s) cards with contacts Part 6: Interindustry data elements. 5/18/2001.	
/J.A.F/	26	International Standard ISO/IEC 7816, Information Technology. Identification cards. Integrated circuit{s) cards with contacts Part 8: Security related interindustry commands. 5/18/2001.	
/J.A.F/	27	International Standard ISO/IEC 7816, Information Technology_ Identification cards. Integrated circuit{s) cards with contacts Part 9: Additional interindustry commands and security attributes. 5/18/2001.	
/J.A.F/	28	International Standard, ISO/IEC 14443-3. Identification Cards Integrated circuit{s) cards with contacts. Part 3: Initialization and anticollision. 7/4/2005.	
/J.A.F/	29	International Standard, ISO/IEC 14443-3. Identification Cards Integrated circuit{s) cards with contacts. Proximity cards. Part 4: Transmission Protocol.7/4/2005.	
/J.A.F/	30	First DRAFT 15th August 2005, Machine Readable Travel Documents, 8/15/2005.	
/J.A.F/	31	International Standard, ISO/IEC 1443-2. Identification cards. Integrated circuit{s) cards with contacts. Proximity Cards. Part 2: Radio frequency power and signal interface. 9/18/2017.	
/J.A.F/	32	"BT Tender for Smart Payphones and Cards", Smart Card News, January 1994.	
/J.A.F/	33	"Swiss Electronic Purse to go Nationwide in 1995", Smart Card News, July 1993.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

/J.A.F/	34	Office Action issued in U.S. Patent Application No. 17/697923, mailed June 8, 2022, 7 pages.
/J.A.F/	35	FINKENZELLER, "RFID Handbook - Fundamentals and Applications in Contactless Smart Cards and Identification", Second Edition, 2003, John Wiley & Sons Ltd.
/J.A.F/	36	RANKI, et al., "Smart Card Handbook", Third Edition, 2003, John Wiley & Sons Ltd.

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

EXAMINER SIGNATURE

Examiner Signature	/JAMARA A FRANKLIN/	Date Considered	04/07/2023

*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	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

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	/Steve Colby, Reg. No. 50,250/	Date (YYYY-MM-DD)	2022-12-26
Name/Print	Steve Colby	Registration Number	50250

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

APPLICANT:	Mynette Technologies, Inc.
APPLICATION NO.:	17/952,176
CONFIRMATION NO.:	8353
FILING DATE:	23-SEP-2022
TITLE:	Methods of Using a Cellular Telephone
EXAMINER:	Unknown
ART UNIT:	2876
ATTY. DKT. NO.:	SMC-83-C12C3

Preliminary Amendment B

In response to the Office Action of December 28, 2022, please Consider the following. Amendments to the claims begin on page 2.

Remarks begin on page 7.

SAMSUNG EXHIBIT 1010, Page 70

Listing of CLAIMS

1. (Previously Presented) A method of performing a financial transaction using a cellular telephone, the method comprising:

placing the cellular telephone within reading range of a wireless communication device, the cellular telephone being configured to communicate wirelessly using an inductive coupling and an RF antenna, wherein communication by the cellular telephone is responsive to a circuit including an electronic switch configured to change a state of the circuit, the circuit being configured to communicate responsive to the state of the circuit;

activating the electronic switch within the cellular telephone to change the state of the circuit, activation of the electronic switch being responsive to a biometric sensor included in the cellular telephone; and

communicating financial account information from the cellular telephone to the wireless communication device responsive to the state of the circuit to facilitate the financial transaction, the communication of the financial account information using the inductive coupling or the RF antenna.

2. (Cancelled) ~~The method of claim 1, wherein the cellular telephone includes the biometric sensor.~~

3. (Original) The method of claim 1, wherein the circuit is configured to facilitate the financial transaction responsive to the biometric sensor.

4. (Original) The method of claim 1, wherein the circuit is configured to approve the financial transaction responsive to the biometric sensor.

5. (Previously Presented) The method of claim 1, wherein the circuit is configured to communicate the financial account information responsive to the biometric sensor.

6. (Original) The method of claim 1, wherein the circuit is changed from a first ON state to a second ON state, responsive to the electronic switch, and wherein the circuit includes a memory configured to store the first and second ON states.

7. (Original) The method of claim 1, wherein the circuit is changed from a first ON state to a second ON state, responsive to the electronic switch, and wherein different

SAMSUNG EXHIBIT 1010, Page 71

amounts of personal information are communicated via the inductive coupling or RF antenna in the first ON state relative to the second ON state.

8. (Original) The method of claim 1, wherein the circuit is configured to store transaction logs.

9. (Original) The method of claim 1, wherein the circuit is configured for a user to select between a plurality of financial accounts for the financial transaction.

10. (Previously Presented) The method of claim 1, wherein the cellular telephone is configured for a user to enter an amount of the financial transaction, and further comprising entering the amount to facilitate the financial transaction.

11. (Previously Presented) The method of claim 1, wherein the circuit is configured to communicate a financial account number via the inductive coupling or RF antenna to facilitate the financial transaction.

12. (Original) The method of claim 1, wherein the cellular telephone includes a user interface configured to enter a financial account number and includes memory configured to store the financial account number for use in the financial transaction.

13. (Previously Presented) The method of claim 1, wherein the cellular telephone is configured for a user to enter a personal identification number (PIN), communication of the financial account information via the inductive coupling or RF antenna being responsive to the personal identification number; and further comprising entering the personal identification number to facilitate the financial transaction.

14. (Cancelled) ~~The method of claim 1, wherein the cellular telephone includes a memory configured to store an encryption key used to facilitate the financial transaction.~~

15. (Original) The method of claim 1, wherein the cellular telephone includes a memory configured to store a key required to change the state of the circuit to facilitate the financial transaction.

16. (Previously Presented) The method of claim 1, wherein the cellular telephone is configured for mechanical insertion of an electronic key, the electronic key including a personal identification number, a signal communicated via the

inductive coupling or RF antenna to facilitate the financial transaction being responsive to entry of the personal identification number by a user.

17. (Previously Presented) The method of claim 1, wherein the cellular telephone is configured to store a financial account number and the communication via the inductive coupling or RF antenna including the financial account number.

18. (Previously Presented) The method of claim 1, wherein activating the electronic switch is responsive to data stored in memory of the cellular telephone and the data stored in the memory includes biometric data.

19. (Original) A method of performing a financial transaction using a cellular telephone, the method comprising:

placing the cellular telephone within reading range of a wireless communication device, the cellular telephone being configured to communicate wirelessly using an RF antenna, wherein the RF antenna is responsive to a circuit including an electronic switch configured to change a state of the circuit, the circuit being configured to communicate via the RF antenna responsive to the state of the circuit;

activating the electronic switch within the cellular telephone to change the state of the circuit, activation of the electronic switch being responsive to entry of a personal identification number; and

communicating financial account information from the cellular telephone to the wireless communication device responsive to the state of the circuit to facilitate the financial transaction, the communication of the financial account information using the RF antenna.

20. (Currently Amended) The method of claim 19, wherein the communication of the financial account information is responsive to a biometric sensor and a mechanical switch included in the cellular telephone.

21. (Original) The method of claim 19, further comprising approving the financial transaction using a biometric sensor.

22. (Cancelled) ~~The method of claim 19, further comprising approving the financial transaction using a mechanical switch.~~

SAMSUNG EXHIBIT 1010, Page 73

23. (Previously Presented) The method of claim 19, wherein the cellular telephone includes a user interface configured for a user to enter a financial account number for use in the financial transaction. .

24. (Previously Presented) The method of claim 19, wherein the circuit is configured for a user to select between a plurality of financial accounts for the financial transaction.

25. (Original) The method of claim 19, wherein the circuit is changed from a first ON state to a second ON state, responsive to the electronic switch, and wherein different amounts of personal information are communicated via the RF antenna in the first ON state relative to the second ON state.

26. (Original) The method of claim 19, wherein the circuit is configured to store transaction logs.

27. (Previously Presented) The method of claim 19, wherein the circuit is configured to communicate a financial account number via the RF antenna to facilitate the financial transaction.

28. (Cancelled) ~~The method of claim 19, wherein the cellular telephone is configured for insertion of a memory, the memory including account information and a personal identification number, and a signal communicated via the RF antenna to facilitate the financial transaction being responsive to the account information and the personal identification number~~.

29. (Previously Presented) The method of claim 19, wherein the cellular telephone is configured for storing a password in memory of the cellular phone, the password being entered by a user of the cellular phone to engage in the transaction.

30. (Previously Presented) The method of claim 19, wherein the cellular telephone is configured for insertion of an electronic key, the electronic key being configured to store the personal identification number, the communication via the RF antenna being responsive to the personal identification number.

31. (Previously Presented) The method of claim 1, wherein the financial account information includes an account number corresponding to a financial account of a user of the cellular telephone.

32. (Previously Presented) The method of claim 1, wherein the financial account information is stored in a memory on the cellular telephone, the financial account information corresponding to one of a plurality of financial accounts of a user of the cellular telephone, the method further comprising:

presenting a user interface to the user, the user interface being configured to allow the user to select a specific member of the plurality of financial accounts of the user for the financial transaction; and

wherein the step of communicating financial account information includes communicating financial account information corresponding to the selected specific member of the plurality of financial accounts.

33. (Previously Presented) The method of claim 19, wherein the cellular telephone is configured for a user to enter an amount of the financial transaction.

34. (Previously Presented) The method of claim 23, wherein the cellular telephone includes memory configured to store the financial account number, wherein the circuit is configured for the user to select between a plurality of financial accounts for the financial transaction; and further comprising selecting a specific member of the plurality of financial accounts for the financial transaction.

REMARKS

Claims 1, 3-13, 15-21, 23-27 and 29-34 are currently pending herein.

Claim 20 is currently Amended.

Claims 2, 14, 22 and 28 were previously cancelled.

Examiner Interview

The Applicant and Examiner Franklin held an Examiner Interview on Feb. 2, 2023. The Applicant and Examiner discussed the need for a Terminal Disclaimer. The Examiner pointed out several references, which have since been included in a filed IDS.

Conclusion

In view of the filed Terminal Disclaimer, Applicant believes that all claims are now in condition for allowance and requests a notice of allowance.

Respectfully submitted,

Date: March 14, 2023 /Steven M. Colby 50,250/

Dr. Steven M. Colby, JD, Ph.D.
(Reg. No. 50,250)
Partner, Rimon PC
CEO, Mynette Technologies, Inc.

Electronic Acknowledgement Receipt

EFS ID:	47692301
Application Number:	17952176
International Application Number:	
Confirmation Number:	8353
Title of Invention:	Methods of Using a Cellular Telephone
First Named Inventor/Applicant Name:	Steven Michael Colby
Customer Number:	43198
Filer:	Steven M. Colby
Filer Authorized By:	
Attorney Docket Number:	SMC-83-C12C3
Receipt Date:	16-MAR-2023
Filing Date:	23-SEP-2022
Time Stamp:	11:41:55
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		SMC-83-C12C3-Amendment-B-filing.pdf	138801 e33bafcc1118d51cf1005ea4e9ea04eb8d947443	yes	7

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Request for Reconsideration-After Non-Final Rejection	1	1
	Claims	2	6
	Applicant Arguments/Remarks Made in an Amendment	7	7

Warnings:	
Information:	
Total Files Size (in bytes):	138801

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 17/952,176	Filing Date 09/23/2022	☐ 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 $240 =	
☐ 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

AMENDMENT	03/16/2023	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 30	Minus	** 30	= 0		x $40 =	0
	Independent (37 CFR 1.16(h))	* 2	Minus	*** 3	= 0		x $192 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) 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.	SLIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/APRIL L. WALKER/
*** 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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/952,176	09/23/2022	Steven Michael Colby	SMC-83-C12C3	8353

43198 7590 02/08/2023
Rimon Law, P.C. - SMC
Steven Colby
423 Washington Street, Suite 600
San Francisco, CA 94111

EXAMINER
FRANKLIN, JAMARA ALZAIDA

ART UNIT	PAPER NUMBER
2876	

NOTIFICATION DATE	DELIVERY MODE
02/08/2023	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.rimonlaw@clarivate.com
karen.hagerman@rimonlaw.com
steven.colby@rimonlaw.com

Applicant-Initiated Interview Summary	Application No. 17/952,176	Applicant(s) Colby, Steven Michael		
	Examiner JAMARA A FRANKLIN	Art Unit 2876	AIA (First Inventor to File) Status No	Page 1 of 1

All Participants (applicant, applicants representative, PTO personnel)	Title	Type
JAMARA A FRANKLIN	Primary Examiner	Telephonic
Steven Colby	Attorney of Record	

Date of Interview: 02 February 2023

Issues Discussed:

Non-statutory Double Patenting

The applicant's representative and the examiner discussed the standing of the current double patenting rejection.

/JAMARA A FRANKLIN/ Primary Examiner, Art Unit 2876	

Applicant is reminded that a complete written statement as to the substance of the interview must be made of record in the application file. It is the applicants responsibility to provide the written statement, unless the interview was initiated by the Examiner and the Examiner has indicated that a written summary will be provided. See MPEP 713.04
Please further see:
MPEP 713.04
Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews, paragraph (b)
37 CFR § 1.2 Business to be transacted in writing

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

Doc Code: DIST.E.FILE **Document Description: Electronic Terminal Disclaimer - Filed**	PTO/SB/25 U.S. Patent and Trademark Office Department of Commerce

Electronic Petition Request	**TERMINAL DISCLAIMER TO OBVIATE A PROVISIONAL DOUBLE PATENTING REJECTION OVER A PENDING "REFERENCE" APPLICATION**
Application Number	17952176
Filing Date	23-Sep-2022
First Named Inventor	Steven Colby
Attorney Docket Number	SMC-83-C12C3
Title of Invention	Methods of Using a Cellular Telephone

☒ 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
MYNETTE TECHNOLOGIES, INC.	100%

The owner(s) of 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 any patent granted on pending reference Application Number(s)

17697923 filed on 03/18/2022

as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application. 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 any patent granted on the reference application 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 any patent granted on the instant application that would extend to the expiration date of the full statutory term of any patent granted on said reference application, "as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application," in the event that any such patent granted on the pending reference application: 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 shortened by any terminal disclaimer filed prior to its grant.

◉ 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 _____

◉ 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	/Steven M. Colby 50,250/
Name	Steven M. Colby

*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:	17952176
Filing Date:	23-Sep-2022
Title of Invention:	Methods of Using a Cellular Telephone
First Named Inventor/Applicant Name:	Steven Michael Colby
Filer:	Steven M. Colby
Attorney Docket Number:	SMC-83-C12C3

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.: 17952176

Filing Date: 23-Sep-2022

Applicant/Patent under Reexamination: Colby

Electronic Terminal Disclaimer filed on February 3, 2023

☒ 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:	47480049
Application Number:	17952176
International Application Number:	
Confirmation Number:	8353
Title of Invention:	Methods of Using a Cellular Telephone
First Named Inventor/Applicant Name:	Steven Michael Colby
Customer Number:	43198
Filer:	Steven M. Colby
Filer Authorized By:	
Attorney Docket Number:	SMC-83-C12C3
Receipt Date:	03-FEB-2023
Filing Date:	23-SEP-2022
Time Stamp:	17:58:35
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$170
RAM confirmation Number	E202323H58323616
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	43554 05e6404a97dc9365ef3e4943066222a146d269ee	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	37931 2ae5beb4c6a1c76ac85b548b6e65a3167bbf50c8	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	81485		

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/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	17952176
Filing Date	2022-09-23
First Named Inventor	Colby
Art Unit	2876
Examiner Name	Jamara Alzaida Franklin
Attorney Docket Number	SMC-83-C12C3

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					

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]
	1							

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]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

	1	"Pantech GI100 - Full Phone Specifications" in GSMArena, June 2004, accessed at https://www.gsmarena.com/pantech_gi100-806.php, 2 pages, last accessed February 2, 2023.	
	2	"Counterclockwise: the fingerprint reader goes back, front, back, and side to side" in GSMArena, November 26, 2017, accessed at https://www.gsmarena.com/counterclockwise_the_fingerprint_reader-news-28418.php, 3 pages, last accessed February 2, 2023.	
	3	"Pantech GI100 Fingerprint Scanning Handset - Download Scientific Diagram," March 2008, accessed at https://www.researchgate.net/figure/Pantech-GI100-fingerprint-scanning-handset_fig11_227059965, 1 page, last accessed February 2, 2023.	
	4	"Fujitsu F505i - the world's first fingerprint scanning phone" from The Flipside Story, February 22, 2021, accessed at https://www.youtube.com/watch?v=gWFy3rsK5dg and https://www.theflipside.info/f505i.php (2 pages), last accessed February 2, 2023.	

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	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

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	/Steve Colby, Reg. No. 50,250/	Date (YYYY-MM-DD)	2023-02-02
Name/Print	Steve Colby	Registration Number	50250

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

Electronic Acknowledgement Receipt

EFS ID:	47472501
Application Number:	17952176
International Application Number:	
Confirmation Number:	8353
Title of Invention:	Methods of Using a Cellular Telephone
First Named Inventor/Applicant Name:	Steven Michael Colby
Customer Number:	43198
Filer:	Steven M. Colby/Susan Stewart
Filer Authorized By:	Steven M. Colby
Attorney Docket Number:	SMC-83-C12C3
Receipt Date:	02-FEB-2023
Filing Date:	23-SEP-2022
Time Stamp:	16:41:13
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)	IDS_C12C3_SB08_Feb_2023.pdf	1035491 802d8a29e8fc360558e47daa46b33c7df11d0f9a	no	4

Warnings:

Information:					
A U.S. Patent Number Citation or a U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form for autoloading of data into USPTO systems. You may remove the form to add the required data in order to correct the Informational Message if you are citing U.S. References. If you chose not to include U.S. References, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.					
2	Non Patent Literature	NPL_1_Pantech_GI100_Full_phone_specifications.pdf	461012 d664b28bf9f8d39d8c2e50dcb553a309f3cbed65	no	2
Warnings:					
Information:					
3	Non Patent Literature	NPL_2_Counterclockwise_the_fingerprint_GSMArena.pdf	699825 9a380301489893e555eba6ac17f3e0f4713d6a77	no	3
Warnings:					
Information:					
4	Non Patent Literature	NPL3_Pantech-GI100_Fingerprint_Scanning_Handset.pdf	32526 d1d4f61a3dfbf5502f35c1fc45e337174686605d	no	1
Warnings:					
Information:					
5	Non Patent Literature	NPL_4_The_Flipside_Story_Fujitsu_F505i.pdf	407794 b8a1135348721224 5bce0c278e682dec5c53e1ff	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	2636648	

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.
17/952,176	09/23/2022	Steven Michael Colby	SMC-83-C12C3	8353

43198 7590 12/28/2022
Rimon Law, P.C. - SMC
Steven Colby
423 Washington Street, Suite 600
San Francisco, CA 94111

EXAMINER
FRANKLIN, JAMARA ALZAIDA

ART UNIT	PAPER NUMBER
2876	

NOTIFICATION DATE	DELIVERY MODE
12/28/2022	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.rimonlaw@clarivate.com
karen.hagerman@rimonlaw.com
steven.colby@rimonlaw.com

Office Action Summary	Application No. 17/952,176	Applicant(s) Colby, Steven Michael	
	Examiner JAMARA A FRANKLIN	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 _____.

☐ 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) 1-30 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) 1-30 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 9/23/22 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 _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

DETAILED ACTION

The instant application is a continuation of application no. 17/728,412. Claims 1-30 are currently pending.

Notice of Pre-AIA or AIA Status

The present application is being examined under the pre-AIA first to invent provisions.

Claim Objections

Claim 1 is objected to because of the following informalities:

In claim 1, line 6, the word "(verb)" appears to be erroneously present.

Appropriate correction is required.

Double Patenting

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

Claim 1-30 are provisionally rejected on the ground of nonstatutory double patenting as being unpatentable over claim 1-24 of copending Application No. 17/697,923/ Publication No. 2022/0207251 (reference application). Although the claims at issue are not identical, they are not patentably distinct from each other because both the instant application and Publication No. 2022/0207251 claim:

Regarding claim 1, a method of performing a financial transaction using a cellular telephone, the method comprising:

placing the cellular telephone within reading range of a wireless communication device, the cellular telephone being configured to communicate wirelessly using an inductive coupling and an RF

antenna, wherein the communication (verb) is responsive to a circuit including an electronic switch configured to change a state of the circuit, the circuit being configured to communicate responsive to the state of the circuit;

activating the electronic switch within the cellular telephone to change the state of the circuit; and

communicating financial account information from the cellular telephone to the wireless communication device responsive to the state of the circuit to facilitate the financial transaction, the communication of the account information using the inductive coupling or the RF antenna (see claim 1 of Pub No. '251);

the method of claim 1, wherein the circuit is changed from a first ON state to a second ON state, responsive to the electronic switch (see claim 4 of Pub No. '251);

the method of claim 1, wherein the circuit is changed from a first ON state to a second ON state, responsive to the electronic switch, and wherein different amounts of personal information are communicated via the inductive coupling or RF antenna in the first ON state relative to the second ON state (see claim 5 of Pub No. '251);

the method of claim 1, wherein the circuit is configured to store transaction logs (see claim 8 of Pub No. '251);

the method of claim 1, wherein the circuit is configured for a user to select between a plurality of financial accounts for the financial transaction (see claim 9 of Pub No. '251);

the method of claim 1, further comprising entering a personal identification number or a password to facilitate the financial transaction (see claim 11 of Pub No. '251);

the method of claim 1, wherein the circuit is configured to communicate an account number via the inductive coupling or RF antenna to facilitate the financial transaction (see claim 12 of Pub No. '251);

the method of claim 1, wherein the cellular telephone includes a user interface configured to enter a financial account number and includes memory configured to store the financial account number for use in the financial transaction (see claim 16 of Pub No. '251);

the method of claim 1, wherein the cellular telephone is configured for a user to enter a personal identification number (PIN), communication of the financial account information via the inductive coupling or RF antenna being responsive to the personal identification number (see claim 14 of Pub No. '251);

the method of claim 1, wherein the cellular telephone includes a memory configured to store an encryption key used to facilitate the financial transaction (see claim 17 of Pub No. '251);

the method of claim 1, wherein the cellular telephone includes a memory configured to store a key required to change the state of the circuit to facilitate the financial transaction (see claim 17 of Pub No. '251);

the method of claim 1, wherein the cellular telephone is configured for insertion of an electronic key, the electronic key including a personal identification number, a signal communicated via the inductive coupling or RF antenna to facilitate the financial transaction being responsive to entry of the personal identification number by a user (see claim 21 of Pub No. '251);

the method of claim 1, wherein the cellular telephone is configured for insertion of an electronic key, the electronic key including an account identifier and the communication via the inductive coupling or RF antenna being responsive to the account identifier, the electronic key being configured to store a password or personal identification number (see claim 21 of Pub No. '251).

Claims 1-18 lack the teaching of a biometric sensor.

One of ordinary skill in the art would have readily recognized that a biosensor would be beneficial as an added element of security for a transaction to limit fraudulent spending or hacking.

Therefore it would have been obvious at the time the invention was made to modify claims 1-24 of Pub No '251 to arrive at claims 1-18 of the instant application.

Regarding claim 19, a method of performing a financial transaction using a cellular telephone, the method comprising:

placing the cellular telephone within reading range of a wireless communication device, the cellular telephone being configured to communicate wirelessly using an RF antenna, wherein the RF antenna is responsive to a circuit including an electronic switch configured to change a state of the circuit, the circuit being configured to communicate via the RF antenna responsive to the state of the circuit;

activating the electronic switch within the cellular telephone to change the state of the circuit, activation of the electronic switch being responsive to entry of a personal identification number; and

communicating financial account information from the cellular telephone to the wireless communication device responsive to the state of the circuit to facilitate the financial transaction, the communication of the financial account information using the RF antenna (see claim 1 of Pub No. '251);

the method of claim 19, further comprising approving the financial transaction using a mechanical switch (see claim 2 of Pub No. '251);

the method of claim 19, wherein the cellular telephone includes a user interface configured to enter a financial account number and includes memory configured to store the financial account number for use in the financial transaction (see claim 1 of Pub No. '251);

the method of claim 19, wherein the circuit is configured for a user to select between a plurality of financial accounts for the financial transaction (see claim 9 of Pub No. '251);

the method of claim 19, wherein the circuit is changed from a first ON state to a second ON state, responsive to the electronic switch, and wherein different amounts of personal information are

communicated via the RF antenna in the first ON state relative to the second ON state (see claim 6 of Pub No. '251)

the method of claim 19, wherein the circuit is configured to store transaction logs (see claim 8 of Pub No. '251);

The method of claim 19, wherein the cellular telephone is configured for insertion of a memory, the memory including account information and a personal identification number, and a signal communicated via the RF antenna to facilitate the financial transaction being responsive to the account information and the personal identification number (see claim 9 of Pub No. '251).

One of ordinary skill in the art would have readily recognized that the claims of the instant application are an obvious variant of the claims of the Pub No. '251 and differ only in terminology. Therefore it would have been obvious at the time the invention was made to modify claims 1-24 of Pub No '251 to arrive at claims 19-30 of the instant application.

This is a provisional nonstatutory double patenting rejection because the patentably indistinct claims have not in fact been patented.

Allowable Subject Matter

Claims 1-30 are allowable over prior art.

The following is a statement of reasons for the indication of allowable subject matter: the prior art of record fails to teach or fairly suggest either alone or in combination thereof:

Regarding claim 1, a method of performing a financial transaction using a cellular telephone, the method comprising:

placing the cellular telephone within reading range of a wireless communication device, the cellular telephone being configured to communicate wirelessly using an inductive coupling and an RF

antenna, wherein the communication is responsive to a circuit including an electronic switch configured to change a state of the circuit, the circuit being configured to communicate responsive to the state of the circuit;

activating the electronic switch within the cellular telephone to change the state of the circuit, activation of the electronic switch being responsive to a biometric sensor; and

communicating financial account information from the cellular telephone to the wireless communication device responsive to the state of the circuit to facilitate the financial transaction, the communication of the account information using the inductive coupling or the RF antenna; and

regarding claim 19, a method of performing a financial transaction using a cellular telephone, the method comprising:

placing the cellular telephone within reading range of a wireless communication device, the cellular telephone being configured to communicate wirelessly using an RF antenna, wherein the RF antenna is responsive to a circuit including an electronic switch configured to change a state of the circuit,

the circuit being configured to communicate via the RF antenna responsive to the state of the circuit;

activating the electronic switch within the cellular telephone to change the state of the circuit, activation of the electronic switch being responsive to entry of

a personal identification number; and

communicating financial account information from the cellular telephone to the wireless communication device responsive to the state of the circuit to facilitate the financial transaction, the communication of the financial account information using the RF antenna.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JAMARA ALZAIDA FRANKLIN whose telephone number is (571)272-2389. The examiner can normally be reached **Monday-Friday, 9:00am-4:30pm**.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **Michael G. Lee** can be reached on **571-272-2398**. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: https://patentcenter.uspto.gov. Visit https://www.uspto.gov/patents/apply/patent-center for more information about Patent Center and https://www.uspto.gov/patents/docx for information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

December 20, 2022

JAF

/JAMARA A FRANKLIN/
Primary Examiner, Art Unit 2876

Notice of References Cited	Application/Control No. 17/952,176	Applicant(s)/Patent Under Reexamination Colby, Steven Michael	
	Examiner JAMARA A FRANKLIN	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-20220207251-A1	06-2022	Colby; Steven Michael	G06Q20/3278	1/1
	B					
	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.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/952,176	Colby, Steven Michael
	Examiner	**Art Unit**
	JAMARA A FRANKLIN	2876

CPC - Searched*		
Symbol	**Date**	**Examiner**
G06K7/10158; G06K7/10316; G06K19/07709; G06K19/07758; G06Q20/227; G06Q20/3278; G06Q20/4012	12/20/2022	JAF

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**
assignee and inventor search	12/20/2022	JAF
considered parent application no. 17/728,412	12/20/2022	JAF
G06K7/10158; G06K7/10316; G06K19/07709; G06K19/07758; G06Q20/227; G06Q20/3278; G06Q20/4012	12/20/2022	JAF
similarity search	12/20/2022	JAF

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**

/JAMARA A FRANKLIN/ Primary Examiner, Art Unit 2876	

SAMSUNG EXHIBIT 1010 Page 107

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/952,176	Colby, Steven Michael
	Examiner	**Art Unit**
	JAMARA A FRANKLIN	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	12/20/2022								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								
	22	✓								
	23	✓								
	24	✓								
	25	✓								
	26	✓								
	27	✓								
	28	✓								
	29	✓								
	30	✓								

Bibliographic Data

Application No: 17/952,176

Foreign Priority claimed: ○ Yes ◉ No

35 USC 119 (a-d) conditions met: ☐ Yes ☑ No ☐ Met After Allowance

Verified and Acknowledged: /JAMARA A FRANKLIN/ (Examiner's Signature) (Initials)

Title: Methods of Using a Cellular Telephone

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
09/23/2022	705	2876	
RULE			

APPLICANTS

INVENTORS

Steven Michael Colby, Verdi, NV, UNITED STATES

CONTINUING DATA

This application is a CON of 17728412 04/25/2022

17728412 is a CON of 17522697 11/09/2021 PAT 11347949

17522697 is a CON of 16186543 11/11/2018 PAT 11170185

16186543 is a CIP of 15418726 01/28/2017 PAT 10503940

15418726 is a CON of 14660825 03/17/2015 PAT 9569777

14660825 is a CIP of 14468110 08/25/2014 PAT 9495852

14660825 is a CIP of 13481104 05/25/2012ABN

14660825 is a CIP of 13084433 04/11/2011ABN

13481104 is a CON of 12777474 05/11/2010ABN

14468110 is a CON of 12577209 10/12/2009 PAT 8816826

12577209 is a CON of 11468026 08/29/2006ABN

13084433 is a CON of 11458620 07/19/2006 PAT 7924156

11458620 is a CIP of 11420721 05/26/2006ABN

11458620 is a CIP of 11382265 05/08/2006ABN

11458620 is a CIP of 11382054 05/08/2006ABN

11458620 is a CIP of 11382264 05/08/2006ABN

11458620 is a CIP of 11382050 05/07/2006ABN

11458620 is a CIP of 11382053 05/07/2006ABN

11458620 is a CIP of 11382052 05/07/2006ABN

11458620 has PRO of 60746636 05/06/2006

11468026 has PRO of 60746636 05/06/2006

11458620 has PRO of 60744154 04/03/2006

11468026 has PRO of 60744154 04/03/2006

11468026 has PRO of 60782068 03/13/2006

11458620 has PRO of 60782068 03/13/2006

11458620 has PRO of 60758751 01/13/2006

11468026 has PRO of 60758751 01/13/2006

11458620 has PRO of 60752933 12/21/2005

11468026 has PRO of 60752933 12/21/2005

11458620 has PRO of 60715641 09/10/2005

11468026 has PRO of 60715641 09/10/2005

11468026 has PRO of 60712308 08/30/2005

11458620 has PRO of 60712308 08/30/2005

11458620 has PRO of 60700884 07/19/2005

11382050 has PRO of 60685331 05/27/2005

11382050 has PRO of 60678428 05/06/2005

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

10/21/2022

**** SMALL ENTITY ****

STATE OR COUNTRY

UNITED STATES

ADDRESS

FILING FEE RECEIVED

$3,430

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L1	17422	(G06K7/10158 OR G06K7/10316 OR G06K19/07709 OR G06K19/07758 OR G06Q20/227 OR G06Q20/3278 OR G06Q20/4012).cpc.	(US-PGPUB; USPAT)	OR	ON	ON	2022/12/19 03:23 PM
L2	7	(colby.in. colby.as.) AND (activating.clm. AND switch.clm.)	(US-PGPUB; USPAT)	OR	ON	ON	2022/12/19 03:32 PM
L3	45	(Artificial Intelligence) Similar to: Unpublished Application # Text: (US-3488114-A OR KR-950006844-A OR US-3591267-A OR DE-4319929-A1 OR GB-2033133-A OR GB-2033134-A OR EP-0572719-A1 OR US-2995313-A OR US-4973988-A OR TW-201202047-A OR US-3359469-A OR US-4408237-A OR DE-4015933-A1 OR CN-109983296-B OR US-20050237510-A1 OR WO-2004090953-A1 OR KR-20050111572-A OR KR-101096479-B1 OR JP-2004311459-A OR JP-4362862-B2 OR EP-1610362-A1 OR EP-1610362-B1 OR TW-I513590-B OR KR-20110128930-A OR JP-5719311-B2 OR JP-S59201039-A OR JP-2012515359-A OR DE-2912548-A1 OR CN-113534394-A OR GB-1499543-A OR EP-0044280-B1 OR US-20160054539-A1 OR JP-6841685-B2 OR CH-637884-A5 OR EP-2605053-A1 OR KR-20180000126-A OR US-20180250966-A1	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO))	OR	ON	ON	2022/12/20 07:58 PM

		OR EP-0401475-A2 OR EP-3545253-B1 OR DE-10018797-B4 OR TW-I405456-B OR DE-2652390-A1 OR DE-3833371-A1 OR KR-101820522-B1 OR EP-3674767-B1 OR JP-6038404-B2 OR DE-602005001533-T2 OR EP-0401475-B1 OR KR-880006675-A OR WO-2012137739-A1).did.					

PE2E SEARCH - Search History (Interference)

There are no Interference searches to show.

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	17952176
Filing Date	2022-09-23
First Named Inventor	Colby
Art Unit	2876
Examiner Name	Jamara Alzaida Franklin
Attorney Docket Number	SMC-83-C12C3

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					

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]
	1							

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]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

	1	"Mobile Credit Card from Barclaycard and Mercury", Smart Card News, June 1994.	
	2	"Lufthansa AirPlus Card for Frequent Flyers", Smart Card News, March 1993, Vol. 2, No. 2.	
	3	"Portugal to Lead Europe with Electronic Purse", Smart Card News, May 1993, Vol. 2, No. 5.	
	4	"Patient Smart Card Trials in Portugal and UK", Smart Card News, May 1994	
	5	"Sun Launches Java Card API for Smart Cards", Smart Card News, November 1996, Vol. 5, No. 11.	
	6	"Social Security Card Pilot in Spain to Prevent Fraud", Smart Card News, November 1994.	
	7	"Russian Banks to Introduce Smart Card Technology", Smart Card News, November 1993.	
	8	"Spanish Banks to Launch Electronic Purse Scheme", Smart Card News, October 1993.	
	9	"British Gas Leads with UK National Network", Smart Card News, September 1992, Vol. 1, No. 1.	
	10	"Bank Passbook and Purse in Indonesia", Smart Card News, September 1993.	
	11	"Mikcon Austria Bid for World Ticket Card", Smart Card News, September 1994.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

	12	"Rabobank Success in Electronic Banking", Smart Card News, February 1993, Vol. 2, No. 2.	
	13	"Emergency Health Card Trials to Start in Ireland", Smart Card News, March 1995.	
	14	Passport Statistics, Travel.State.Gov, hllps://travel.state.gov/contenl/travel/en/passports/afler/passport-statistics.html.	
	15	In the United States Court of Federal Claims, Case 1:16-cv-01647-SGB, Document 68, Filed 8/17/18, 43 pages.	
	16	International Standard ISO/IEC FEDIS 14443-1: Final Draft. Identification cards- Contactless Integrated circuit{s) cards - Proximity Cards Parts 1: Physical characteristics. ISO/IEC 2000, 1/11/2000.	
	17	ISO/IEC JTC1/SC-17. Identification cards- Contactless integrated circuit{s) cards- Proximity cards - Part 2: Radio frequency power and signal interface, 10/8/2003.	
	18	ISO/IEC JTC 1/SC 17. Identification cards m Contactless integrated circuit{s) cards - Proximity cards - Part 3: initialization and anticollision, 7/27/2000.	
	19	ISO/IEC JTC 1/SC 17, Identification cards m Contactless integrated circuit{s) cards - Proximity cards - Part 4: Transmission protocol, 12/4/2000.	
	20	Biometrics Deployment of Machine Readable Travel Documents, ICAO NTWG Biometrics TR v2-0 final TAG 15 7/6/2004.	
	21	Machine Readable Travel Documents. Development of A Logical Data Structure - LOS for Optional Capacity Expansion Technologies, LOS-technical report -Version 1.7 Approved 6/4/2004.	
	22	Machine Readable Travel Documents. Supplement to 6th Edition. Part 1.Doc 9303.Release_ 4.June2006 6/19/2006.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

	23	Machine Readable Travel Documents Technical Report, PKI for Machine Readable Travel Documents offering ICC Read-Only Access. TR-PKI for MRTDs offering ICC Read-Only Access VI. 1. 10/4/2004.	
	24	International Standard ISO/IEC 7816, Information Technology. Identification cards. Integrated circuit{s) cards with contacts.Part 4: Interindustry commands for interchange. 5/18/2001.	
	25	International Standard ISO/IEC 7816, Information Technology. Identification cards. Integrated circuit{s) cards with contacts Part 6: Interindustry data elements. 5/18/2001.	
	26	International Standard ISO/IEC 7816, Information Technology. Identification cards. Integrated circuit{s) cards with contacts Part 8: Security related interindustry commands. 5/18/2001.	
	27	International Standard ISO/IEC 7816, Information Technology_ Identification cards. Integrated circuit{s) cards with contacts Part 9: Additional interindustry commands and security attributes. 5/18/2001.	
	28	International Standard, ISO/IEC 14443-3. Identification Cards Integrated circuit{s) cards with contacts. Part 3: Initialization and anticollision. 7/4/2005.	
	29	International Standard, ISO/IEC 14443-3. Identification Cards Integrated circuit{s) cards with contacts. Proximity cards. Part 4: Transmission Protocol.7/4/2005.	
	30	First DRAFT 15th August 2005, Machine Readable Travel Documents, 8/15/2005.	
	31	International Standard, ISO/IEC 1443-2. Identification cards. Integrated circuit{s) cards with contacts. Proximity Cards. Part 2: Radio frequency power and signal interface. 9/18/2017.	
	32	"BT Tender for Smart Payphones and Cards", Smart Card News, January 1994.	
	33	"Swiss Electronic Purse to go Nationwide in 1995", Smart Card News, July 1993.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

	34	Office Action issued in U.S. Patent Application No. 17/697923, mailed June 8, 2022, 7 pages.	
	35	FINKENZELLER, "RFID Handbook - Fundamentals and Applications in Contactless Smart Cards and Identification", Second Edition, 2003, John Wiley & Sons Ltd.	
	36	RANKI, et al., "Smart Card Handbook", Third Edition, 2003, John Wiley & Sons Ltd.	

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	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

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	/Steve Colby, Reg. No. 50,250/	Date (YYYY-MM-DD)	2022-12-26
Name/Print	Steve Colby	Registration Number	50250

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

Electronic Acknowledgement Receipt

EFS ID:	47273925
Application Number:	17952176
International Application Number:	
Confirmation Number:	8353
Title of Invention:	Methods of Using a Cellular Telephone
First Named Inventor/Applicant Name:	Steven Michael Colby
Customer Number:	43198
Filer:	Steven M. Colby/Susan Stewart
Filer Authorized By:	Steven M. Colby
Attorney Docket Number:	SMC-83-C12C3
Receipt Date:	26-DEC-2022
Filing Date:	23-SEP-2022
Time Stamp:	17:30:53
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	Non Patent Literature	NPL2-1.PDF	884669 d27223a7757a309939bd32b029ed57abd076b43c	no	20

Warnings:

Information:					
2	Non Patent Literature	NPL2-2.PDF	1024554 1cff6cbf206c0affb47d9e56ae07da4570a1044b	no	20
Warnings:					
Information:					
3	Non Patent Literature	NPL2-3.PDF	964451 b1a41c10447771ff307b5f67ac39641ccc6f0f5a	no	20
Warnings:					
Information:					
4	Non Patent Literature	NPL2-4_Patient.PDF	986408 19320a92dfb2eeffa8f3c4f076f35035e7a11869	no	21
Warnings:					
Information:					
5	Non Patent Literature	NPL2-5_Sun_Launch.PDF	1320716 6abbbd44e324c63999098f2d1b10c50c1c8ed772	no	20
Warnings:					
Information:					
6	Non Patent Literature	NPL2-6_SSCard_Spain.PDF	910720 748bda0e357dfa6f2e8b7dc16a5c3e94174dfe04	no	20
Warnings:					
Information:					
7	Non Patent Literature	NPL2-7_Russian_Banks.PDF	826993 37125e1fc8c151ad7a69c030b7b09ee7b158c39d	no	20
Warnings:					
Information:					
8	Non Patent Literature	NPL2-8_Spanish_Banks.PDF	707544 4e1bccda0e88d14d06859d95de2aff491c7aa2ad	no	22
Warnings:					
Information:					

9	Non Patent Literature	NPL2-9_BritishGas.PDF	1106282 76dfdf82f4d396b72a2d9e1050fb120b494107e0	no	20
Warnings:					
Information:					
10	Non Patent Literature	NPL2-10_Bank_Passbook.PDF	670966 bcfa6009b5e0efc73cf7ab60ebc28dad0223056a	no	20
Warnings:					
Information:					
11	Non Patent Literature	NPL2-11_Mikon_Austria.PDF	907215 a63c6098ca4c6f52c2ef8e98b8e02f478dba6ecb	no	20
Warnings:					
Information:					
12	Non Patent Literature	NPL2-12_Rabobank.PDF	1014896 1bbb3709a60ae531275caf43cd33e6a324846989	no	20
Warnings:					
Information:					
13	Non Patent Literature	NPL2-13_Emergency.PDF	746354 7c4eda5b8c58bee806c17f56b5044667dfd7ed14	no	19
Warnings:					
Information:					
14	Non Patent Literature	NPL2-14_Passport_Stats.PDF	52258 e8c8dfeeb8ccd23af5df382e9220af9fb8e149ba	no	3
Warnings:					
Information:					
15	Non Patent Literature	NPL2-15_USCFC2018.PDF	689130 ffc7f135ab35df638b898f7e2dd6e8e61a93b93b	no	43
Warnings:					
Information:					

16	Non Patent Literature	NPL2-16_ISO_IEC_FEDIS.PDF	219895 84d5312a02a4497f260cc9e9701d1a59db043890	no	12
Warnings:					
Information:					
17	Non Patent Literature	NPL2-17_ISO_IEC_JTC1Pt2.PDF	402795 77fbb35473ba2a04f6b517104ac180d528874640	no	19
Warnings:					
Information:					
18	Non Patent Literature	NPL2-18_ISO_IEC_Pt3.PDF	1332372 44594132ae12c3f1461417e1cd1d7d889d9aae31	no	54
Warnings:					
Information:					
19	Non Patent Literature	NPL2-19_ISO_IEC_pt4.PDF	790910 ee2a525d6f3bff0dcf5f983ac2127b7456296ea8	no	42
Warnings:					
Information:					
20	Non Patent Literature	NPL2-20_Biometrics_Deploy.PDF	1782414 2af4f255a1c896b5546fa54c9cda37b34711c8e0	no	60
Warnings:					
Information:					
21	Non Patent Literature	NPL2-21_Mach_Readable.PDF	3087947 4896b626875ec4b4b4e65d04621019c7c322b7d6	no	92
Warnings:					
Information:					
22	Non Patent Literature	NPL2-22_MR_Travel_Docs.PDF	1255976 3d7fde504d022c97cbb44b2ea075a2a6d5b7c516	no	40
Warnings:					
Information:					

23	Non Patent Literature	NPL2-23_MR_TravelDocs_2004.PDF	1975710 41c18d4edf4bc4052c30dc32deb35d6d6e6f1ac9	no	57
Warnings:					
Information:					
24	Non Patent Literature	NPL2-24_ISO_IEC_7816pt4.PDF	3039236 3a7a9b75ecc36ab762eef5dd0e3cb10d45d4084f	no	51
Warnings:					
Information:					
25	Non Patent Literature	NPL2-25_ISO_IEC_7816pt6.PDF	1092868 864a4ab78049dafc55a5eb0d6b2884f4cfd4d830	no	21
Warnings:					
Information:					
26	Non Patent Literature	NPL2-26_ISO_IEC_7816pt8.PDF	1657614 24a2eef6c07e96037bde5d23a7db87888ecbf87e	no	32
Warnings:					
Information:					
27	Non Patent Literature	NPL2-27_ISO_IEC_7816_pt9.PDF	1778062 b165e97acf8e2289c4299dbb489b96d203fdfd6c	no	40
Warnings:					
Information:					
28	Non Patent Literature	NPL2-28_ISO_IEC_14443-3pt3.PDF	1404039 be0d5e126deb48f55b682d87f1dda5a69b9df964	no	58
Warnings:					
Information:					
29	Non Patent Literature	NPL2-29_ISO_IEC_14443-3pt4.PDF	922724 9a19b8314646e6769a61103096050b8fb8243fff	no	44
Warnings:					
Information:					

30	Non Patent Literature	NPL2-30_FirstDraft.PDF	4614884 a2b5d5b8e0e53036a6157744322f3ed9fc5639f9	no	126
Warnings:					
Information:					
31	Non Patent Literature	NPL2-31_ISO_IEC_1443-2pt2.PDF	414022 05092f0531d2b7144985f630a3dd68ea0a35014d	no	18
Warnings:					
Information:					
32	Non Patent Literature	NPL2-32_BT.PDF	812879 2fee80c830aa620f6c4c92c2d820367e46cab1d5	no	20
Warnings:					
Information:					
33	Non Patent Literature	NPL2-33_Swiss.PDF	994861 f5ef91458b642cc5f5130a1619fe3e11c91f2a72	no	27
Warnings:					
Information:					
34	Non Patent Literature	NPL2-34_Office_Action_June2022.pdf	206640 c67bdf6ccb78eed35645f1d1b74cd9db2693ca66	no	7
Warnings:					
Information:					
35	Non Patent Literature	NPL2-35pt1_Finkenzeller.PDF	17395931 fe378afe5999bc0808d80e2c5a79be74742ccd7b	no	109
Warnings:					
Information:					
36	Non Patent Literature	NPL2-35pt2_Finkenzeller.PDF	16979560 a278e3da6292f9b56dd68b9a8722c518632d586d	no	108
Warnings:					
Information:					

37	Non Patent Literature	NPL2-35pt3_Finkenzeller.PDF	17889230 b5a396579498a725119bcda0ca26eaa8897f3665	no	109
Warnings:					
Information:					
38	Non Patent Literature	NPL2-35pt4_Finkenzeller.PDF	18780363 4a9b95f40215159aad61a2c21903b5b15bd17718	no	108
Warnings:					
Information:					
39	Non Patent Literature	NPL2-36pt1_Ranki.PDF	22953727 3d84050dc9909e306ba3a77f21df5f0f48cb7c41	no	141
Warnings:					
Information:					
40	Non Patent Literature	NPL2-36pt2_Ranki.PDF	23331149 9c47938906af8dda1328c63830a2aea0a2545fc8	no	140
Warnings:					
Information:					
41	Non Patent Literature	NPL2-36pt3_Ranki.PDF	24366668 cde76cb61d0a07f91b07249e5df9d590227e9cb2	no	142
Warnings:					
Information:					
42	Non Patent Literature	NPL2-36pt4_Ranki.PDF	23485861 1a74576a5b78d3a99a6cbb08ec2cc8b05d7649dd	no	141
Warnings:					
Information:					
43	Non Patent Literature	NPL2-36pt5a_Ranki.PDF	12930439 77b7c8afd8d99e61d21b2ac03dc05a1a3d0f9793	no	70
Warnings:					
Information:					

44	Non Patent Literature	NPL2-36pt5b_Ranki.PDF	14220469 494b580cde7f4f2de668194cf276112c9add257a	no	71
Warnings:					
Information:					
45	Non Patent Literature	NPL2-36pt6_Ranki.PDF	24323453 39d312cefd5a1e88c9a5446e77516de861d50468	no	141
Warnings:					
Information:					
46	Non Patent Literature	NPL2-36pt7_Ranki.PDF	21923223 6ad474893d6f74236fe1d0ea47e807a941253368	no	140
Warnings:					
Information:					
47	Non Patent Literature	NPL2-36pt8_Ranki.PDF	19262971 246d7fcbc4789bcca7399557811ceb0027e5d1ca	no	137
Warnings:					
Information:					
48	Information Disclosure Statement (IDS) Form (SB08)	IDS_C12C3_SB08_Pt2.pdf	1037148 61dc227c9f500bd660111ccf51c6742fde3823e7	no	7
Warnings:					
Information:					
A U.S. Patent Number Citation or a U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form for autoloading of data into USPTO systems. You may remove the form to add the required data in order to correct the Informational Message if you are citing U.S. References. If you chose not to include U.S. References, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.					
			Total Files Size (in bytes):	299479196	

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/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	17952176
Filing Date	2022-09-23
First Named Inventor	Colby
Art Unit	2876
Examiner Name	Jamara Alzaida Franklin
Attorney Docket Number	SMC-83-C12C3

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	5528222	A	1996-06-18	Moskowitz et al.	
	2	6111506	A	2000-08-29	Yap et al.	
	3	6785405	B2	2004-08-31	Tuttle et al.	
	4	7243840	B2	2007-07-17	Bason et al.	
	5	7837119	B2	2010-11-23	Graf et al.	
	6	4774148	A	1988-09-27	Goto	
	7	7336184	B2	2008-02-23	Smith et al.	
	8	6863220	B2	2005-03-08	Selker	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

	9	6972662	B1	2005-12-06	Ohkawa et al.	
	10	4068232	A	1978-01-10	Meyers et al.	
	11	4880683	A	1989-11-14	Stow	
	12	7083083	B2	2006-08-01	Droz	
	13	6041412	A	2000-03-21	Timson et al.	
	14	6121544	A	2000-09-19	Petsinger	
	15	6424029	B1	2002-07-23	Giesler	
	16	5869412	A	1999-02-09	Yenni et al.	
	17	6135503	A	2000-10-24	Lob et al.	
	18	7040981	B2	2006-05-09	Iliescu et al.	
	19	6213702	B1	2001-04-10	Wesselink	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

	20	7375631	B2	2008-05-20	Moskowitz et al.	
	21	5815190	A	1998-09-29	Ohshima	
	22	5627544	A	1997-05-06	Snodgrass	
	23	7246754	B2	2007-07-24	Siuta et al.	
	24	6344155	B1	2002-02-05	Kitahara et al.	
	25	7336184	B2	2008-02-26	Smith et al.	
	26	6863220	B2	2005-03-08	Selker	
	27	5606313	A	1997-02-25	Allen et al.	
	28	5815190	A	1998-09-29	Ohshima et al.	
	29	6262364	A	2001-07-17	Yoshikawa et al.	
	30	6097292	A	2000-08-01	Kelly et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

	31	7701408	B2	2010-04-20	Bombay et al.	
	32	5963144	A	1999-10-05	Kruest	
	33	6008727	A	1999-12-28	Want et al.	
	34	6025783	A	2000-02-15	Steffens, Jr.	
	35	6380845	B2	2002-04-30	Tuttle	
	36	8487828	B2	2013-07-16	Bombay et al.	
	37	7479882	B2	2009-01-20	Mahaffey	
	38	7924156	B2	2011-04-12	Colby	
	39	7719425	B2	2010-05-18	Colby	
	40	9524485	B2	2016-12-20	Colby	
	41	9569777	B2	2017-02-14	Colby	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

	42	8744359	B2	2014-06-03	Ramsten et al.	
	43	7042332	B2	2006-05-09	Takamura et al.	
	44	7466216	B2	2008-12-16	Kawamura et al.	
	45	7346061	B2	2008-03-18	Takayama et al.	
	46	6859650	B1	2005-02-22	Ritter	

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	20060065714	A1	2006-03-30	Jesme	
	2	20060044206	A1	2006-03-02	Moskowitz et al.	
	3	20060261171	A1	2006-11-23	Buursma et al.	
	4	20050188167	A1	2005-08-25	Squibbs et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

	5	20050141256	A1	2005-06-30	Yamakazi et al.	
	6	20050140495	A1	2005-06-30	Yamakazi et al.	
	7	20040064698	A1	2004-04-01	Zhang	
	8	20050240778	A1	2005-10-27	Saito	
	9	20020108704	A1	2002-08-15	Umezawa et al.	
	10	20030168514	A1	2003-09-11	Rancien et al.	
	11	20030057286	A1	2003-03-27	Yamagishi et al.	

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	0383059	EP	A1	1990-08-22	Dordevic		
	2	2397272	GB	A	2004-07-21	Lawrence et al.		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

	3	2004/038644	WO	A2	2004-05-06	Powell et al.		
	4	1075781	EP	B1	2001-02-14	Yenni et al.		
	5	11-348471	JP	A	1999-12-12	Funaki et al.		

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	SCHNEE, Thomas, "In Hanau, the portable bus ticket plays at the right price", Berlin, 01nel.com, 5/2/2005.	
	2	DELEURENCE, Guillaume, "Caen, the city where you pay and get information by taking out your mobile phone", J1nel.com, 10/20/2005.	
	3	Microsoft NFC Blog	
	4	"Identification cards- Contaclless integrated circuit{s) cards- proximity cards Part 2: Radio Frequency power and signal interface" - ISO/IEC 14443-2, July 1, 2001.	
	5	"Technical Report - PKI for Machine Readable Travel Documents offering ICC Read-Only access", ICAO PKI, October 1, 2004.	
	6	"Identification cards- Contactless integrated circuit{s) cards- proximity cards Part 3: Initialization and anticollision" - ISO/IEC 14443-3, February 1, 2001.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

	7	ELLIS, "Use of Contaclless Integrated Circuits in Machine Readable Travel Documents". ICAO/NTWG, April 16, 2003.	
	8	"Technical Report - Development and Specification of Globally Interoperable Biometric Standards for Machine Assisted Identity Confirmation using Machine Readable Travel Documents", ICAO/NTWG, version 2.0, May 21, 2004.	
	9	FINKENZELLER, "RFID Handbook - Fundamentals and Applications in Contactless Smart Cards and Identification", Second Edition, 2003, John Wiley & Sons Lid.	
	10	JUELS, et al., "Squealing Euros: Privacy Protection in RFID-Enabled Banknotes", Conference Paper in Lecture Notes in Computer Science, January 27-30 2003.	
	11	mifare Data Sheet, Functional Specification, Revision 3.1, Phillips Semiconductors, October 2002.	
	12	"Machine Readable Passports, Specifications for Discretionary Expansion of Data Storage Capacity and Globally nteroperable Biometric Identification", ICAO, Second Draft, Part 1 Volume 2, November 18, 2004.	
	13	"Technical Report - Development of a Logical Data Structure - LOS for Optional Capacity Expansion Technologies", CAO, Revision 1.7, May 18, 2004.	
	14	RANKI, et al., "Smart Card Handbook", Third Edition, 2003, John Wiley & Sons Lid.	
	15	"Annex I - Use of Contactless Integrated Circuits in Machine Readable Travel Documents offering ICC read-only access", ICAO, Version 1.1, October 1, 2004.	
	16	Invalidity of U.S. Patent No. 7,924,156 in view of Mi Fare® Functional Product Specification, Revision 3.1, Published October 2002.	
	17	Invalidity of U.S. Patent No. 7,924,156 in view of RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, Second Edition ("RFID Handbook"), 2003.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

	18	Invalidity of U.S. Patent No. 7,924,156 in view of Smart Card Handbook, Third Edition ("Smart Card Handbook"), 2003.	
	19	Invalidity of U.S. Patent No. 7,924,156 in view of "Squealing Euros: Privacy Protection in RFID-Enabled Banknotes" ("Juels"), published January 27-30, 2003.	
	20	Invalidity of U.S. Patent No. 7,924,156 in view of Juels et al., Security and Privacy Issues in E-Passports ("Juels-2"), No later than April 26, 2005.	
	21	Invalidity of U.S. Patent No. 7,924,156 in view of Knospe - RFID Security (2004) ("Knospe")	
	22	Invalidity of U.S. Patent No. 7,924,156 in view of Gao et al., An Approach to Security and Privacy of RFID System for Supply Chain ("Gao"), September 2004.	
	23	Invalidity of U.S. Patent No. 7,924,156 in view of Weis - Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems (2004).	
	24	Invalidity of U.S. Patent No. 7,924,156 in view of EPC Global Specification for RFID Protocols ("EPC Global"), January 2005.	
	25	Invalidity of U.S. Patent No. 7,924,156 in view of ICAO 2003 "Use of Contactless Integrated Circuits in MRTDs" APRIL J003 {"ICAO 2003"), April 16, 2003.	
	26	Invalidity of U.S. Patent No. 7,924,156 in view of Morgantown ePassports Interoperability Test Sessions, July 27-29, J004.	
	27	Invalidity of U.S. Patent No. 7,719,425 in view of "ANNEX I - Use of Contaclless ICs in MRTDs" {"Annex I"), May 5, 2004.	
	28	KINNEGING, "Technical Report - PKI for Machine Readable Travel Documents Offering ICC Read-Only Access" {Version 1.1, October 1, 2004). {"ICAO PKI").	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

	29	Technical Report - PKI for Machine Readable Travel Documents Offering ICC Read-Only Access {Version V0.43, April 2, 2004).	
	30	ISO/IEC 14443-1, Identification cards - Contactless integrated circuit{s) cards - Proximity cards Part 1: Physical Characteristics, April 15, 2000.	
	31	ISO/IEC 14443-2, Identification cards - Contactless integrated circuit{s) cards - Proximity cards Part 2: Radio frequency power and signal interface, July 1, 2001.	
	32	ISO/IEC 14443-3, Identification cards - Contactless integrated circuit{s) cards - Proximity cards Part 3: Initialization and anticollision, February 1, 2001.	
	33	TECHNICAL REPORT: DEVELOPMENT OF A LOGICAL DATA STRUCTURE - LDS For OPTIONAL CAPACITY EXPANSION TECHNOLOGIES, ICAO, Revision 1.7, May 18, 2004.	
	34	Technical Report: Development and Specification of Globally Interoperable Biometric Standards for Machine Assisted Identity Confirmation using Machine Readable Travel Documents, ICAO-NTWG, Version 2.0, May 21, 2004.	
	35	Specifications for discretionary expansion of Data Storage Capacity and Globally Interoperable Biometric Identification, CAO, Part 1, Volume 2, November 18, 2004.	
	36	Securing (biometric) data stored in a contaclless chip, ICAO-NTWG, Version 0.7, September 15, 2003.	
	37	In the United States Court of Federal Claims, Case 16-cv-01647-RTH, Defentants' February 19, 2021 PRCFC 6-7 Invalidity Contentions, Filed 2/19/21, 105 pages.	
	38	KUKLINSKI, "Automated Authentication of Current Identity", 2004 IEEE Conference on Technologies for Homeland Security, Cambridge, MA, April 21 22, 2004	
	39	'Denmark to Launch First Country-wide Scheme", Smart Card News Ltd., Brighton England, 1992.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

	40	"Post Office Plans £19.5m Terminal Network in UK", Smart Card News, April 1993, Vol. 2, No. 4.	
	41	"P&O Passengers Enjoy Cashless Cruising", Smart Card News, April 1994.	
	42	"Smart Card Payphones on Channel Tunnel Trains", Smart Card News, August 1994.	
	43	"Japan and USA to Push Smart Card Technology", Smart Card News, August 1993.	
	44	"NatWest Launch Mondex Global Electronic Cash", Smart Card News, December 1993.	
	45	"British Govt Launches Smart Card Initiative", Smart Card News, December 1997, Vol. 6, No. 12.	
	46	"Gaudi Multiservice Smart Card Trials in Dublin", Smart Card News, February 1994.	
	47	"Austria Starts Trials for National Electronic Purse", Smart Card News, February 1995.	
	48	"Smart Card Being Used in Swiss Ski Resorts", Smart Card News, January 1993, Vol. 2, No. 1.	
	49	"Shell Loyalty Scheme Launched in Scotland", Smart Card News, July 1994.	
	50	"Major Stored Value Card Plan in Australia", Smart Card News, June 1993.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

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	17952176
	Filing Date	2022-09-23
	First Named Inventor	Colby
	Art Unit	2876
	Examiner Name	Jamara Alzaida Franklin
	Attorney Docket Number	SMC-83-C12C3

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	/Steve Colby, Reg. No. 50,250/	Date (YYYY-MM-DD)	2022-12-26
Name/Print	Steve Colby	Registration Number	50250

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.

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

(11) Publication number: **0 383 059 A1**

(12) **EUROPEAN PATENT APPLICATION**

(21) Application number: **90101342.5**

(51) Int. Cl.[5]: **D03D 15/00, G21F 3/02**

(22) Date of filing: **23.01.90**

(30) Priority: **22.06.89 DE 8907655 U**
15.02.89 YU 336/89

(43) Date of publication of application:
22.08.90 Bulletin 90/34

(84) Designated Contracting States:
GR

(71) Applicant: **FINEX HANDELS-GMBH**
Erzgiessereistrasse 24
D-8000 München 2(DE)

(72) Inventor: **Dordevic, Zoran, Prof.**
Ul. Sv. Markovica 26
YU-11000 Beograd(YU)

(74) Representative: **Patentanwälte Viering & Jentschura**
Steinsdorfstrasse 6
D-8000 München 22(DE)

(54) **Textile fabric shielding electromagnetic radiation, and clothing made thereof.**

(57) Textile fabric shielding electromagnetic radiation, and clothing made thereof. The textile fabric is made of threads spun of textile fibers, containing cotton, and of steel fibers having a diameter of 6 to 10 µm. The number of mixed yarn threads in warp direction and in weft direction each is 18 to 20 threads per cm, and the yarn fineness of the textile fabric is especially 38 to 40 tex. The textile fabric guarantees a shielding of 20 to 40 dB against electromagnetic radiation at a frequency of 10 GHz. The fabric has the quality of usual clothing, and the clothing thereof is designed with respect to proportions, seams, fasteners, and other special features in a manner such that especially people wearing pacemakers, or hospital and radar personnel, are protected against electromagnetic radiation.

EP 0 383 059 A1

Textile fabric shielding electromagnetic radiation, and clothing made thereof

The invention concerns a textile fabric shielding electromagnetic radiation, and clothing made thereof.

From DE-A-29 23 286, a textile fabric is known whose orthogonally crossing warp threads and weft threads are made of spun mixed yarn of steel fibres of stainless steel and of textile fibres. The steel fibres may be extremely thin, less than 25 micrometers in diameter, for example. According to this document, the mesh is proposed to measure at least 0.5 cm^2. This textile fabric is designed for carpet floors or working garments, for example, in order to obtain an antistatic network and thus prevent electrostatic charging.

However, such a fabric does not provide effective protection against microwaves and other electromagnetic radiation, to which in particular the hospital personnel, for example, when operating electromedical equipment such as X-ray, ECG and EEG apparatus and the like, and the personnel for operating radar installations, for example, are exposed. In the course of electronization, also heart pacemakers are miniaturized and refined, but at the same time rendered susceptible to electromagnetic radiation interference such as occurrs in everyday life due to, for example, broadcast and TV stations arnd various electrical apparatus, electric motors, electrical and electronic ignition control devices in motor vehicles, shavers, electrical household appliances, and electronic computer installations and the like. Modern heart pacemakers are designed so as to take over the pacemaker function only when the normal heart rhythm is disturbed, but not to interfere when the heart rhythm is normal. The occurrence of electromagnetic radiation, however, may result in a disturhance of the heart pacemaker control such that incorrect information on the current heart activity may be received and the control may fail in that case.

While it is true that clothing which shields against electromagnetic radiation exist, such as the vest known from US-A-4 196 355. However, this vest, due to its construction and weight, is much too heavy and uncomfortable to be suitable for normal applications.

According to the invention, a textile fabric and clothing made thereof are provided, which are effectively suitable for shielding against electromagnetic radiation, in particular in the microwave range, and, at the same time, do not restrict the wearing comfort of usual clothing.

The invention is based on the perception that total shielding against electromagnetic radiation is not necessary, since radiation below certain intensities can be accepted without health impairment, and that this provides the possibility of achieving sufficient shielding by means of clothing even without restriction on the wearing comfort.

For shielding against electromagnetic radiation, the invention provides a textile fabric whose orthogonally crossing warp threads and weft threads are made of spun mixed yarn of steel fibers of stainless steel and of textile fibers. To this end, the textile fabric has the quality of fabrics for usual clothing, wherein the textile fibers comprise cotton fibers and are twined with the steel fibers which measure 6 to 10 micrometers in diameter and constitute a content of 10 to 15 % per weight of the mixed yarn, the distribution of the warp threads and the weft threads in the fabric and the composition of the warp threads and the weft threads being substantially the same, the number of mixed yarn threads in warp direction and in weft direction each is 18 to 20 threads per cm, and the yarn fineness of the textile fabric is in the range of 30 to 50 tex (g per km), especially of 38 to 40 tex, such that a shielding by 20 to 40 dB against electromagnetic radiation at a frequency of 10 GHz is established by the fabric.

Owing to the content and fineness of steel fibers suggested in accordance with the invention, a textile fabric suitable for effective shielding against excessive electromagnetic microwave radiation can be obtained in a clothing fabric quality, which textile fabric is not too stiff. Hence, clothing can be made which is comparable to clothing without steel fibers. For the shielding effect, it is essential that the steel fibers and the textile fibers are spun and twined with each other in a manner such that a substantial part of the steel fibers is exposed on the exterior surface of the mixed yarn and sufficient mutual electrical contact of the fibers is achieved in the warp and weft threads at the crossings of the fabric to form a Faraday cage. The average number of the steelfibers in the yarn cross-section is preferably 10 to 15.

Preferably, the thickness of the steel fibers measures 8 micrometers, and the content of the steel fibers in the mixed yarn is preferably 13,5 % per weight. The length of the steel fibers is preferably in the range of the length of the cotton fibers and, hence, measures 3 to 10 centimeters. Although it is further possible to provide a mixture of cotton fibers and polyamide fibers, it is preferred to provide textile fibers exclusively of cotton. Cotton is capable of absorbing moisture and improves the electrical conductibility with increasing moisture absorption.

Although a twined one-thread yarn, i.e., a yarn only single-twined, may be used, it is preferred to

SAMSUNG EXHIBIT 1010, Page 144

use a mixed yarn made of double-twined mixed yarn threads, each of which is made of textile fibers and steel fibers in a twined manner, wherein the single threads have a yarn fineness of 16 to 20 tex and a degree of turns of 550 to 650 turns, especially Z-turns, per m, and wherein the degree of turns of the double-threads is 400 to 480 turns, especially Z-turns, per m.

The textile fabric according to the invention is light (the weight of the textile fabric is preferable in the region of 160 g per m^2) and permeable to air and washable like other cloths without impairment of the shielding effect against electromagnetic radiation as would be the case if there were no discrete steel fibers but, instead, for example, a metal coating of the textile fibers. Moreover, the textile fabric according to the invention may be dyed such that pleasing and fashionable articles of clothing can be made of it.

A textile fabric according to the invention having been proved and being excellently effective to shield heart pacemaker against microwave radiation was made of pure cotton with spun with steel fibers. The warp threads and weft threads were made of double-twined yarn of a fineness of R 38 to 40 tex made of single-threads of a fineness of R 16 to 18 tex. The degree of turns of the single threads was 590 to 640 Z per m and that of the Yarn was 420 to 440 Z per m. The content of steel fibers spun into the single-threads was about 13,5 % per weight of the mixed yarn. The thread density of the textile fabric was 18 to 20 threads per cm, each, in warp direction and in weft direction and the average weigth of the textile fabric was 160 g per m^2. The textile fabric had an elongation of 9 to 14 % at a breaking force of 638 to 672 N.

The clothing according to the invention is completely or partly made of a textile fabric according to the invention. This textile fabric may completely form the clothing or may be provided as its interior lining. It is also possible to line the textile fabric itself with a lining of different textile material. For the manufacture of this textile fabric, usual pieces of fabric are cut out which are sewed together along joint seams. According to the invention, it is essential that the textile fabric is made of the above-presented textile/steel-fiber fabric according to the invention and covers at least the upper part of the body and the hip area of the person wearing the clothing as well as at least the person's upper arms approximately to the elbows. To avoid interruption of the shielding effect in the area of the joint seams, the joint seams should be turned up into each other and sewed together by at least two seams with a sewing yarn that is also a textile-fiber/steel-fiber mixed yarn of the kind according to the invention. However, the content of steel fibers in the sewing yarn may possibly be greater than the content in the threads of the textile fabric. All fasteners of the clothing, such as zip and button fasteners, should be free of metal and be underlayed with an interior border band or flap made of the textile-fiber/steel-fiber fabric according to the invention and provide an overlap breadth of at least 5 and preferably 7 centimeters. If pockets are provided in the textile fabric, these pockets should not be inserted into but put on the fabric, in order to avoid interruptions of the shielding effect.

In a preferred embodiment of a clothing according to the invention, the clothing is in the form of a shirt or T-shirt which has at least elbow-length sleeves, covers the hip area of the person wearing the shirt and is provided with a closable neckline that, even when not closed, is covered by an interior flap made of the textile-fiber/steel-fiber fabric according to the invention. As proven by numerous experiments, such a clothing is most suitable for wearers of heart pacemakers to attain an effective shielding of the heart pacemaker against electromagnetic radiation disturbances and, at the same time, achieving the wearing comfort of other shirts or T-shirts. Owing to the invention, shirts or T-shirts of this kind may be manufactured in such a way that they look like other shirts or T-shirts and, hence, the fact that a person needs a heart pacemaker is not discernible from this kind of clothing.

In another preferred embodiment, clothing according to the invention suitable for the personnel of radar installations takes the shape of an overall, in which the textile-fiber/steel-fiber fabric according to the invention covers the upper part of the body as well as at least the upper arms and the hip area, at least down to the knees.

As protective clothing for hospital staff against the influence of electromagnetic radiation emitted by electromedical apparatus, two-piece clothing consisting of a jacket or blouse and a pair of trousers is suggested, wherein the pair of trousers is overlapped by the jacket or blouse by at least 10 centimeters and the jacket or blouse in its chest area has overlapping parts of textile-fiber/steel-fiber fabric held together by Velcro-type fasteners. Since clothing according to the invention is made of comfortable textile material, it can be worn completely closed, while the Velcro-type fasteners prevent the jacket or blouse from being worn open. In this arrangement, one of the overlapping parts of textile fabric preferably extends to one shoulder of the wearing person, and the other part of textile fabric extends at least to the middle of the person's body. The waist measurement of the trousers of this clothing is preferably also adjustable by means of Velcro-type fasteners. In such clothing according to the invention, an interior lining may be formed of the textile-fiber/ steel-fiber fabric according to the invention, while the exterior side of the clothing

SAMSUNG EXHIBIT 1010, Page 145

may, for example, made of light cotton cloth of a quality usual for hospital clothing.

When the clothing according to the invention is embodied by an overall or two-piece suit, a stand-up collar containing textile fabric material according to the invention is preferably additionally provided.

The invention will now be explained with regard to clothing according to the invention and depicted in the drawings. In the drawing:

Fig. 1 illustrates clothing according to the invention in the form of a T-shirt or shirt,

Fig. 2 illustrates clothing according to the invention in the form of an overall,

Figs. 3 to 5 illustrates clothing according to the invention in the form of a two-piece suit from the front, lateral and rear sides,

Figs. 6 and 7 illustrate front and side views of the jacket of the clothing according to Figures 3 to 5,

Figs. 8 and 9 illustrate front and side views of pair of trousers of the clothing according to Figures 3 to 5, and

Fig. 10 illustrates the design of the joint seams of the clothing according to Figures 3 to 9.

The T-shirt or shirt according to Fig.1 is provided for persons wearing a heart pacemaker and is designed to shield the heart pacemaker against electromagnetic radiation, especially in the microwave range. For this purpose, the T-shirt is made of the fabric described in detail above which is woven from a mixed yarn of cotton and steel fibers intertwined with each other. The T-shirt completely covers the upper part of the body of the wearer, and clearly extends with its lower rim 6 beyond the hip area of the wearer. The neckline 2 of the T-shirt equipped with a folded collar 1 can be closed by means of a zip fastener 3 of plastic material, the zip fastener being underlayed with an interior flap 4 completely covering the neckline 2 even when the zip fastener 3 is completely open. The interior flap 4 is made of the same textile fabric material as the other parts of the T-shirt, whose sleeves 5 are elbow-length so that no detrimental radiation can intrude laterally from the sleeves 5, either. These sleeves 5 should be at least 20 centimeters long.

The overall according to Fig.2 may, for example, be used as working clothing for radar personnel and is also made of the textile fabric parts according to the invention. The overall can be closed up to the upper rim of the stand-up collar 7 by means of the zip fastener 3, is also made of plastic material, and is underlayed over its entire length with an interior border band (not shown) which is at least 7 centimeters broad and made of the textile fabric material. The pockets 10 are put on the textile fabric material and sewed to it. These pockets may be made of a different textile cloth.

The two-piece protective suit according to Figures 3 to 9 is provided as protective clothing for hospital personnel exposed to microwave radiation arising from electromedical apparatus. The jacket, as well as the trousers of this protective suit, are made of an outer cloth such as light cotton fabric material developing no protective effect, and of a lining made of the textile fabric material according to the invention. This lining extends over the entire clothing. The front part of the jacket has a widened outer portion 14 extending up to one shoulder and an inner portion 13 extending with its interior border 17 to the middle of the chest. The jacket is closed by means of Velcro-type fastener strips 18 when laying together the outer portion 14 on the inner portion 13. The jacket 15 is provided with a stand-up collar 7 and elbow-length sleeves 5.

The pair of trousers 16 can be closed in the front by means of a zip fastener 3 which is underlayed with a particularly wide interior border band 21 of a width of at least 5 centimeters. The waist measurement of the trousers is adjustable by means of Velcro-type fastener strips 18. In addition, the trousers have put-on pockets 10.

The respective clothing according to Figs. 1 to 9 are tailored of fabric pieces which are sewed together along joint seams 19. As can be seen from Fig.10, the joint seams 19 are turned up into each other and sewed together by at least two seams 20.

Claims

1. Textile fabric whose orthogonally crossing warp threads and weft threads are made of spun mixed yarn of steel fibers of stainless steel and of textile fibers, characterized in that the textile fabric has the quality of fabrics for usual clothing, wherein the textile fibers comprise cotton fibers and are twined with the steel fibers which measure 6 to 10 micrometers in diameter and constitute a content of 10 to 15 % per weight of the mixed yarn, the distribution of the warp threads and the weft threads in the fabric and the composition of the warp threads and the weft threads being substantially the same, the number of mixed yarn threads in warp direction and in weft direction each is 18 to 20 threads per cm, and the yarn fineness of the textile fabric is in the range of 30 to 50 tex, especially of 38 to 40 tex, such that a shielding by 20 to 40 dB against electromagnetic radiation at a frequency of 10 GHz is established by the fabric.

2. Textile fabric according to claim 1, characterized in that the mixed yarn is made of double-twined mixed yarn threads each of which is made of textile fibers and steel fibers in a twined manner, wherein the single threads have a yarn fineness of 16 to 20 tex and a degree of turns of 550 to 650

SAMSUNG EXHIBIT 1010, Page 146

turns, especially Z-turns, per m, and wherein the degree of turns of the double-threads is 400 to 480 turns, especially Z-turns, per m.

3. Textile fahric according to claim 1, characterized in that the fiber thickness of the steel fibers measures 8 micrometers, and the content of the steel fibers in the mixed yarn is 13,5 %.

4. Textile fabric according to claim 1, characterized in that the length of the steel fibers is 3 to 10 centimeters.

5. Textile fabric according to claim 1, characterized in that the textile fibers are made only of cotton.

6. Textile fabric according to claim 1, characterized in that the weight of the textile fabric is 130 to 190 g per m^2, preferably about 160 g per m^2.

7. Clothing completely or partly made of one piece of textile fabric, the clothing covering at least the upper part of the body and the hip area of the wearer, and further comprising sleeves, the piece of textile fabric conprising fabric parts sewed together along joint seams and being adapted to be opened and closed at least in the neck-chest area, characterized in that the textile fabric has the features of any of the claims 1 to 6, the sleeves (5) are at least elbow-length, the joint seams (19) are turned up into each other and are sewed together by at least two seams (20) of sewing yarn consisting of the mixed yarn, and the fastener (3, 18) is free of metal and underlayed with an interior border band (21) or flap (4) of the textile fabric and of a breadth of at least 5 centimeters.

8. Clothing according to claim 7, characterized in that the textile fabric provided with pockets (10) made of a textile sewed onto the textile fabric made of steel fibers and textile fibers.

9. Clothing according to claim 7, characterized in that it is embodied by a T-shirt having elbow-length sleeves (5) and is made of steel fibers and textile fibers.

10. Clothing according to claim 7, characterized in that it is a one-piece overall having a stand-up collar (7), wherein the textile fabric covers the legs of the wearer at least down to the knees.

11. Clothing according to claim 11, characterized in that it is made of a jacket (15) or blouse and a pair of trousers (16), wherein the pair of trousers (16) are overlapped by the jacket (15) or blouse, respectively, by at least 10 centimeters, and the jacket (15) or blouse, respectively, has textile fabric parts (13, 14) overlapping each other and being held together by Velcro-type fasteners (18) connecting the textile fabric parts (13, 14) with each other.

12. Clothing according to claim 11, characterized in that one of the overlapping textile fabric parts (13 or 14) extends to one shoulder of the wearer, and the other textile fabric part extends at least so far that its interior border band (17) extends to the middle of the body when the jacket (15) is closed.

13. Clothing according to claim 11, characterized in that adjustability of the waist measurement of the trousers (16) is provided by means of Velcro-type fasteners (18) made of plastic material.

14. Clothing according to claim 7, characterized in that the jacket (15) or blouse, respectively, has a stand-up collar (17) comprising the fabric made of steel fibers and textile fibers.

SAMSUNG EXHIBIT 1010, Page 147

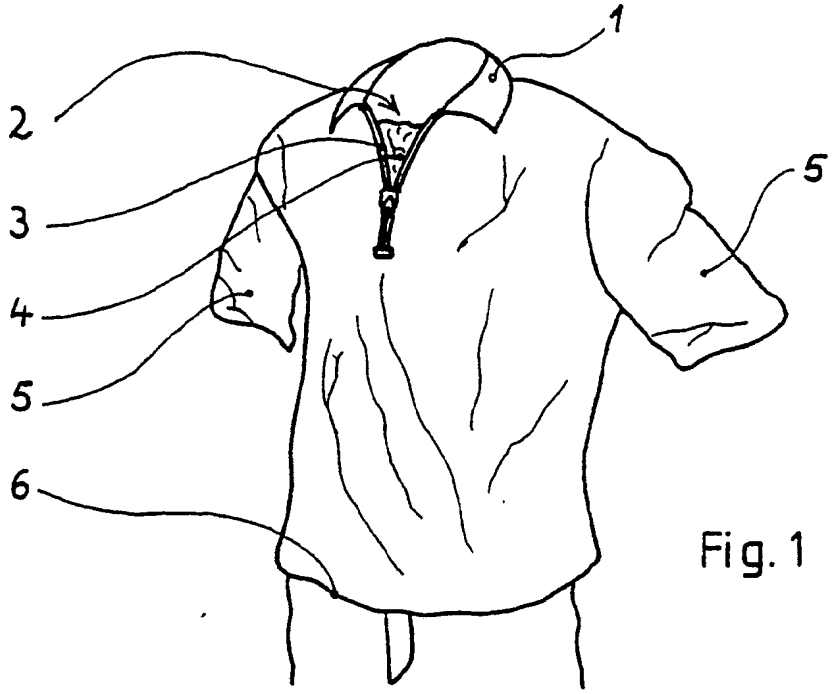


Fig. 1

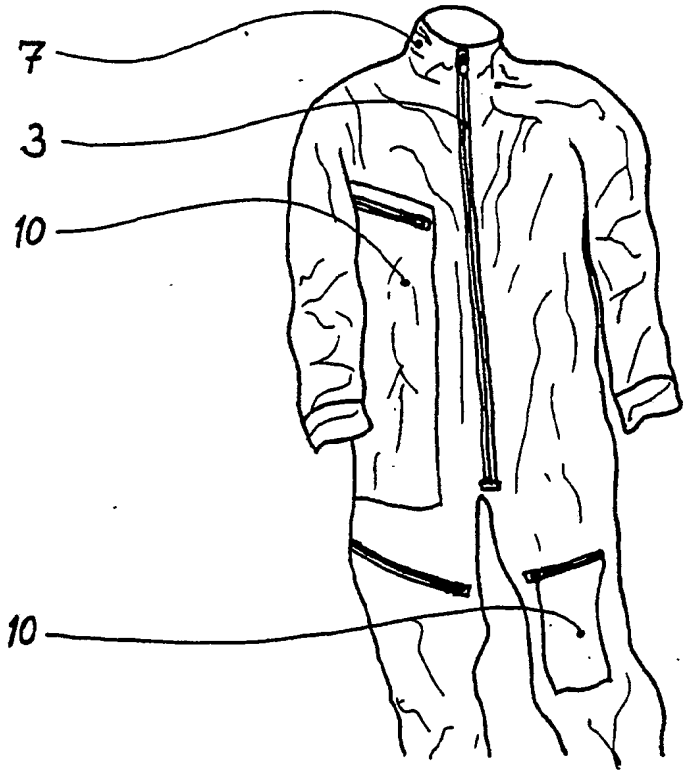


Fig. 2

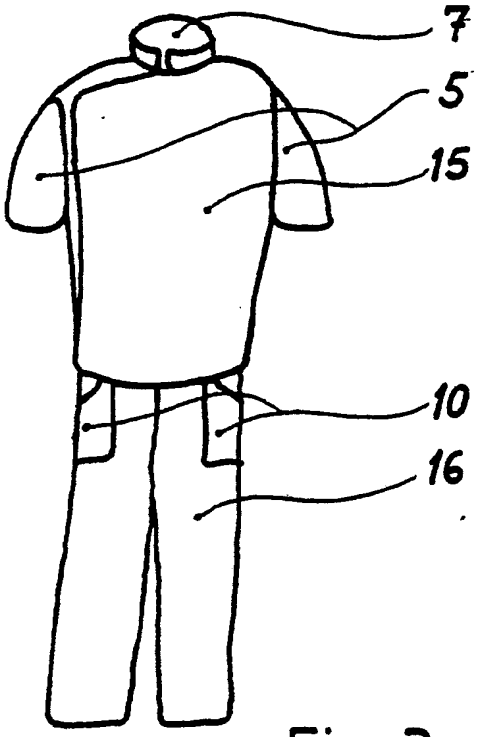


Fig. 3

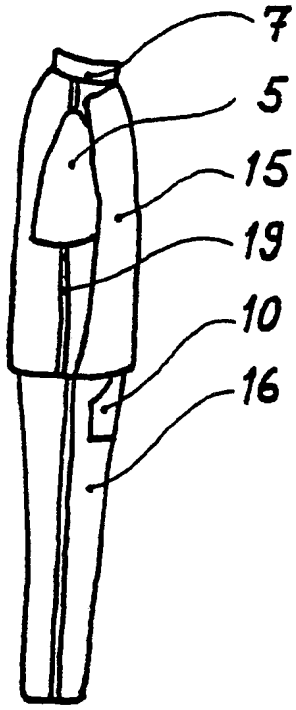


Fig. 4

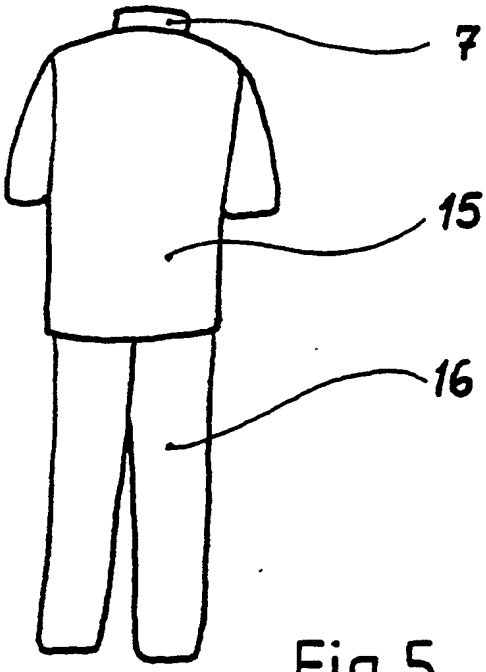


Fig. 5

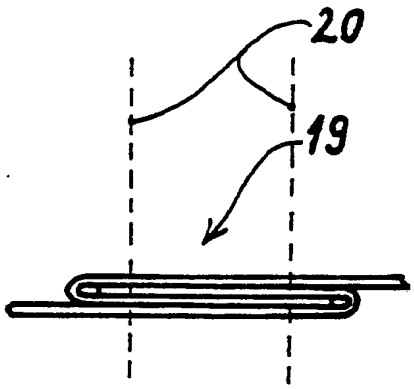


Fig. 10

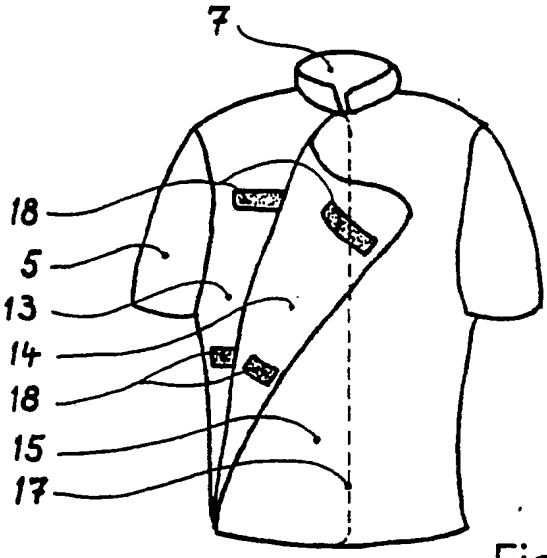


Fig. 6

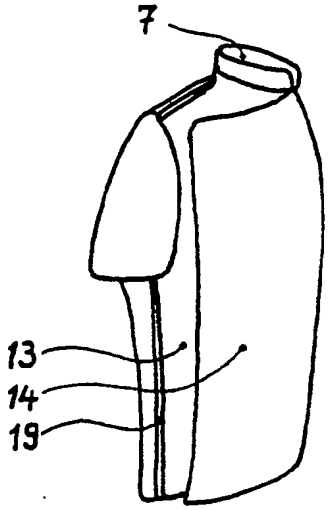


Fig. 7

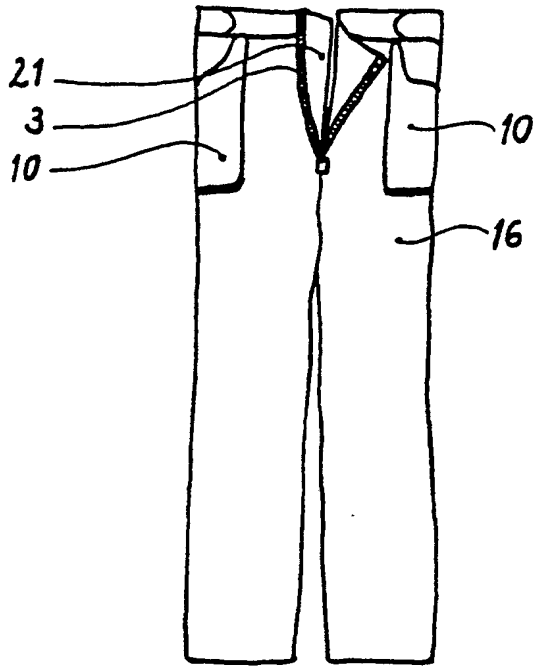


Fig. 8

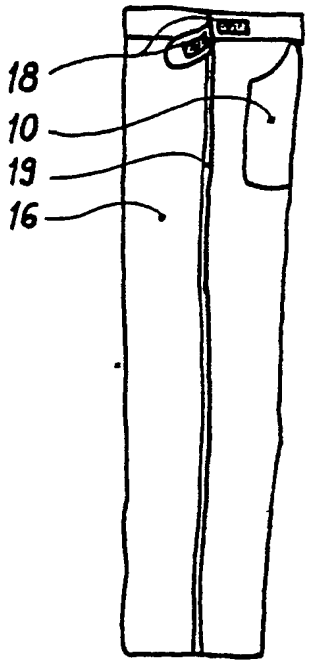


Fig. 9

European Patent Office

EUROPEAN SEARCH REPORT

Application Number

EP 90 10 1342

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl.5)
A	US-A-3987613 (WOODS) * claim 4 * ---	1, 4	D03D15/00 G21F3/02
A	US-A-4590623 (KITCHMAN) * column 4, lines 9 - 13; figures 1-4 * ---	1, 7	
A	FR-A-2311117 (BARRACUDAVERKEN AB) * claims 5, 6 * ---	1, 4	
A	US-A-3288175 (VALKO) ---		
A	GB-A-1474300 (KURARY CO LTD) ---		
A	DE-U-8804771.7 (KULLMANN) ---		
A,D	DE-A-2923286 (N.V.BEKAERT S.A.) ---		
A,D	US-A-4196355 (MAINE) -----		

TECHNICAL FIELDS SEARCHED (Int. Cl.5)

D03D
D02G
D04B
A41D
H05F
G21F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	29 MAY 1990	VAN GELDER P.A.

1

EPO FORM 1503 03.82 (P0401)

CATEGORY OF CITED DOCUMENTS

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

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

& : member of the same patent family, corresponding document

(12) UK Patent Application (19) GB (11) 2 397 272 (13) A

(43) Date of A Publication 21.07.2004

(21) Application No: 0300906.5

(22) Date of Filing: 15.01.2003

(71) Applicant(s):
Hewlett-Packard Company
(Incorporated in USA - Delaware)
3000 Hanover Street, Palo Alto,
California 94304, United States of America

(72) Inventor(s):
Richard Anthony Lawrence
James Thomas Edward McDonnell
Stefek Malkowski Zaba
Keith Alexander Harrison
John Deryk Waters

(74) Agent and/or Address for Service:
Richard Anthony Lawrence
Hewlett-Packard Limited, IP Section,
Filton Road, Stoke Gifford, BRISTOL,
BS34 8QZ, United Kingdom

(51) INT CL^7:
B42D 15/00 , G06K 19/07 , G07D 7/00

(52) UK CL (Edition W):
B6A AC12 AC91 ADE ATC
U1S S2120

(56) Documents Cited:
EP 1179811 A1 **EP 1179810 A1**
EP 1148440 A1 **EP 1139302 A1**
US 20020170973 A1 **US 20020057440 A1**

(58) Field of Search:
UK CL (Edition V) **B6A**
INT CL^7 **B42D, G06K, G07D**
Other: **EPODOC, JAPIO, WPI, Full text patent databases.**

(54) Abstract Title: **Tamper resistant physical documents containing wirelessly read electronic memories**

(57) A security document 901 includes a printed document and one or more memory circuits or tags 904. These are read by wireless or other non-contact means. They are attached to the printed document in a tamper resistant region 903. Thus the memory circuit is physically isolated to inhibit tampering or to indicate when tampering has occurred. The memory tag is read by means of a stylus 910 and processor 911. Data read from the tag is downloaded, decrypted and displayed 912. The data may include a signature which may be compared visually with the signature 902 on the document for verification. Data may include an image of the authorised bearer of the security document to permit him to be granted access to an account or asset.

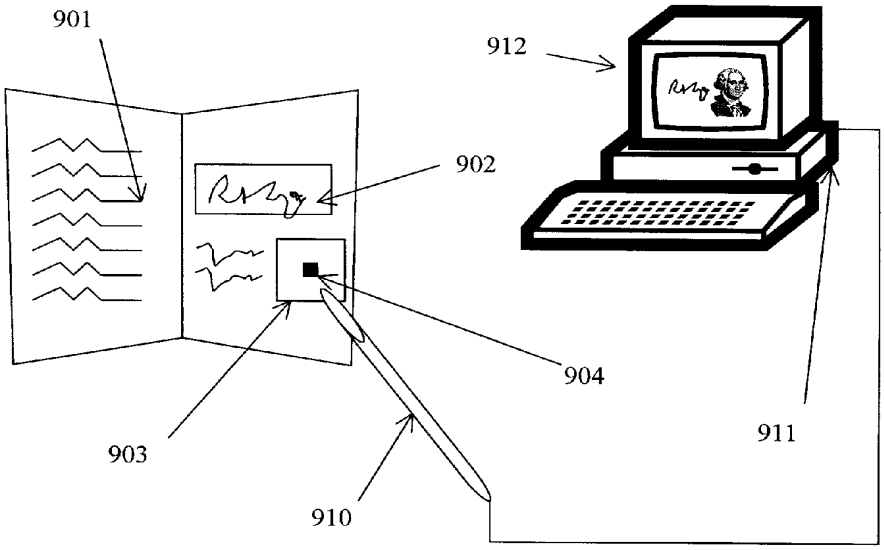


Figure 9

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

Original Printed on Recycled Paper

GB 2 397 272 A

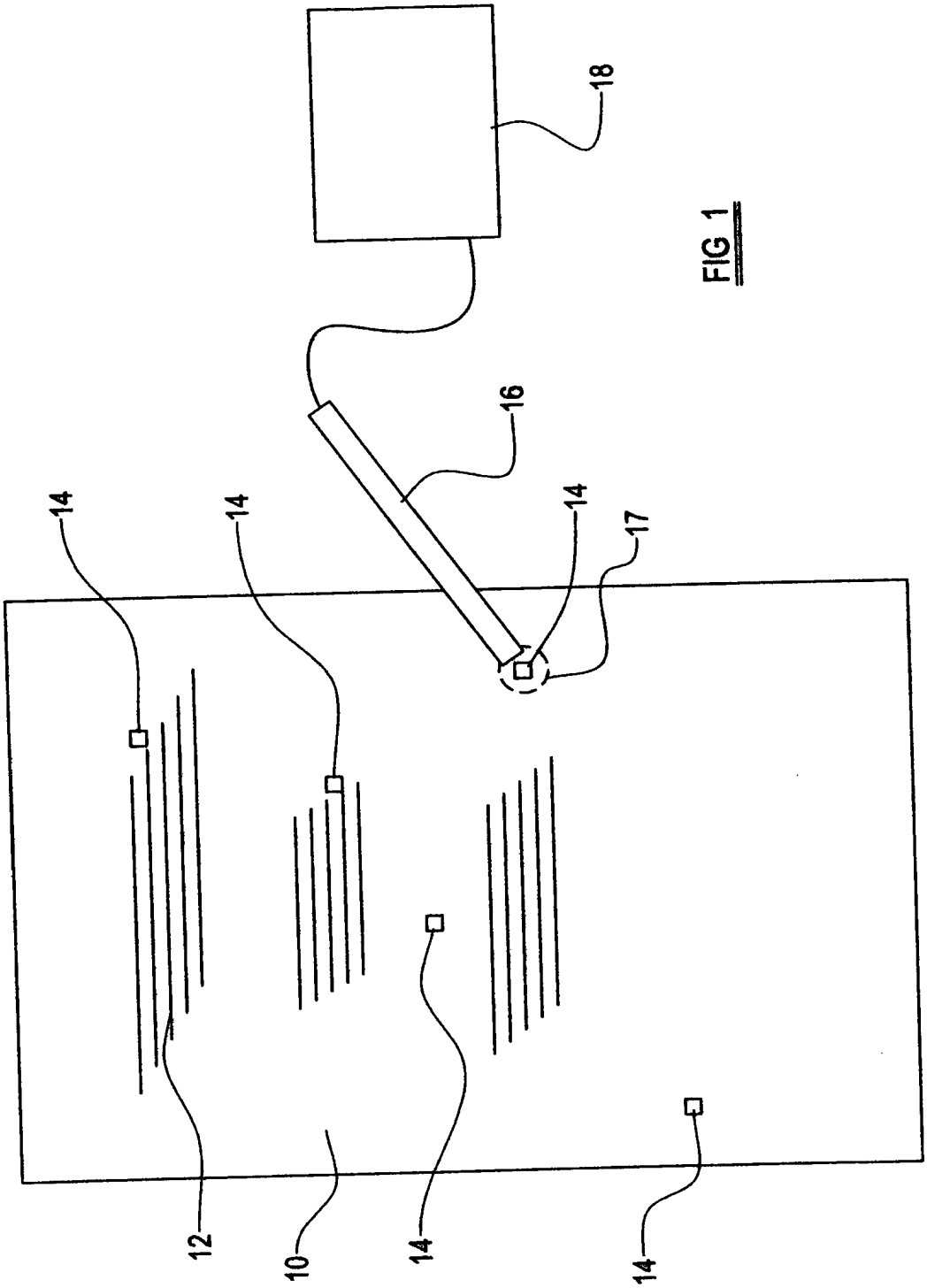


FIG 1

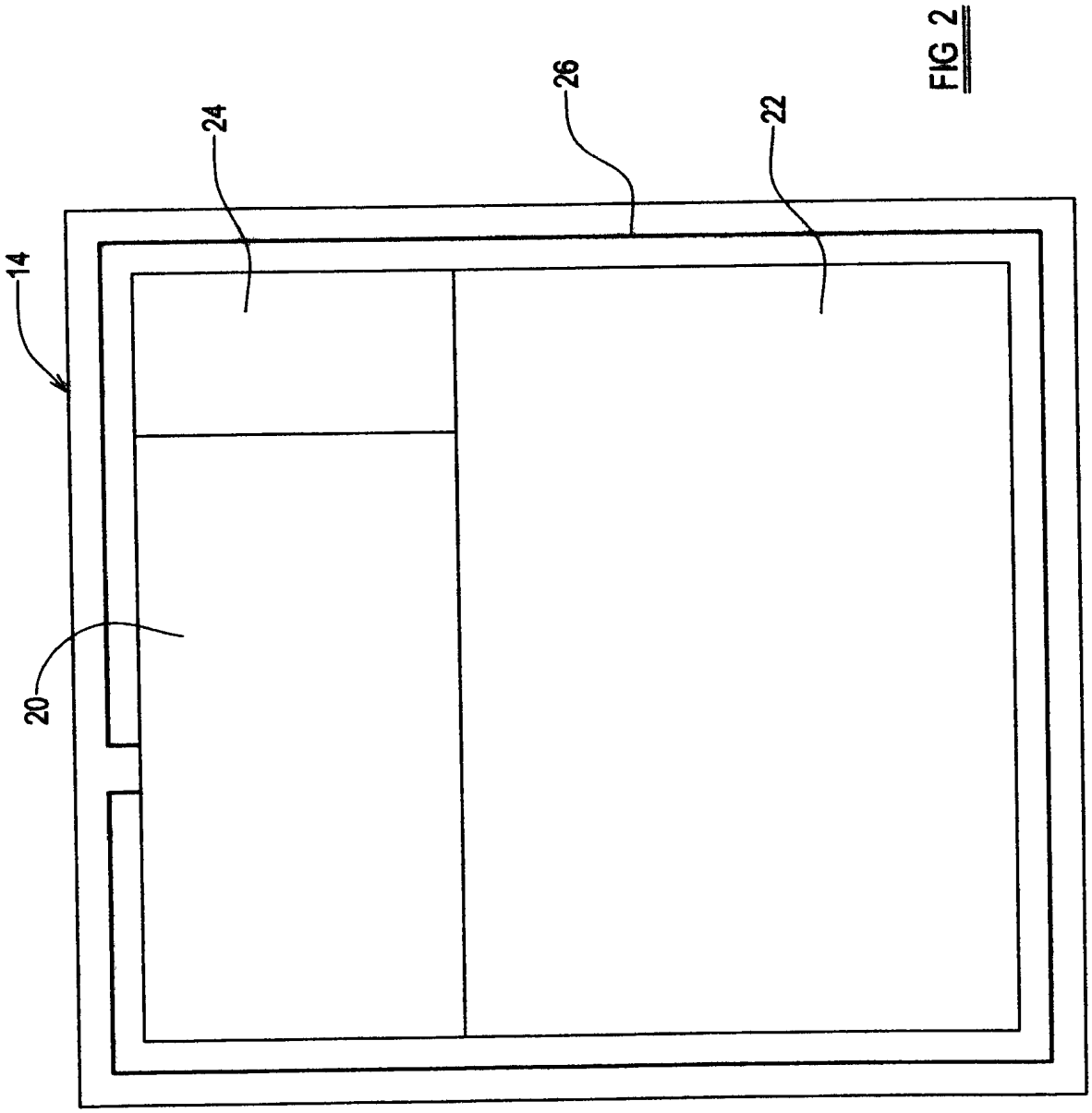


FIG 2

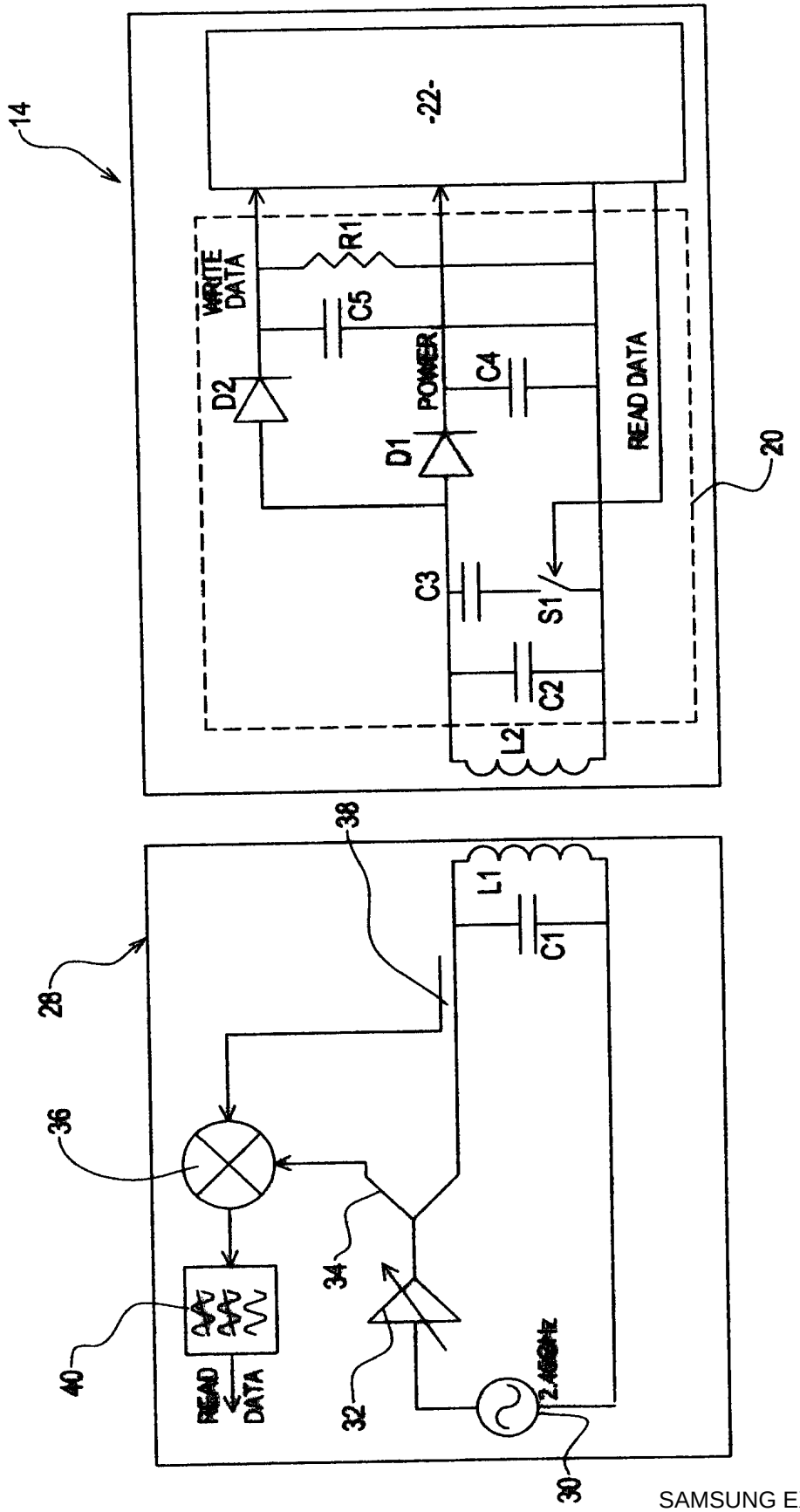

14
-22-
WRITE DATA
R1
C5
D2
POWER
C4
D1
READ DATA
20
C3
S1
C2
L2
28
38
L1
C1
36
34
40
READ DATA
32
2.4GHz
30

FIG 3

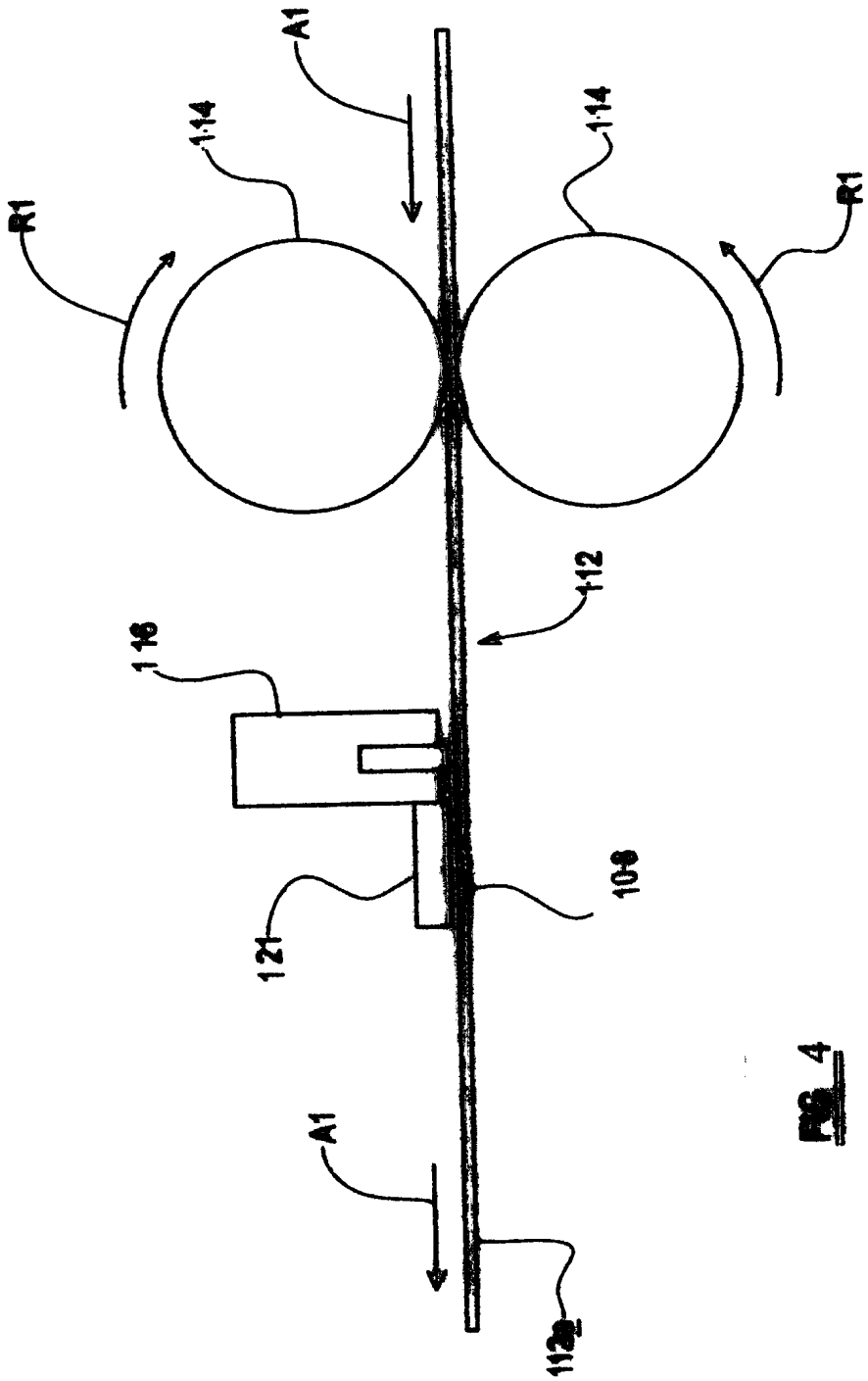


FIG. 4

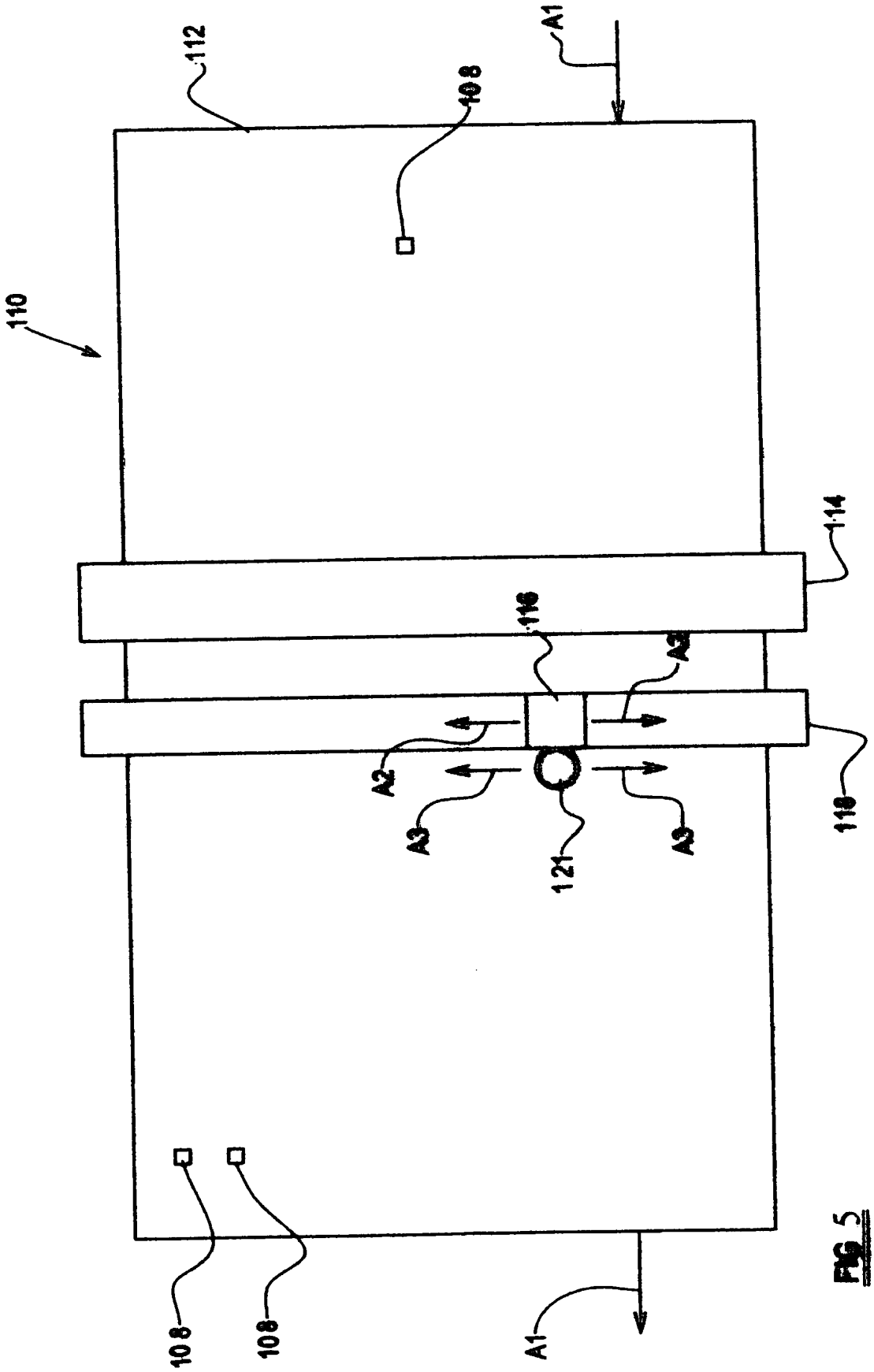


FIG. 5

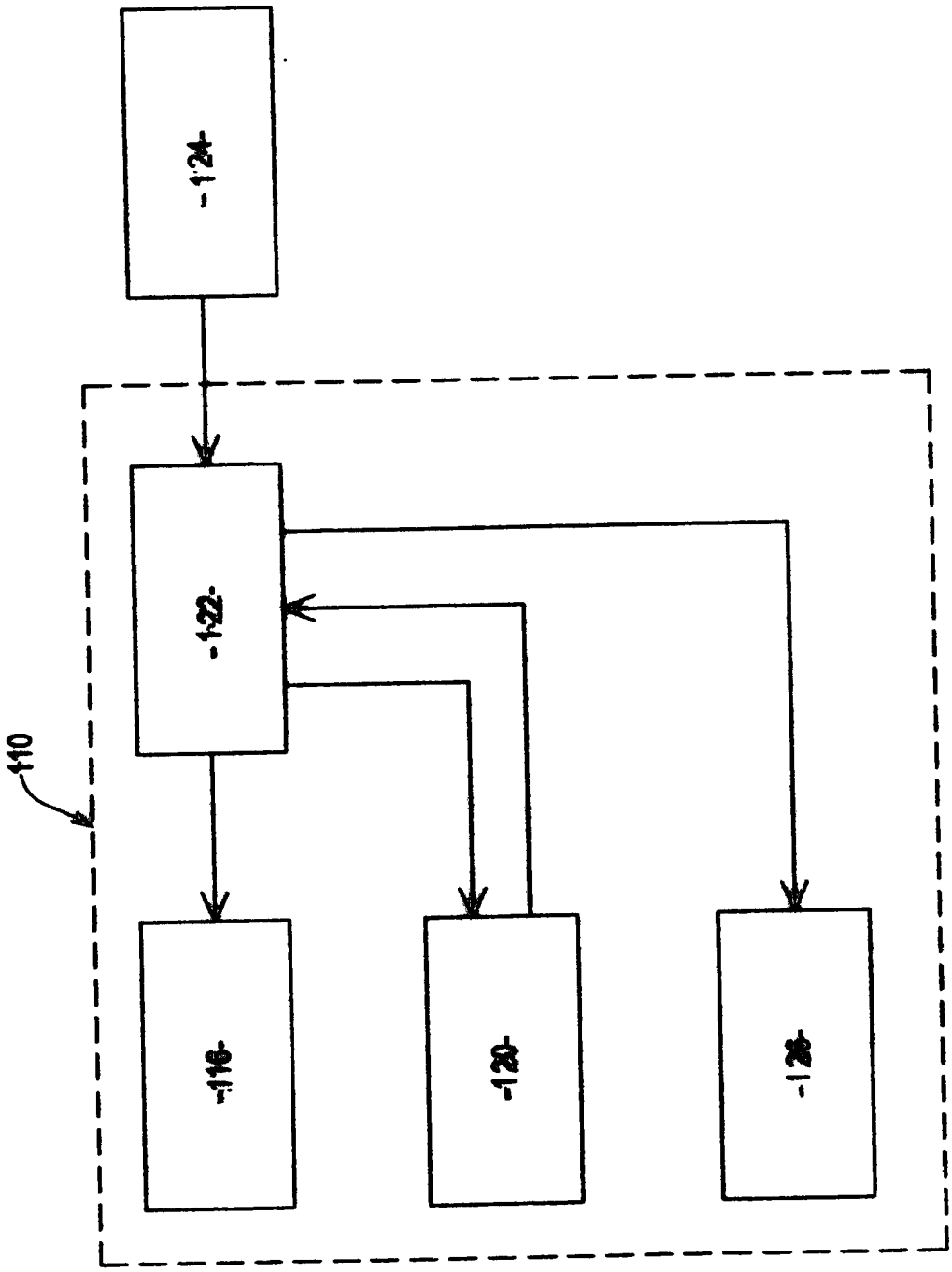


FIG. 6

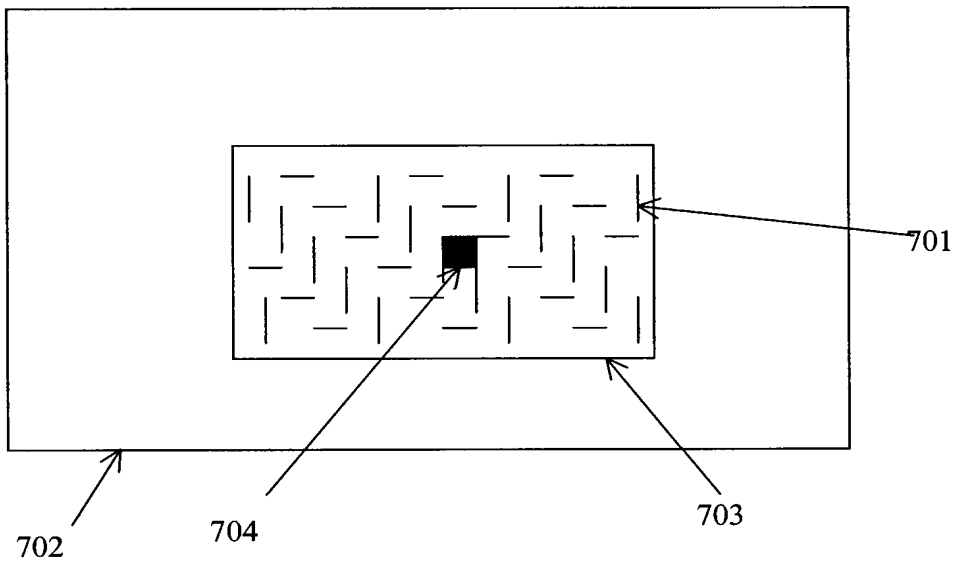


Figure 7

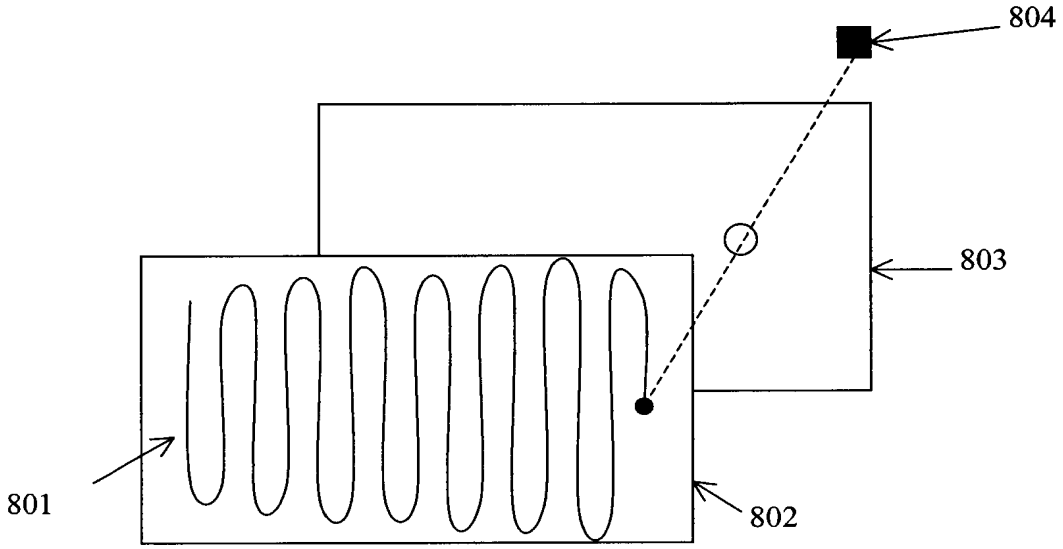


Figure 8

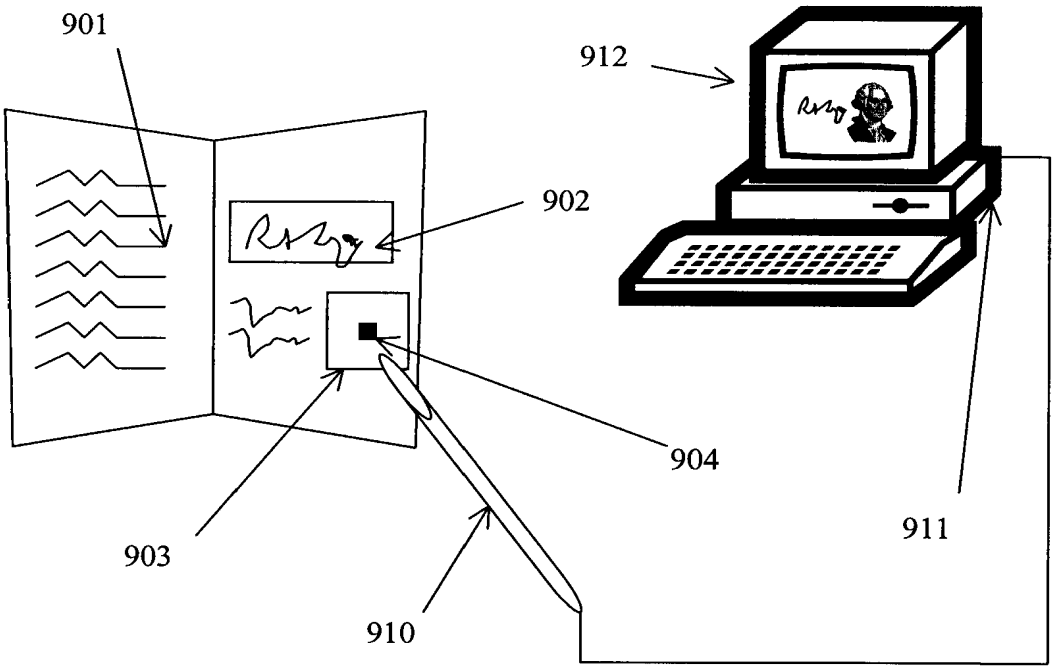


Figure 9

2397272

SECURE PHYSICAL DOCUMENTS, AND METHODS AND APPARATUS FOR PUBLISHING AND READING THEM

Field of the Invention

The invention relates to secure physical documents, to methods by which they can be created, and to methods by which they can be read. Aspects of the invention are particularly suitable for use in passbooks, either to identify an authorised bearer (such as passports) or to allow access by an authorised bearer to an asset (such as bank books).

Background to the Invention

It is well known for smart cards (both conventional smart cards with contacts, and inductively powered contactless smart cards) to contain information identifying a bearer and to allow access to a user asset. Security passes are a further example of a technology in which inductively powered devices are used to identify a bearer – for conventional security pass technology, the presence of a valid security pass is sufficient to operate the security mechanism.

For a number of applications, existing technologies such are these are unsatisfactory. They may be relatively insecure – in the case of a conventional security pass, simply obtaining the security pass may be enough to enable access for an unauthorised person. Many techniques for physical attack upon smart cards are known, and smart cards are also an unsatisfactory form factor for many applications – such as a passport, or a bank passbook. In such cases a known approach is to provide a physical book and a separate smart card – however, it would clearly be desirable to provide instead a physical document that provides a satisfactory measure of security, while preserving the possibility of providing various significant information digitally, as is possible with a smart card.

Summary of the Invention

In a first aspect, the invention provides a security document, comprising a printed document and one or more memory circuits attached to or incorporated within the printed document adapted to be read wirelessly, wherein data in the memory circuit is protected from access by an unauthorised reader, and wherein the memory circuit is physically isolated so as to inhibit physical tampering or to indicate when physical tampering has occurred.

The combination of elements allows for security models that do not currently exist. As the memory spot is accessed wireless (and is preferably also wirelessly powered, most conveniently) inductively powered, it can be embedded in the document, allowing forms of tamperproofing that involve physical isolation from potential attacks. Data can be held which personalises the document to a user in a way that is not readily obvious (for example, an image of the user held electronically in a document which itself contains no visible image of the user). In certain embodiments, the memory spot can be provided with processing power to enable a security exchange to be conducted with a reader so as to prevent unauthorised readers from gaining access to the retained information in any useful form.

In a second aspect, the invention provides a method of publishing a security document, comprising: determining first information for printing in a printed document, and second information for writing to one or more memory circuits for attachment to or incorporation within the printed document; protecting the second information from unauthorised reading; printing the first information in the printed document; writing the second information to one or more memory circuits adapted to be read wirelessly for attachment to or incorporation within the printed document; and physically isolating the one or more memory circuits so as to inhibit physical tampering or to indicate when physical tampering has occurred.

In a third aspect, the invention provides a method of reading a security document comprising a printed document and one or more memory circuits attached to or incorporated within the printed documents, comprising: obtaining authorisation information to read the security document; reading first information printed in the

printed document; wirelessly powering at least one memory circuit and wirelessly reading protected second information stored in said memory circuit;reading the second information by using the authorisation information; and comparing the second information to the first information.

Description of Drawings

Specific embodiments of the invention will now be described, by way of example, with reference to the accompanying drawings, of which:

Figure 1 illustrates a sheet of paper annotated with electronic data in a manner illustrative of an embodiment of the invention;

Figure 2 illustrates an RFID memory tag sutiable for use in the embodiments of the invention;

Figure 3 illustrates the circuitry of the memory tag of Figure 2 and of a read/write device for wireless communication with the memory tag;

Figure 4 is a schematic of the main elements of a printing device suitable for executing a method according to embodiments of the invention from the side;

Figure 5 is a schematic of the apparatus of Figure 4 from above;

Figure 6 is a block diagram of the control of the apparatus of Figures 4 and 5;

Figure 7 describes a tamper-evident security feature for a security document with respect to physical tampering;

Figure 8 describes a tamper-resistant security feature for a security document with respect to physical tampering; and

Figure 9 shows a security document according to an embodiment of the invention and a method for reading it.

Description of Specific Embodiments

There will first be described, with reference to Figures 1 to 3, a particularly suitable technology by which memory circuits can be attached to or incorporated within printed documents to enable security documents according to embodiments of the invention to be produced. The memory circuits described, referred to as memory tags, are a form of inductively powered circuit read and written by radio-frequency communication – as such they resemble the existing RFID tag – but it will be

appreciated by the skilled person that alternative forms of memory circuit may also be employable for the purpose described. There will then be described, with reference to Figures 4 to 6, an exemplary method of printing documents whose content for is divided between a printed document and one or more memory circuits attached to or incorporated within printed documents – the publishing of such documents will also be discussed, particularly in the context of security documents. There will then be described, with reference to Figures 7 and 8, approaches that may be employed to physical isolation of a memory tag using tamper resistant or tamper evident technologies. After this, there will be described approaches for protecting information stored in a memory tag against reading by an unauthorised reader. Finally, there will be described with reference to Figure 9 a suitable approach for reading a security document employing features of the preceding Figures.

Figure 1 illustrates an item, in this case a sheet of paper 10, bearing printing 12, which has been annotated with electronic data using a plurality of memory tags 14. The memory tags 14 have been secured to the sheet of paper 10 at various locations over its surface, although they may alternatively be embedded in the paper sheet 10, preferably in locations identified by the printing 12, in order to assist in locating them for the purposes of reading data from or writing data to the memory tags 14.

A hand held reader device 16 is used to communicate with the memory tags 14 in wireless manner, as will be discussed further below. The reader device 16 is also connected to a host computer, display, data rendering device or other apparatus 18 to which the data read from the memory tags 14 is passed. In the general case for this technology, reader device 16 will also be able to write to the memory tags 14 – however, in the case of security documents, this will either be prevented, or such writing will only be in addition to, rather than to replace, security data stored within the memory tag 14.

Referring now to Figure 2, a schematic of a memory tag 14 is shown. The memory tag 14 is an RFID memory tag provided on a chip, and comprises an RFID transponder circuit 20, a memory 22, a power supply capacitor 24 and an antenna coil 26 having only a few turns e.g. five, or as in this case a single turn. The RFID transponder circuit 20 operates at 2.45GHz, is of an area of approximately 0.5 mm^2, and will be described further below. The memory 22 provides 1Mbit of capacity of non-volatile memory and is of an area of approximately 1 mm^2, and may generally

FRAM (ferroelectric random access memory) or MRAM (magnetoresistive random access memory) or similar memory technology requiring low power – in the case of security applications, an appropriate form of read only memory (ROM) may instead be employed. The memory tags 14 are of a substantially square shape in plan view with an external dimension D for their sides of around 1mm.

Referring now to Figure 3, the circuitry of a memory tag 14 and circuitry 28 of the read/write device 16 are illustrated schematically, using conventional component identifications (C-capacitor, L-inductance, R-resistor, D-diode and S-switch). The RFID transponder circuit 20 of the memory tag 14 comprises a capacitor C2 which, in combination with the antenna coil L2(26), forms a resonant circuit with component values being chosen to tune the combination to approximately 2.45GHz for inductive coupling with the read/write device 16. The portion of transponder circuit 20 responsible for power supply is diode D1 and capacitor C4(24), with diode D1 rectifying the alternating current generated by the inductive coupling and the capacitor C4 acts as a power supply storage. The portion of the transponder circuit 20 responsible for receiving transmitted data from the reader device 16 is diode D2, capacitor C5 and resistor R1 which form a simple envelope detector; the data thus received is stored in memory 22 (in the case of a security document, memory 22 may be divided into RAM which can be written to by the reader 16, and ROM which cannot be so written to – writing to the memory tag 14 may of course be inhibited altogether). The portion of the transponder circuit 20 responsible for the reading of data from the memory 22 is the tuned circuit L2/C2 in combination with S1 and C3, switching C3 in and out of the circuit using S1 changes the resonance of tuned circuit L2/C2 resulting in phase modulation of the reflected power from the memory tag 14 to the reader device 16.

The circuit 28 of the reader device 16 comprises a signal generator 30 which generates a signal at the chosen frequency of 2.45GHz. This signal passes via an amplitude modulator 32, where it is amplitude modulated with data to be written to the memory tag 14, and a splitter 34, to an antenna L1 and capacitor C1 which form a tuned circuit. The component values of L1 and C1 being chosen to tune it to 2.45GHz, as for the tuned circuit in the memory tag 14, in order to maximise inductive coupling between the two circuits, and thus transmission of power and data to the memory tag 14.

The splitter 34 takes a part (as much as 50% of the power) of the amplitude modulated signal, for use as a reference signal, and passes it to a multiplier 36. The signal received from the memory tag 14, via the tuned circuit L1/C1 and divided from the outgoing signal by a coupler 38, is also passed to the multiplier 36. Thus the transmitted amplitude modulated signal and received signal are multiplied and then pass through a low pass filter 40 to provide a signal comprising the phase modulation from the memory tag 14 and thus indicative of the data read from the memory tag 14. This signal is then passed to the host computer or other device 18 to which the reader device 16 is connected, for subsequent data processing.

One amplitude modulation format which may be used to apply the data to be transmitted to the 2.45GHz signal is Amplitude Shift Keying (ASK) which only requires the simple envelope detector D2/C5 described in the circuit 20. However, other amplitude modulation formats may also be employed. Further alternatives are Frequency Shift Keying (FSK) and Phase Shift Keying (PSK) that provide near constant envelope modulation, that is without any significant amplitude modulation, however these options have more complex demodulation requirements and thus demand more complex circuitry in the memory tag 14.

With the apparatus of memory tag 14 and reader device 16 described above power transfer of around 25% can be achieved with a distance of around 1.8mm between the antennae L1 and L2, of the reader device 16 and memory tag 14 respectively. This is sufficient to transfer enough power to the memory tag 14 for it to operate.

The memory tags 14 have an external dimension D of around 1mm, as described above, and therefore the reader device 16 can communicate with them over a relatively short range, in this example of approximately 2D, (as illustrated on Figure 1 by broken circle 17). However, the distance over which the reader device 16 and memory tag 14 will communicate effectively will clearly vary with the exact details of their construction, and it may therefore be up to 10D. Distances greater than this would limit the ability to use a plurality of memory tags 14 on a single sheet of paper 10, or other item, due to the distances which would be necessary between the memory tags 14 to ensure that the read/write device 16 does communicate with the desired memory tag 14 out of a number present. To ensure that communication is with the correct memory tag 14 in every circumstance a communication distance of 5D or less is preferable.

The memory tags 14 will preferably have a data rate of 10Mbitss^{-1}, which is two orders of magnitude faster than is typical in prior art devices. Such a data rate would enable the read/write device 16 to be held over the memory tag for a very short period of time ("brush and go") for the data to be read or written as appropriate.

Although the memory tags 14 described above operate at 2.45GHz it should be understood that memory tags operating at other frequencies may be used to implement the invention. Factors affacting the choice of operating frequency for the memory tags are: a) government regulations concerning radio frequency transmissions; b) adequate bandwidth (consistent with government regulations); c) frequency high enough to render the physical size of components in the memory tag small enough to keep the area of silicon required low (and hence the cost to manufacture low); d) frequency low enough to provide adequate performance when using low-cost high-volume CMOS technology to manufacture the memory tag.

It should further be appreciated that memory tags of this functional type can be produced without using RFID technology. For example, optical technologies can be used to power, read and write to memory tags, as described in the applicant's earlier British Patent Application No. 0227152.6.

Referring to Figures 4 and 5, apparatus 110 for printing onto a base medium and data writing to a memory tag in or on the base medium is illustrated. This embodiment is for use with a base medium in the form of sheet paper 112, to which memory tags 108 have been applied or within which memory tags 108 have been embedded (as shown in Figure 4). The memory tags 108 are RFID memory tags for which the manner of writing data to the tags and reading data from the tags is well known (see above, but in addition for example the RFID Handbook, Klaus Finkenzeller, 1999, John Wiley & Sons). For simplicity only those parts of the apparatus 110 which need to be shown to describe the invention are illustrated and described. It will be understood that the apparatus 110 includes much known technology from the prior art of printers, and from the prior art of RFID memory tags, which is not described here.

The apparatus 110 includes paper feed rollers 114 which are driven to rotate as indicated by arrows R1 to feed the paper sheets 112 through the apparatus 110 along a first axis in the direction indicated by arrows A1.

The apparatus 110 further includes a print head 116, which in this example is of ink jet form, mounted on a print head carriage 118 which extends across the

apparatus 110 substantially perpendicular to the axis A1. The print head 116 is moveable back and forth along the print head carriage 118, in known manner. Thus the print head 116 is moveable back and forth along a second axis indicated by arrows A2, substantially perpendicular to the axis A1, to enable the print head 116 to access most of the upper surface 112a of the paper sheet 112 as it moves through the apparatus 110, and thus to print anywhere on that accessible area of surface 112a as required.

The apparatus 110 also includes a memory tag read/write device 120 which operates in known manner to write data to and/or read data from memory tags as required using an inductive coil 121. The inductive coil 121 of the memory tag read/write device 120 is connected to the print head 116 for movement back and forth along the print head carriage 118 with the print head 116. Thus the inductive coil 121 is moveable back and forth along a third axis indicated by arrows A3, substantially perpendicular to the axis A1, and parallel to the axis A2, to enable the memory tag read/write device 120 to read data from and/or write data to memory tags 108 located anywhere on or in the accessible area of the paper sheet 112, as will be described further below.

Referring now also to Figure 6, the apparatus 110 also includes a main processor 122 and a mechanics controller 126, which controls all the mechanical operations of the apparatus 110, (i.e. the paper feed rollers 114, the movement of the print head 116 and inductive coil 121 along the print head carriage 118). The main processor 122 receives instruction signals from a host computer 124, including the details of:

what to print;

where to print it;

where the memory tag 108 is or tags 108 are in/on the paper sheet 112; and

what data to write to the memory tag(s) 108.

The main processor 122 sends command signals as required to:

the mechanics controller;

the print head 116; and

the memory tag read/write device 120,

to implement the instruction signals.

Thus the paper sheet 112 is fed through the apparatus 110 and has the required information printed on its upper surface 112a. At the same time the memory tags 108

on or within the paper sheet 112 have the necessary data written to them by the memory tag read/write device 120, with the movement of the memory tag read/write device 120 (and print head 116) being paused with the memory tag read/write device 120 over the or each memory tag 108 as necessary for the data writing to take place.

The manner of co-ordination of the printing and data writing processes will depend on a number of factors. If, for example, the memory tags 108 are only present adjacent the top and/or bottom of the paper sheet 112 then the data writing process can take place before and/or after the printing. This would avoid the necessity for the printing process to be interrupted, and would make the co-ordination simpler. Further, when implemented with an inkjet printer, which in general requires a pause, after printing has been completed before the paper sheet is ejected, to allow the ink to dry, the data writing process could conveniently take place during this pause for memory tags present adjacent the bottom of the paper sheet 112.

In embodiments of the invention, the memory tags 108 will typically be read by hand held readers. Thus in order to assist users in the future to locate the memory tags 108 on the paper sheet 112 the memory tags 108 may have icons printed over their locations which can be readily identified by users. It is of course possible in the case of security documents that the location of memory tags 108 may not be advertised in this fashion, and that the position of memory tags may be concealed or multiple memory tags, some of which contain deceptive content, are provided, and that part of the authorisation information received by an authorised reader of the document is the knowledge of which memory tag 108 contains the valid information.

The memory tag read/write device 120 may, in addition to writing the data to the memory tags 108, also conduct a read operation to check that the data has written successfully before the paper sheet 112 is moved on following the data write operation. Alternatively, particularly if the apparatus 110 is operating at high speed, a separate data check device (not shown) may be included in the apparatus such that this operation takes place downstream of a memory tag write device which in this case need not also be capable of data reading.

It will be readily appreciated by the person skilled in the art that the modification to a conventional printing technology (in this case, the functional structure of the printing device is that customarily found in inkjet printing technology) can be employed to functional structures used in other printing technologies, such as

laserjet and digital presses (such as HP Indigo™ presses). This last technology is particularly suitable for mass production of documents, for example book publication.

It can be seen from the above that there is no fundamental complexity involved in creating and publishing documents in accordance with embodiments of the invention using printing technology described in Figures 4 to 6. As for the content generation stage, conventional word processing and web publishing software (such as Microsoft® Word and Microsoft® Frontpage™ respectively) familiarly allows inserts of data of a different data type – in web publishing in particular, it is familiar to determine an icon for rendering that has a hyperlink function and can serve, if activated by a reader of the document, to link to another page or a file (such as a sound clip). Essentially the same approach can be taken here – the user composing the document on host computer 124 can place or identify a memory tag position on the page being composed and may designate a particular file to be stored in that memory tag. The document for printing, the files for the memory tags, and all placement information can then be provided by the document generation software on host computer 124 to the main processor 122 of the printing device for rendering as described above.

The security document contains at least two discrete forms of protection for the security information stored in the memory tag: protection against physical tampering, and protection against unauthorised reading. These will be considered in turn, together with any modification to the basic technology described above (in many cases it will be necessary for the physical isolation step to be completed after the document creation stages indicated above – in particular, to convert the memory tag to a read-only one, either by physically modifying the memory tag structure after writing or by preventing write access to the memory tag).

As the memory tag is both read and powered wirelessly, it is possible for it to be physically isolated (by encapsulation or otherwise). This physical isolation needs to be such that the memory tag can still be powered and read, and such that it can still be incorporated within or attached to the printed document. It is possible to protect the memory tag against the effects of physical tampering and still accept these constraints. Approaches to protection against tampering include using tamper-evident protection, and using tamper-resistant protection. Examples of each will now be described.

Tamper-evident protection does not itself prevent physical tampering. It does, however, show when physical tampering has occurred. For tamper-evident protection, it is necessary only that physical tampering will result in irreparable effects to the physical document that will be apparent on subsequent inspection. An example is the tamper-evident signature strip described in US Patent No. 5762378, in which the fabric of the tamper-evident area is weakened by a pattern of cuts through the paper substrate (illustrated in exemplary fashion in Figure 7) in such a way that the cuts 701 through the paper substrate 702 in the tamper-evident area 703, which here also includes a memory tag 704, are such that attempts at physical modification within the tamper-evident area 703 will lead to irregular tearing patterns.

Tamper-resistant protection, by contrast, aims to prevent physical tampering. By "tamper-resistant", it is not here implied that a tamper-resistant device is immune to all forms of tampering, however technically sophisticated. As is described in the literature of tamper protection (see, for example "Tamper Resistance – a Cautionary Note", by Ross Anderson and Markus Kuhn, published in "The Second USENIX Workshop on Electronic Commerce Proceedings", Oakland, California, November 18-21, 1996, pp 1-11), most forms of tamper resistance can be overcome with sufficient time, money, and technical sophistication. Here, it is understood that protection is "tamper-resistant" if it is sufficient to increase significantly the level of difficulty for an attacker in achieving effective physical tampering.

As indicated above, a significant consideration in achieving effective tamper-resistant protection is that the ability to read data from the memory tag should be preserved. Full electromagnetic shielding of the memory tag – one known tamper-resistance technique – is thus not an option. A technique which may be an option, however, is effective design of the memory tag antenna. Figure 8 shows an antenna structure for tamper protection. An antenna 801 on a Mylar sheet 802 is attached through an earth plane sheet 803 to the memory tag 804 – the whole assembly being encapsulated and fixed on to the paper document (not shown). Advantageously, the memory tag in this arrangement may be written to, and then physically prevented from being rewritten, before the construction of the tamper-protected device. The meandering structure of the antenna (which may of course be a great deal more complex than shown here) has a secondary use as an inhibitor of the memory tag. A physical property of the antenna (such as its impedance, or time of flight along it) may be measured by the memory tag (which therefore will need to be provided with

appropriate measurement circuits – the construction of which will be readily determinable by the skilled person) and compared with a known value. If this value is not returned, this will be taken as indicative of physical tampering (for example, the shorting together of two adjacent wires in the antenna) and the memory tag will not allow itself to be read by any reader.

Additional tamperproofing technologies, some but not all of which are applicable to the present use (again, this will be clearly evident to the person skilled in the art) are discussed in the applicants European Patent Application Publication No. 1273997. Again, for many of the techniques described here it will be desirable to write to the memory tag and to physically prevent further writing to the memory tag (or to a specific memory of the memory tag) before completing the tamperproofing process itself.

In addition to physical resistance to the effects of tampering, the memory tag itself provides security protection in that the information it holds is only usefully accessable to an authorised reader. This can be achieved in a number of ways, depending on factors such as the degree of security required, the length of time for which security is required, and the processing capacity (if any) available on the memory tag itself. Options, in ascending level of security, are described below.

(1) <u>Pure memory without additional security features on tag – all security operations take place before writing to tag.</u>

The security operations in this case take place on or before writing – for example, that the data stored in the memory tag is written with a secret. (For example, a hash function is used to take a hash over the picture of the holder, their access permissions, a reference to any credentials they produced when the badge was first created, and so on. The hash is authenticated using a secret shared among all authorised readers which could then be used (for example) as the access code in a keyed hash or MAC (Message Authentication Code). This may work very well in short term applications (eg entry to a specific event), but is less readily applicable to circumstances in which it is desired to write to the memory tag, particularly where it is necessary for the memory tag to contain updatable state information.

(2) <u>Memory tag with unique ID</u>

This provides substantial advantages for applications where writing to the memory tag is necessary. Each write to the memory tag which wishes to preserve integrity now incorporates the spot's unique ID in the hash which is MACed or

signed; and each validator asks the spot afresh for its unique ID in recomputing the information-to-be-validated. This makes casual copying from one memory tag to another detectable, as the difference in unique IDs between the original and the clone will cause the hash comparison to fail.

There are a number of ways to create a unique ID. For maximum trackability, the format of a unique-ID may be (or is the unkeyed hash of) a manufacturer ID: week code: batch code: sequential number. An untrackable approach would be for the memory tag to contain a hardware-based random number generator (RNG), and upon first activation (maybe during manufacturing test) the RNG runs, the resulting unique-ID is written into write-once storage, and the writeability of that storage is reliably and permanently disabled. There's also a choice over how the unique ID is made accessible to the readers and writers: this can range from returning a raw ID to returning only a hash of a random number supplied by a reader with the unique ID. For random generation, to prevent clashes it would be desirable to have at least 256 bit unique Ids.

(3) Memory tag with unique ID, and on-spot hashing (with some access-protected storage)

This is the lowest security level which requires processing capacity on the memory tag. It is suitable for applications in which duplication of credentials must be detectable. It is particularly suitable where the memory tag should be relied upon to deliver results of processing over data it doesn't directly reveal, should be able to self-check the integrity of data it stores, or should be able to participate in providing confidentiality for data it stores.

Without its own processing, the memory tag needs to rely on the other components of a writing/reading/credentialing/validating system to hold all long-term and short-term secrets. A first cryptographic processing technology to employ in the tag itself is hashing, with SHA-1 being a logical choice of hash function. Hash functions are fast to execute, use relatively little RAM and code space, and are a building-block for reliable integrity checks.

One immediate use of an on-chip hashing capability is to hide the raw unique ID value from readers, instead of reporting the result of hashing that ID and a reader-supplied value. The use of that additional value would vary: it may be recorded alongside information recorded on memory tag, to allow a later recalculation of a hashed value; it may in other uses be a secret which is deliberately *not* recorded on the

memory tag, allowing for a hash value recorded on the memory tag to be revalidated only by a validator which knows that secret value. An on-chip hashing function would also allow the memory tag to implement cryptographically-protected write-once storage, using a rolling hash of the data written into the "update-only" memory keyed with the unique ID so that the memory tag itself can report the integrity of the append-only log.

Using the hash function, it is possible to implement on-chip encryption. Briefly described, this can be done by hashing (a transform of) the unique ID and the starting address of a block of memory to create a pseudo-random stream which we XOR against the block of memory. What is stored is that encrypted form, while to read it out to a suitably-privileged reader (that would be a reader who can supply the extra secret needed for the transform of the unique ID) we recreate the keystream and XOR it against the stored data to derive plaintext.

Arrangements of this type allow for the possibility of access control: that areas of memory may be either encrypted or simply not returned to a reader unless that reader provides some suitable secret. The hash-derived keystream provides one way of doing that, with the chip returning contents of memory locations either as-they-are or XORed against a keystream determined by a combination of the unique ID and a reader-supplied quantity (a similar approach can be applied to writing). This still leaves the chip responding to all requests from all readers to read memory (with the notable exception of the uniqueID itself), relying on the result to be unintelligible without the correct key having been supplied. It may in some cases be advantageous to give the chip the capability of simply not responding to particular commands, and/or parameter values for some commands (for example, particular address ranges), unless the reader can supply an authentication value (or prove knowledge of an authentication value).

(4) <u>Memory tag with unique ID, on-spot hashing, and asymmetric cryptographic capability</u>

This is appropriate where the memory tag has responsibility for control of data it stores, and can receive and transmit data with confidentiality and integrity. It is not apparent that many applications will require this approach to security, as the overall security of the system will generally be better improved by considering another aspect of the system (such as secure handling of authentication information provided to authorised readers).

Adding asymmetric cryptographic capability — RSA and elliptic-curve capability are both possibilities — to the spot has some notable costs: the codespace and memory requirements are non-trivial, the execution times for public-key operations are substantial (whole seconds), the management of key material and partial results becomes more complicated, and if the memory tags are expected to understand standard-format certificates too, the processing requirements go up some more. The advantage, though, is that we get a well-understood way of both validating data as having come from the memory tag, and sending it data which only it can read, without having to share the material for creating the validation and decrypting the data with any entity outside the memory tag (whether it's firmware in the reader/writer or code executing on a conventional host — PC, PDA, or similar).

(5) Memory tag with unique ID, on-spot hashing, and both asymmetric and symmetric cryptographic capability

This is useful where the memory tag is required to be a self-standing cryptographic object implementing a sophisticated information management policy. Again, the number of application scenarios where this will be appropriate may be rare. This is in part because the memory tag doesn't have human-interface capabilities of its own: so although it is now capable of doing symmetric cryptography as well as asymmetric, any bulk data it is handling still has to be passed, as plaintext, either into or out of the memory tag to interact with a person (be read, listened to, dictated in, or whatever). Thus, you have to trust the interaction device not to violate your security policy — i.e. to handle that valuable plain text resulting as securely as the highly secure memory tag.

Appropriate processing for achieving hashing and asymmetric and symmetric cryptographic capability is well understood by the skilled person, and will not be further described here.

Using the approaches described above, a security document can be created which comprises a printed document and one or more memory tags. These memory tags are memory circuits adapted to be read wirelessly (preferably, inductively powered also) and are attached to or incorporated within the printed document. Data in the memory circuit is protected from access by an unauthorised reader, either by measures taken in writing the data, or by presence of a unique ID or cryptographic

capacity in the memory tag itself. The memory tag is physically isolated so as to inhibit physical tampering (for example, by tamper-resistant techniques of the kind discussed with reference to Figure 8) or to indicate when physical tampering has occurred (for example, by tamper-evident techniques of the kind discussed with reference to Figure 7).

A security document of this type is shown in Figure 9, which also illustrates how a document of this type would be read. A security document 901 contains printed material and a signature strip 902, signed by an authorised bearer. Embedded within the security document 901 is a memory tag 903 embedded in a tamper-resistant region 903. A reader for the memory tag comprises a stylus 910 used in conjunction with a computer or other processing device 911 – the processing device has a display 912.

The reader accesses the memory tag 903. The physical isolation and protection of the memory tag, together with the security policy employed in writing to or electronically protecting the memory tag, should be sufficient to give adequate confidence to the authorised reader that the memory tag has not been subverted. The information in the memory tag is then downloaded, after whatever security interchange between the memory tag processor (if there is one) and the processor 911 is required, and decrypted or otherwise converted to usable form by use of the authorisation information, to which processor 911 has access. The results are then displayed on display 912. In this case, what is displayed is the signature matching the signature on the signature strip 902, but also the face of an authorised bearer – the user of the reading device can therefore determine not only whether the security document is valid (by the matching of the signatures) but also whether it is being carried by the correct person – this information not being available to an unauthorised bearer, as the security document itself contains no printed picture.

Such a security document could be used, as in the scenario described above, identify an authorised bearer of the security document. However, it could also be used to allow access to a specified asset or assets by the authorised bearer (such as a bank account). A part of this process could be to update state information (such as a withdrawal log) on the memory tag itself, for a memory tag which contains writable memory.

CLAIMS

1. A security document, comprising a printed document and one or more memory circuits adapted to be read wirelessly attached to or incorporated within the printed document, wherein data in the memory circuit is protected from access by an unauthorised reader, and wherein the memory circuit is physically isolated so as to inhibit physical tampering or to indicate when physical tampering has occurred.

2. A security document as claimed in claim 1, wherein the memory circuit is inductively powered.

3. A security document as claimed in claim 2, wherein the memory circuit receives and transmits data wirelessly at radio frequency.

4. A security document as claimed in any preceding claim, wherein physical isolation of the memory circuit employs one or more tamper-evident strips.

5. A security document as claimed in any preceding claim, wherein an antenna of the memory circuit is adapted for detection or resistance of physical tampering.

6. A security document as claimed in any preceding claim, wherein the security document is adapted to identify an authorised bearer of the security document.

7. A security document as claimed in claim 6, wherein the security document is adapted to allow access to a specified asset or assets by the authorised bearer.

8. A method of publishing a security document, comprising:
   a. determining first information for printing in a printed document, and second information for writing to one or more memory circuits for attachment to or incorporation within the printed document;
   b. protecting the second information from unauthorised reading;
   c. printing the first information in the printed document;

d. writing the second information to one or more memory circuits adapted to be read wirelessly for attachment to or incorporation within the printed document; and

e. physically isolating the one or more memory circuits so as to inhibit physical tampering or to indicate when physical tampering has occurred.

9. A method of reading a security document comprising a printed document and one or more memory circuits attached to or incorporated within the printed documents, comprising:

a. obtaining authorisation information to read the security document;

b. reading first information printed in the printed document;

c. wirelessly powering at least one memory circuit and wirelessly reading protected second information stored in said memory circuit;

d. reading the second information by using the authorisation information; and

e. comparing the second information to the first information.

10. A method as claimed in claim 9, further comprising comparing the second information to one or more characteristics of a bearer of the security document.

The Patent Office

19

INVESTOR IN PEOPLE

Application No: GB 0300906.5
Claims searched: 1-10

Examiner: Richard Pannett
Date of search: 30 July 2003

Patents Act 1977 : Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance	
X	1-3,5,8	EP 1148440 A1	(HITACHI) See: abstract; column 1 lines 5-12; column 10 lines 30-57; column 26 lines 24-30; figure 3.
X	1-3,8,9	EP 1179810 A1	(EUROPEAN CENTRAL BANK) See: abstract; paragraphs [0006]-[0009]; figures 1-8.
X	1-3,5	EP 1179811 A1	(EUROPEAN CENTRAL BANK) See: abstract; paragraphs [0016],[0023]; figure 2.
X	9	EP 1139302 A1	(HITACHI) See: abstract; column 3 lines 39-54; column 17 lines 2-32; figure 11.
A		US 2002/0057440 A1	(WEINER) See: abstract; paragraph [0030]; figures 1-3,5.
A		US 2002/0170973 A1	(TERAURA) See: abstract; paragraphs [0007],[0066].

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC[V]:

B6A

Worldwide search of patent documents classified in the following areas of the IPC[7]:

B42D, G06K, G07D

The following online and other databases have been used in the preparation of this search report:

EPODOC, JAPIO, WPI, Full text patent databases.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 May 2004 (06.05.2004)

PCT

(10) International Publication Number
WO 2004/038644 A2

(51) International Patent Classification[7]: G06K

(21) International Application Number: PCT/US2003/034036

(22) International Filing Date: 27 October 2003 (27.10.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/421,050 25 October 2002 (25.10.2002) US

(71) Applicant: MATRICS, INC. [US/US]; Columbia Corporate Park 1, 8850 Stanford Boulevard, Suite 3000, Columbia, MD 21045 (US).

(71) Applicants and
(72) Inventors: POWELL, Kevin, J. [US/US]; 1202 Cherry Tree Lane, Annapolis, MD 21403 (US). SHANKS, Wayne, E. [US/US]; 1731 Lancaster Street, Baltimore, MD 21231 (US). BANDY, William, R. [US/US]; 2406 Bell Branch Road, Gambrills, MD 21054 (US).

(74) Agents: SOKOHL, Robert, E. et al.; 1100 New York Avenue, N.W., Washington, DC 20005-3934 (US).

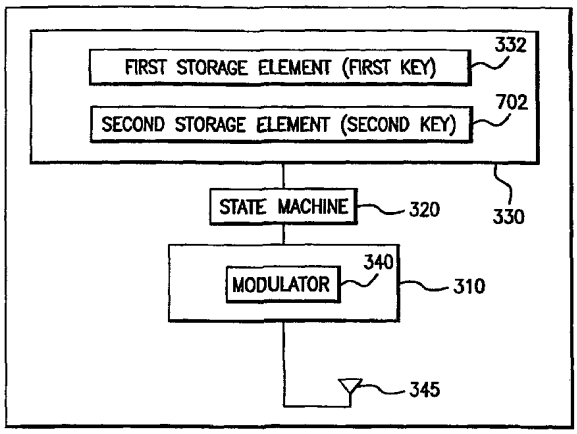
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: OPTIMIZATION OF A BINARY TREE TRAVERSAL WITH SECURE COMMUNICATIONS



(57) Abstract: Methods and systems for the negotiation of a population of RFID tags with improved security is provided. In one aspect, a binary traversal is performed to singulate tags without using information that directly identifies the tags in the tag population. A key is generated to identify each RFID tag of the population of RFID tags. The generated key does not include bits identifying an item with which the particular RFID tag is associated. A binary tree algorithm is operated to identify one or more tags in the population of RFIDs tags using the generated keys. In another aspect, frequency hopping and/or spread spectrum techniques are used to provide improved security while negotiating tags. In another aspect, the reader causes the tags to scroll series of bits back to the reader for each bit sent to the tags to provide improved security.

WO 2004/038644 A2

Optimization Of A Binary Tree Traversal With Secure Communications

Background Of The Invention

Field of the Invention

[0001] The present invention generally relates to radio frequency identification (RFID) tags, and more particularly to secure negotiation of a population of RFID tags.

Background Art

[0002] In an RFID system, an RFID reader interrogates one or more RFID tags for information. The RFID reader may be required to distinguish between and communicate with a large number of different RFID tags within a given communication range. Typically, a unique identification number identifies each tag. It is important that the RFID reader is capable of quickly and accurately reading the identification (ID) number associated with each tag. In order to interrogate a particular tag, typically, the reader broadcasts the identification number of the tag, in a bit-by-bit fashion, and the tag responds.

[0003] However, such RFID systems can suffer from security problems. In a first security problem, a signal transmitted from the reader to a tag may travel a long distance, such as a distance of miles. Thus, when the reader broadcasts a complete tag ID number, an undesired third party can receive this broadcast, and collect this transmitted data. Thus, an undesired third party can obtain the identification number of the tag in this manner.

[0004] In a second security problem, an undesired third party can fool or "spoof" an RFID reader into broadcasting the identification number of a tag in order to

collect it. For example, in such a situation, the undesired third party responds to broadcasts of a reader. The undesired third party transmits false tag responses to the reader to cause bit collisions that thereby cause the reader to broadcast the identification number bits.

[0005] Thus, what is needed is a way of communicating with tags on an open-air communication channel, while protecting tag data, such as the tag identification number.

Brief Summary Of The Invention

[0006] The present invention provides for secure communications (i.e., negotiations) between readers and tags. According to the present invention, a reader can communicate with tags on an open-air communication channel, while keeping tag data, such as tag identification numbers, secure.

[0007] According to embodiments of the present invention, conventional binary traversal algorithms can be modified to provide for secure communications between readers and tags. For example, a conventional binary tree traversal algorithm can be modified to provide for the secure negotiations.

[0008] For example, a method of secure negotiation of a population of RFID tags is implemented so that a complete tag number is not transmitted over the air. The steps in the method can include the following: (1) operating a binary tree algorithm to identify an RFID tag in a population of RFIDs tags; (2) receiving bits from one or more of said population of said RFID tags during said binary tree algorithm; and (3) echoing said received bits back to said population of RFID tags only at forks in said binary tree algorithm.

[0009] In another aspect, a method of secure negotiation of a population of RFID tags is implemented so that a binary traversal is performed that contains no application data. The steps in the method can include the following: (1) generating a key to identify an RFID tag of the population of RFID tags, wherein

the key does not include bits identifying an item with which the RFID tag is associated; (2) operating a binary tree algorithm to identify the RFID tag in a population of RFIDs tags; and (3) receiving bits from the RFID tag during the binary tree algorithm.

[0010] In an aspect, the generating step includes the step of selecting a number from a sequence of numbers to use as the key.

[0011] In another aspect, the generating step includes the step of using a randomly generated number as the key.

[0012] In another aspect, the generating step includes the step of dynamically generating a number prior to each traversal of the population of RFID tags to use as the key.

[0013] In another aspect of the present invention, a method and system for a radio frequency identification (RFID) tag to communicate with a RFID reader with improved security is described. The tag stores a corresponding first key, which can be an identification number. The first key comprises a first bit pattern. A first at least one bit is received from the reader to cause the tag to respond to a binary traversal operation with a second key, defined by a second bit pattern. A binary traversal operation is engaged with the reader. During the binary traversal operation, a series of bits are received from the reader, and the tag responds to each bit of the series of bits with a corresponding bit of the second bit pattern. The tag is thereby singulated, using the second bit pattern of the second key.

[0014] In aspects, the second bit pattern can be read from storage in the tag.

[0015] In another aspect, the bit values for each bit of the second bit pattern can be randomly generated during operation of the tag. In an aspect, the randomly generated second bit pattern can then be stored.

[0016] In another aspect, a second binary traversal operation can be engaged with the reader. During the second binary traversal operation, the tag can respond with the stored second bit pattern, or can respond with a newly randomly generated second bit pattern.

[0017] In another aspect of the present invention, a radio frequency identification (RFID) tag is described. The tag includes an antenna, a modulator, a first storage, and a second storage. The modulator is coupled to the antenna. The modulator is configured to backscatter modulate bits received from the antenna with response bits. The first storage stores a first bit pattern (i.e., first key) that defines an identification number. The second storage stores a second bit pattern (i.e., second key) that does not include bits identifying an item with which the RFID tag is associated. A first bit combination received from a reader causes the tag to respond to a binary traversal with the first bit pattern. The second bit combination received from the reader causes the tag to respond to a binary traversal with the second bit pattern.

[0018] In an aspect, the tag includes a random bit pattern generator for generating the second bit pattern. In one aspect, the generated second bit pattern is stored in the second storage. In an alternative aspect, the generated second bit pattern is not stored, and the second storage is not present. In this aspect, the second bit pattern is transmitted by the tag in a response to the reader as the second bit pattern is generated.

[0019] In another aspect of the present invention, a method and system for a radio frequency identification (RFID) reader to communicate with a population of RFID tags with improved security is presented. Each tag in the population stores a corresponding first key, which can be an identification number, and which includes a first bit pattern. A first at least one bit is transmitted to the population of tags to cause tags to respond to a binary traversal operation with a second bit pattern. A substantially constant signal is transmitted to the population of tags. A plurality of bits of the second bit pattern are received from a first tag during transmission of the substantially constant signal. The transmission of the substantially constant signal to the population of tags is terminated by the reader to stop the first tag from transmitting further bits of the second bit pattern. A

substantially constant signal can be repeatedly transmitted to the tags, and terminated, in order to receive additional pluralities of bits from the first tag.

[0020] In another aspect of the present invention, frequency hopping techniques and/or spread spectrum techniques can be used by the reader to improve security.

[0021] These and other objects, advantages and features will become readily apparent in view of the following detailed description of the invention.

Brief Description Of The Drawings/Figures

[0022] The accompanying drawings, which are incorporated herein and form a part of the specification, illustrate the present invention and, together with the description, further serve to explain the principles of the invention and to enable a person skilled in the pertinent art to make and use the invention.

[0023] FIG. 1 is a block diagram of an environment where one or more tag readers communicate with one or more tags, according to an embodiment of the present invention.

[0024] FIG. 2 is a block diagram illustrating an architectural overview of communication between one ore more readers and one or more tags, according to an embodiment of the present invention.

[0025] FIG. 3A is a block diagram of an illustrative tag according to an embodiment of the present invention.

[0026] FIG. 3B illustrates an example unique tag identification number.

[0027] FIG. 4 is a state diagram illustrating various operating states of an RFID tag, according to an embodiment of the present invention.

[0028] FIG. 5 shows a flowchart providing example steps for a reader to communicate with a population of RFID tags with improved security using bit scrolling, according to an example embodiment of the present invention.

[0029] FIG. 6 shows a signal diagram representing an example communication between a reader and tag, according to an example embodiment of the present invention.

[0030] FIG. 7 shows an example tag that includes a second storage element for storing the bit pattern of a second key, according to an embodiment of the present invention.

[0031] FIG. 8 shows an example tag that includes a random bit pattern generator, according to an example embodiment of the present invention.

[0032] FIGS. 9A and 9B show flowcharts providing example steps for a tag to communicate with a RFID reader with improved security, using a second key, according to example embodiments of the present invention.

[0033] FIGS. 10A and 10B show flowcharts providing example steps for a reader to communicate with a population of RFID tags with improved security, using a second key, according to example embodiments of the present invention.

[0034] The present invention will now be described with reference to the accompanying drawings. In the drawings, like reference numbers indicate identical or functionally similar elements. Additionally, the left-most digit(s) of a reference number identifies the drawing in which the reference number first appears.

Detailed Description Of The Invention

Tag Interrogation Environment

[0035] Before describing the present invention in detail, it may be helpful to describe an example environment in which the invention may be implemented. This example environment is shown for illustrative purposes, and the present invention is not limited to this environment. FIG. 1 illustrates an environment

100 where one or more RFID tag readers 104 communicate with an exemplary population of RFID tags 120, according to the present invention. As shown in FIG. 1, the population of tags 120 includes seven tags 102a-102g. According to embodiments of the present invention, a population of tags 120 may include any number of tags 102. In some embodiments, a very large numbers of tags 102 may be included in a population of tags 120, including hundreds, thousands, or even more.

[0036] Exemplary environment 100 also includes one or more readers 104. These readers 104 may operate independently or may be coupled together to form a reader network, as shown in FIG. 2. A reader 104 may be requested by an external application to address the population of tags 120. Alternatively, the reader may have internal logic that initiates communication. When the reader is not communicating with the population of tags, the reader 104 typically does not emit RF energy. This allows other readers to act upon the same population of tags, but from a different orientation, so as to achieve as complete of coverage with RF signals into the entire population of tags as possible. In addition, the same reader may act upon the same population of tags using a different frequency to increase tag coverage.

[0037] According to the present invention, signals 110 and 112 are exchanged between a reader 104 and the tags 102 according to one or more interrogation protocols. An exemplary interrogation protocol is the binary tree traversal protocol described below. Signals 110 and 112 are wireless signals, such as radio frequency (RF) transmissions. Upon receiving a signal 110, a tag 102 may produce a responding signal 112 by alternatively reflecting and absorbing portions of signal 110 according to a time-based pattern or frequency. This technique for alternatively absorbing and reflecting signal 110 is referred to herein as backscatter modulation. The present invention is also applicable to RFID tags that communicate in other ways.

[0038] FIG. 2 is a block diagram of an example RFID system 200 providing communications between one or more readers 104 and tags 102, according to an embodiment of the present invention. RFID system 200 includes a user application domain 290, a network of readers 104a-n, and one or more tags 102. Note that the invention is applicable to a single reader, as well as to a plurality of readers coupled in a network, as shown in FIG. 2. Hence, although "reader" is often referred to herein, it should be understood that the present invention is applicable to any number of readers in any configuration as required by a particular application.

[0039] Each reader 104 communicates with a tag 102 via one or more antenna(e) 210. A variety of antenna configurations are available. For example, in an embodiment, reader 104a can be directly connected to up to four antennas (e.g., antennas 210a-210d). In another example embodiment, reader 104b is coupled to and controls a multiplexer. A multiplexer allows for a greater number of antennas to be switched to a single antenna port of the reader. In this way reader 104b may accommodate a greater number of antennae.

[0040] User application domain 290 may include one or more user applications. User applications may communicate with one or more readers 104 via a communications network or data link. A reader may receive requests regarding one or more tags 102 from the user application domain 290. For example, an application may request a reader 104 to interrogate a population of tags.

[0041] As will be appreciated by persons skilled in the relevant art(s), the present invention can be implemented on a variety of reader platforms and reader network configurations.

Example Tag Embodiments

Structural Overview

[0042] FIG. 3A is a block diagram of a tag 102, according to an example embodiment of the present invention. Tag 102 includes a RF interface portion 310, a state machine 320, a data storage section 330, and an antenna 345. Data storage section 330 may include one or more memory elements as required by a particular application. Data storage section 330 stores information used by tag 102 to communicate with reader 104. In an embodiment, information stored in data storage module 330 includes a storage element 332.

[0043] In accordance with such an embodiment, each tag 102 is identified by a key, which is typically a unique identification number. The bit pattern of the unique tag identification number may be permanently stored or may be temporarily stored in storage element 332 of data storage section 330. FIG. 3B depicts an example of the layout of a unique tag identification number 350. Each unique tag identification number 350 has embedded tag identification bits 354 and error detection code bits 358. For example, each unique tag identification number may have a ninety-six (96) bit identification number and a 16-bit error detection code value. However, the present invention is applicable to other tag identification number lengths and error detection code lengths. Throughout this document, the embedded tag identification number 350 is referred to as the tag identification number.

[0044] RF interface portion 310, together with one or more tag antennas 345, provides a bi-directional communications interface with reader 104. RF interface portion 310 receives RF signals from reader 104 through antenna(s) 345 and demodulates the signals into digital information symbols. RF interface portion 310 includes a modulator 340 that modulates digital information symbols into RF signals to be received and interpreted by reader 104. For example, modulator 340

may "backscatter" bits of information onto the RF signal received from reader 104 to respond with information to reader 104.

[0045] State machine 320 may include logic, a processor, and/or other components that control the operation of tag 102. State machine 320 receives demodulated information symbols from RF interface portion 310. State machine 320 also accesses information in data storage section 330 as needed. In an embodiment, state machine 320 is implemented with digital circuitry, such as logic gates. Further details regarding state machine 320 are provided below with reference to FIG. 4.

Operational States of a Tag

[0046] Tag 102 can exist in various operating states. Each of these operating states describes a mode of operation for tag 102. Upon the occurrence of certain events, tag 102 can transition from one operating state to another. For example, upon occurrence of an event, tag 102 can transition from a present operating state, which is the operating state that tag 102 is operating in when the event occurs, to a new operating state, as dictated by the combination of the present operating state and the event.

[0047] Events can be triggered by detection of edges in the transmission from reader 104, by passage of a defined period of time, or by a combination of both edge detection and time passage. Examples of events include master reset event, master dormant event, and a data "NULL."

[0048] FIG. 4 illustrates various operating states in a state diagram for tag 102, according to an embodiment of the present invention. In FIG. 4, each operating state is shown as an oval, and transitions between operating states are shown as connections between the ovals. The transitions are annotated with text that describes a corresponding event.

[0049] The paragraphs below describe the operating states and the respective transitions shown in FIG. 4. These particular states and transitions are presented by way of example only. Additional and alternative operating states, transitions, and transition causing events can be employed without departing from the spirit and scope of the present invention.

[0050] The first state is a dormant state 402. During dormant state 402, tag 102 is largely inactive. Therefore, power is conserved while a tag 102 is in dormant state 402. Tag 102 enters dormant state upon powering up, after receipt of a master dormant event, and at other times described below.

[0051] As shown in FIG. 4, tag 102 transitions from dormant state 402 to calibration state 404 upon a master reset event 452. In an embodiment, tag 102 can only transition to calibration state 404 from dormant state 402. In addition, only a master reset event 452 will result in a transition from dormant state 402. In alternate embodiments, other events may cause transitions from dormant state.

[0052] In calibration state 404, tag 102 initializes its timing circuitry. In an embodiment, in calibration state 404, tag 102 will not generate logical symbols "0," or "1" as they have not yet been defined. Instead, in calibration 4, tag 102 performs an oscillator calibration procedure and a data calibration procedure. The oscillator calibration procedure involves tag 102 receiving multiple oscillator calibration pulses from reader 104, defined herein as edge transition (data) events. Specific timing is provided between edge transition events. Similarly, the data calibration procedure involves tag 102 receiving multiple data calibration pulses from reader 104. Data calibration results in the definition of data symbols used in communication between the reader and the tag.

[0053] As shown in FIG. 4, tag 102 may transition from calibration state 404 to dormant state 402 upon the occurrence of an event 454. In an embodiment, event 454 is defined by the reception of a signal that is not representative of timing signals expected by tag 102. For example, in an embodiment, oscillator calibration signals are defined as 8 pulses of equal length. If the oscillator

calibration pulses received by tag 102 are significantly unequal or not within an expected range of lengths, the pulses may be considered invalid, causing occurrence of an event 454. Hence, when tag 102 receives signals that do not cause successful oscillator calibration or data calibration procedures, event 454 occurs.

[0054] After successful completion of the oscillator calibration procedure, which results in a tuned oscillator, and the data calibration procedure, which results in defined data symbols, tag 102 expects to receive defined data symbols from the reader 104. The data symbols are defined as data "0," data "1," and data "NULL." Master reset and master dormant events may occur at any time, and are immediately processed after occurring.

[0055] After successful completion of the calibration procedures, tag 102 receives a data element from the reader. In a preferred embodiment, the data element is a single bit. For example, receipt of a logical "0" data element directs tag 102 to enter global mode set state 406. Receipt of a logical "NULL" directs tag 102 to enter the tree start state 408, skipping global mode state 406. This receipt of a logical "0" or "NULL" causes tag 102 to ignore its read status, as indicated by the confirmed read flag 334. In this way, the reader can address all tags in a population 120, even tags that have previously been read. However, receipt of a logical "1" directs tag 102 to evaluate a confirmed read flag. In such an evaluation, if the confirmed read flag has been set (i.e., indicating that the tag has already been read), tag 102 transitions to dormant state 402. If the confirmed read flag is not set, tag 102 transitions to global mode set state 406. Thus, by sending a logical "1," the reader can read only those tags that have not been read.

[0056] In an embodiment, tag 102 receives a sequence of bits from reader 104 when in global mode set state 406. When in global mode set state 406, tag 102 accepts and stores serial binary information into registers in a specific predefined order. Global modes are configured in a binary (on or off) configuration. Each bit, as received dynamically from reader 104, programs a register associated with

a mode. The register is associated with a circuit or circuits controlling defined tag functions/modes. In an embodiment of the present invention, defined modes include modulator divisor control, backscatter harmonics limiter control, and backscatter power regulator control.

[0057] Modulator divisor control mode controls the frequency in which modulator 340 of the tag will modulate backscatter. In an embodiment of the present invention, this mode is based on an initial frequency of 2.5 MHz for a data "0" and 3.75 MHz for a data "1." Alternatively, other initial frequencies can be used as would be appreciated by persons skilled in the relevant art(s). Backscatter harmonic limiter mode, when implemented, limits the energy of backscatter harmonics. This limitation reduces the effective emissions from the tag on frequencies above the fundamentals. Backscatter power regulator control mode limits the amount of backscatter power in the fundamental frequency of modulation that is reflected by the antenna attached to the tag.

[0058] As described above, in an embodiment, a tag 102 receives "modes" from the reader 104 in the form of a series of bits. Each mode corresponds to a bit in the series of bits. Thus, a tag recognizes each mode by the location of the corresponding bit in the series of bits. The order of modes in the series of bits can be predefined in the tags during manufacturing of the tags, or can be otherwise defined. Future modes may be defined and assigned to open bits in the sequence, although these can alternatively be defined "on the fly." In an embodiment, the tag will default (power on reset) to the bit value "0" for all modes prior to accepting the first bit in the sequence. In this way, global mode settings are a variable amount of bits. Global modes may be completely omitted in operation if all default values are acceptable for operation.

[0059] Note that in an alternative embodiment, a tag receives a global command from a reader, instead of global mode information. For example, when in a particular state, tag 102 can receive a global command from reader 104. Instead of a bit for each mode (as for global modes), reader 104 transmits an N-bit length

global command to tag 102. For example, the global command can be 8 bits in length, which would provide for 256 possible commands. The commands can be configured to cause tag 102 to perform any operation described elsewhere herein, or otherwise known.

[0060] Tag 102 transitions to tree start state 408 upon receipt of a logical "NULL" data element. During tree start state 408, tag 102 expects a command from reader 104 in the form of a data symbol. In an embodiment, the command is a single bit. For example, receipt of a logical "0" symbol directs tag 102 to enter tree traversal state 410. However, receipt of a logical "1" symbol directs tag 102 to enter mute state 412. In an embodiment, receipt of a logical "NULL" symbol does not effect the state of tag 102 in tree start state.

[0061] When operating in tree traversal state 410, tag 102 transmits its identification number to reader 104 according to a binary traversal protocol that enables reader 104 to quickly interrogate a population of tags 120. An example of a binary traversal protocol is described below.

[0062] Tag 102 may enter mute state 412 from tree traversal state 410 or tree start state 408. For example, tag 102 may enter mute state 412 from tree traversal state after an unsuccessful negotiation of its tag identification number. In mute state 412, tag 102 receives data from reader 104. However, when in mute state 412, tag 102 provides no responses to reader 104. Thus, mute state 412 disables tag 102 from responding to a particular request for an identification number.

[0063] After a successful negotiation of its tag identification number, tag 102 transitions from tree traversal state 410 to command start state 414 upon receipt of a "NULL" symbol from reader 104. A successful negotiation is indicated when tag 102 receives a "NULL" symbol at the tag identification length. During command start mode 414, if a data "0" is received from reader 104, tag 102 enters dormant mode 402. This transition represents a confirmed read of tag 102. Prior to entering dormant state, tag 102 sets the confirmed read flag. This flag then indicates that the tag has been confirmed read by the reader.

[0064] When in command start state 414, if a data "1" is received from reader 104, tag 102 enters command state 416. In an embodiment, receipt of a logical "NULL" symbol does not effect the state of tag 102 in command start state 414.

[0001] Note that during tree traversal operations, one or more tags 102 may be active and in tree traversal state 410, or temporarily inactive and in mute state 412. Any other tags that have been processed (i.e., confirmed read) will be in dormant state 402. Reader 104 may collectively address the full population of tags 120 through implicit instructions. This means that upon receipt of a certain symbol, a tag will determine the instruction based upon its current state. Thus, a tag does not have to receive a complete "explicit" instruction to perform functions, causing less data (e.g., long bit length explicit instructions) to need to be transferred and saving transfer time. For example, reader 104 may send a logical "NULL" symbol to the population of tags. Those tags that are in mute state 412 will transition to tree start state 408. If the "NULL" is received at the bit in the traversal corresponding to the identification number length, then any tag in tree traversal state will transition to command start state 414. If the "NULL" is not received at the bit of the traversal corresponding to the identification number length, then any tag in tree traversal state will transition to mute state 412. Implicit instructions are also used when a fully negotiated tag is in command start state 414 or command state 416 and one or more tags are inactive and in mute state 412.

[0065] When operating in command state 416, tag 102 receives a command from reader 104. The command consists of multiple bits. In an embodiment of the present invention, the command is 8 bits in length, although in other embodiments, the command can have other lengths. Command state 416 allows reader 104 to initiate features and functions on a tag, after the tag has been identified via a successful binary tree traversal. Tag 102 may transition from command state 416 to command mute state 418 upon occurrence of an event 468. In an embodiment, event 468 is defined as the detection of communications errors

within a command or a request for an unknown or disabled function. Tag 102 returns to command start state 414 upon receipt of a logical "NULL" symbol from the reader.

[0066] Command mute state 418 is similar in function to mute state 412. When operating in command mute state 418, tag 102 receives data but does not respond. Tag 102 may return to command start state 414 from command mute state 418 upon receipt of a data "NULL."

Binary Tree Traversal Protocol

[0067] In accordance with an embodiment of the present invention, a binary tree traversal methodology is used in order to establish communication between a reader 104 and one of a population of tags 120 that are within the communication range of the reader. In an embodiment, contention between the tags 102 is avoided by requiring transmissions from each tag 102 to the reader 104 to be unique in a separation of frequency. In alternative embodiments, contentions can be avoided in other ways of communicating. Contention may be defined as communications by multiple transmissions in the same frequency, time, and/or phase that thereby destructively interfere with each other's attempted transmission. Thus, in an example binary traversal algorithm, one bit of information is negotiated at a time between the reader 104 and the current population of tags 102 that the reader is addressing.

[0068] Each tag response is defined by two frequencies, one frequency for a data "0", and the other frequency for a data "1". In such a manner, many tags can simultaneously and non-destructively communicate a data 0. For example, it is not important that the reader cannot differentiate a single data 0 from multiple data 0's, just that there exists a data 0. Alternatively, for example, a tag response may be defined by two time periods, one time period for "0", and the other for "1."

[0069] In an embodiment, the binary tree traversal process eliminates tags from communication until only one tag with a unique number is isolated and verified. As described above, each level in the binary tree represents a bit position in the tag identification number. As the reader proceeds through nodes (and levels) in the binary tree, it directs a subset of the population of tags to remain active and a subset of the population of tags to go inactive. The reader may send out a bit or combination of bits in a signal to cause the tags to begin a binary traversal, as described above. The tags then respond with the first bit of their identification number. The reader then determines which branch of the binary tree to follow. For example, the reader may select a "0" bit as the first bit of interest. The reader transmits the "0" bit. Tags that last sent a "0" bit remain active; those that did not will go inactive. This process continues, where the reader selects one of the "0" and "1" branches of the binary tree. Statistically, on each bit exchange, one half of the tag population will go inactive. This process continues until the reader reaches a node in the last level of the binary tree and results in a unique tag isolation and elimination. This process can be repeated until each tag in the population of tags is isolated.

[0070] For more information concerning binary tree traversal methodology, and, more generally, communication between an RFID reader and a population of RFID tags in accordance with an embodiment of the present invention, see U.S. Patent No. 6,002,544, entitled "System and Method for Electronic Inventory" which is incorporated herein by reference in its entirety, and the following co-pending U.S. Patent Applications, each of which is incorporated by reference herein in its entirety: Application Ser. No. 09/323,206, filed June 1, 1999, entitled "System and Method for Electronic Inventory," Attorney Docket No. 1689.0010001; Application Ser. No. 10/072,885, filed February 12, 2002, entitled "Method, System and Apparatus for Binary Traversal of a Tag Population," Attorney Docket No. 1689.0210001; and Application Ser. No. 10/073,000, filed

February 12, 2002, entitled "Method, System and Apparatus for Communicating with a RFID Tag Population," Attorney Docket No. 1689.0260000.

Example Embodiments of the Present Invention

[0071] The present invention provides for secure communications (i.e., negotiations) between readers and tags. According to the present invention, a reader can communicate with tags on an open-air communication channel, while keeping tag data, such as tag identification numbers, secure.

[0072] According to embodiments of the present invention, binary traversal algorithms, such as described above, can be modified to provide for secure communications between readers and tags. For example, a conventional binary tree traversal algorithm can be modified to provide for the secure negotiations.

[0073] Embodiments of the present invention for communications between readers and tags with improved security are described in detail in the subsections below.

Implied Scroll Embodiments

[0074] According to an embodiment of the present invention, an "implied scroll" is used to provide for improved security during communications between readers and tags. According to this embodiment, a tag "scrolls" by transmitting multiple response bits during a single response interval provided by the reader, instead of the normal single bit response. The reader transmits a substantially constant output signal during which each participating tag scrolls multiple response bits in series to the reader. The reader monitors the scrolling series of response bits from the tag(s), and determines when to terminate the response of the tag(s). The reader can terminate the response of the tag(s) by ending the substantially constant output signal. After ending the response of the tag(s), the reader can transmit one or more subsequent substantially constant output signals to cause

further bit scrolling, and/or can commence the interchange of single bits with the tag(s) through a binary traversal operation.

[0075] In an embodiment, tags can "scroll" or transmit serial streams of bits to the reader in response to an explicit command received from the reader, such as a command bit string. In an alternative embodiment, tags can be caused to scroll bits to the reader by an implied command of the reader. For example, in an embodiment, after the tag transmits a first response bit, the tag waits for a next bit (i.e., a forward link symbol) from the reader. If the tag continues to receive substantially constant/continuous power from the reader for longer than a specific interval, the tag can recognize this as an implicit command to modulate its next response bit back to the reader. The tag can continue to modulate further response bits back to the reader as long as the tag keeps receiving the continuous power signal from the reader. In this manner, a tag can scroll multiple bits to a reader without further intervention from the reader.

[0076] Scrolling can be used to enhance security in various ways. For example, scrolling allows for multiple bits to be transmitted from a tag to the reader for every reader transmitted bit. Because tag bits are transmitted at a lower power, these bits are harder for unwanted third parties to detect. Because fewer reader bits are transmitted during scrolls, there are fewer higher powered bits transmitted that are easier to detect.

[0077] FIG. 5 shows a flowchart 500 providing example steps for a reader to communicate with a population of RFID tags with improved security, using bit scrolling, according to an example embodiment of the present invention. Other structural and operational embodiments will be apparent to persons skilled in the relevant art(s) based on the following discussion. The steps of FIG. 5 are described in detail below, with reference to FIG. 6. FIG. 6 shows a signal diagram 600 representing an example communication between a reader and tag, according to an example embodiment of the present invention.

[0078] Flowchart 500 begins with step 502. In step 502, a first bit is transmitted to the population of tags. For example, the first bit can be transmitted by the reader to begin a binary traversal, or can be any bit within a binary traversal tree. For example, FIG. 6 shows an example first reader bit 602 transmitted by a reader. In the example of FIG. 6, first reader bit 602 is represented by a low signal transmitted by the reader for specific period of time. For illustrative purposes, the signal shown transmitted by the reader in FIG. 6 is shown in logical form, without a carrier frequency, etc.

[0079] In step 504, a substantially constant signal is transmitted to the population of tags. For example, as shown in FIG. 6, a substantially constant RF output is provided by the reader, shown as substantially constant signal portion 604.

[0080] In step 506, a plurality of bits are received from a first tag during transmission of the substantially constant signal. For example, as shown in FIG. 6, a first tag response is shown as first tag response 606a (shown in FIG. 6 as modulating substantially constant signal portion 604 with three cycles of a response backscatter frequency). For instance, first tag response 606a is a normal response of a tag during a binary traversal after receiving a reader bit, first reader bit 602. As shown in FIG. 6, the tag waits a specific time interval 608a from responding with first tag response 606a (or from any other reference point). After specific time interval 608a expires, the tag responds (i.e., scrolls) with a next bit, second tag response 606b. The tag makes this response due to the implied command from the reader, which merely maintains substantially constant signal portion 604. In a likewise manner, after expiration of a second specific time interval 608b, the tag responds (i.e., scrolls) with still another bit, third tag response 606c. Once again, the tag makes this response due to the implied command from the reader, which merely maintains substantially constant signal portion 604.

[0081] In step 508, transmission of the substantially constant signal to the population of tags is terminated to end transmission of the plurality of bits from

the first tag. For example, as shown in FIG. 6, substantially constant signal portion 604 is terminated at point 610. Thus, since another specific time interval 608 did not expire between third tag response 606 and point 610, the tag understands this as the implied command to stop scrolling out response bits. After point 610, the reader can transmit a next reader bit 602 to direct the population of tags down another branch of the binary tree, issue a command, or do any other reader function.

[0082] In an embodiment, the length of an interval 608 that a tag waits before modulating a next response bit back to the reader can be set in various ways. For example, the length of the interval 608 can be preprogrammed into the tag. Alternatively, an interval 608 can be defined in a training/synchronization sequence transmitted from the reader to the tag during operation.

[0083] Such an implied scroll procedure can be useful to enhance binary traversals of tag populations. For example, a length of time required to perform a binary traversal can be reduced. For instance, in an embodiment, during a binary traversal, a reader can transmit bits at nodes in a binary tree where the reader knows that both the "0" and "1" branches of the tree from the node are populated with tags. At other nodes, the reader can allow the tag(s) to scroll bits. If the reader receives both "0" and "1" responses simultaneously from tags, then the reader can terminate the scroll by transmitting a bit that directs which branch the binary traversal at this binary tree "fork" will take. Because binary trees are frequently sparsely populated, an ID number having a large number of bits (e.g., such as 80 bits) can be isolated by the reader only having to transmit much fewer bits (e.g., 3 or 4 bits) to resolve bit collisions/forks in the binary tree, and scrolling through the remaining nodes of the binary tree.

[0084] Note that in an embodiment, a reader may have a limit on how many bits it will allow to scroll continuously before terminating the current bit scroll. For example, the number of scroll bits may be limited in order to keep the reader and tags synchronized. In another example, the number of scroll bits may be limited

so tags do not confuse the continuous signal from the reader with other signals that can be sent by a reader, such as a master reset signal, etc. Thus, for example, scrolls may not be allowed to proceed through more than 10 or 12 bits at a time. For an example 80 bit ID number, scrolling 10 bits at a time will still only require that around 12 percent of the ID number be broadcast from the reader, thus speeding up a binary traversal operation (where all 80 bits are broadcast). Furthermore, in this manner, the tag ID numbers are kept more secret from an undesired third party.

Frequency Hopping and Spread Spectrum Embodiments

[0085] As described above, it is possible for an unwanted third party to fool or "spoof" a reader into revealing complete tag ID numbers. The unwanted third party can transmit a false tag response to cause bit collisions and thus force the reader to transmit bits to resolve the collision. The unwanted third party receives the bits from the reader, and sends out false response signals multiple times to piece together one or more ID numbers of the tag population. Given enough time, the unwanted third party could potentially "spoof out" the entire tag population binary tree.

[0086] Readers that transmit at ultra high frequencies (UHF) can use a frequency hopping spread spectrum approach to mitigate multi path nulls and interference from other readers. Thus, an unwanted third party attempting to spoof a RFID system will have to follow along with the reader frequency hops. If the reader uses a pseudo-random hop sequence, it may be relatively easy for the unwanted third party to follow the reader frequency hops. If the reader uses a true random frequency hop sequence, it is difficult, if not impossible for the unwanted third party to follow the frequency hops. If there are many readers operating simultaneously to negotiate populations of tags, then any one channel, or any sequence of channels that the unwanted third party may select, will contain a

random interleaving of incomplete tree data. Thus, the unwanted third party will be unable to extract meaningful information in a reasonable amount of time.

[0087] For RFID systems that desire improved security but use only one or a few readers, the random frequency hop technique will not be as robust. In an embodiment, to provide an improved system, a reader can transmit a direct sequence spread spectrum signal. In a preferred embodiment, the direct spreading sequence is random. Similarly to the tags, an unwanted third party could listen in on the reader transmission (i.e., the forward link) with a wide band receiver. To spoof a tag, the exact spreading sequence must be known by the unwanted third party before the transmission of the reader is received. The unwanted third party will most likely be receiving and transmitting at a relatively great distance. Thus, even if the unwanted third party can receive the reader transmissions and quickly transmit a modulated replica, the phase shift caused by the propagation delay will likely prevent the reader from de-spreading the unwanted third party's spoofing signal properly. As a result, the spoofing signal will be spread over a wider band than a true tag response, and will be ignored.

[0088] In embodiments, depending on the particular situation, random frequency hopping, random direct sequence spread spectrum, or a hybrid approach can be used to provide robust data protection.

Binary Traversal Embodiments without Application Data

[0089] In another embodiment of the present invention, a binary tree traversal provides for improved security. According to the present embodiment, a binary number of a tag, other than the tag identification number, is used for negotiating a binary traversal. Furthermore, this binary number, or "second key," contains no application data. In other words, the binary number returned to the reader by the tag does not contain information that can be correlated with, or can be used to identify the object to which the tag is associated. By not transmitting application

data to the reader, a tag singulation (i.e., isolation of a single tag) by the reader can occur with security maintained over any information about the item to which the tag is attached. In embodiments, several types of binary numbers can be used in tags to provide varying degrees of security, with different performance tradeoffs.

[0090] Typically, tag ID numbers (i.e., the first key) that are to be negotiated in a binary traversal are required to be unique for all possible tagged items over a period of time. This can entail a lengthy bit sequence to cover uniqueness for large numbers of items, including even trillions of items worldwide. Negotiating such a large number of bits required for tag uniqueness can take a relatively long period of time.

[0091] Typically, however, a particular reader is not capable of powering and/or reading more than a particular number of passive tags. The number of tags that can be powered by a particular reader depends on a tag broadcast power, a distance from the reader to the tags, and other factors. In an example situation, a reader can power about 2000 passive tags, which can be covered by an 11 bit binary string (i.e., 2048 unique values). Hence, in such a situation, it would not be efficient to attempt to always read a complete ID number, such as a 112 bit identification number, for example (e.g., 96 bits ePC plus 16 bits CRC) every time. Statistically, in the present example, there is only a need for 11 bits to accommodate tag uniqueness within the reader field. In embodiments, however, further bits than the minimum may be used for various reasons, such as for error correction, etc.

[0092] According to the present invention, a reader singulates a tag using the bit pattern of a second key. Subsequently, the tag can transmit to the reader its relatively lengthy identification number or item key (e.g., ePC or similar) (i.e., first key), which often contains information about the item the tag is attached to. However, this transmission only has to be done once, as the two keys can be associated in the reader or the host system for future identification. Thus, in such

an embodiment, the second key is shorter than the first key. Note, however, in alternative embodiments, as described below, the second key can be the same length as or longer than the first key. FIG. 7 shows an example tag 700 that includes a second storage element 702 for storing the bit pattern of the second key, according to an embodiment of the present invention.

[0093] The second key can include a single bit pattern, or plurality of combined bit patterns. According to an example embodiment of the present invention, encoding of the second key is broken up into several portions or sections. Each section provides additional uniqueness. For example, a first portion is used as a minimum level of statistical uniqueness in the expected population of tags. For instance, in an expected population of 1024 tags, 10 bits for a first portion is an absolute minimum. Furthermore, additional bits can be added for probability and error detection schemes. Hence, for an example population of 1024 tags, 16 – 24 bits may be used in the first portion. In many cases, a broadcast of this many bits in such a tag population would result in isolation of a single tag. If it is determined that transmission of this many bits does not isolate a tag, then a second portion of the second key can be negotiated, and so on until isolation of a tag is obtained.

[0094] In further example embodiments, the second key can be implemented as follows:

[0095] (A) A simple sequence number: A first tag is assigned a binary number 1 as the second key, a second tag is assigned a binary number 2 as the second key, and so on. These numbers could be assigned when the tags are manufactured, or at any time later. Such a number could be stored in storage 702, such as shown in FIG. 7, for example. However, second keys assigned in the manner may yield information about the tags if detected by an unwanted third party. This is because a range of numbers assigned to a particular population of tags may be known (e.g., by the unwanted third party) to have been produced in a certain date range, or sold for a specific purpose. Thus, knowing such information about the tags,

and having determined the numbers assigned to the tags by eavesdropping, an unwanted third party may be able to deduce information about the objects to which the tags are associated. Thus, although this is a relatively simple solution, some information about the items to which the tags are attached may be undesirably gained through eavesdropping measures.

[0096] (B) Randomly generated static numbers: A random, fixed number may be stored in a tag as the second key. Such a number could be stored in storage 702, such as shown in FIG. 7, for example. The use of such a randomly generated static number avoids the type of eavesdropping described in (A) above. However, an overall number of tagged items in the locality may be obtained by an eavesdropping third party. For example, the unwanted third party could eavesdrop, and record all of the random, fixed numbers assigned to the tags in the local population that are broadcast. The unwanted third party could then compare the recorded values with previous entries obtained by the eavesdropper to determine an estimate, or exact count, of the number of tagged objects present. Thus, this solution is better at keeping the identity of items secure, while possibly allowing an unwanted third party to determine the number of items present.

[0097] Note that the second key can be assigned to be a fixed pseudo-random number. Preferably, the second key is assigned a bit pattern that is non-correlated with the bit pattern of the first key. For example, the second key can be assigned a bit pattern that includes bits corresponding to a location on the wafer in which the integrated circuit chip of the RFID tag was formed. For example, the bit pattern could include bits indicating an X-Y location of the chip on the wafer, or a number of the chip in the wafer. The bit pattern could further include a unique number corresponding to the particular wafer from the chip was removed, to further correlate the second key with the wafer. In another example, the bit pattern of the second key can include bits corresponding to a time stamp, such as a time that the tag was manufactured, a time that the chip was produced, or other relevant time stamp. In another example, the bit pattern of the second key could

include a portion of the bit pattern of the first key. For example, the second key could include bits of the identification number of the tag. In another example, the bit pattern of the second key could include cyclic redundancy check (CRC) processed bits related to the tag, and/or bits processed according to any other error checking algorithm. In another example, bits of the second key could be hashed according to a hashing code. In further embodiments, any combination of these bit patterns can be used in the second key, along with any other bit pattern(s), as desired.

[0098] (C) Dynamically generated numbers: The use of dynamically generated numbers for each tag is relatively even more secure against eavesdropping and spoofing. In this embodiment, the second key can be changed each time the population of tags is negotiated or addressed in a binary traversal operation. Because of this, an outside eavesdropping system could not tell whether a new second key transmitted by a tag applies to a new item, or to an existing item that is being read again with a new second key. Thus, in this embodiment, the number of items present cannot be readily determined, as in the embodiment of (B) described above.

[0099] FIG. 8 shows an example tag 800 that includes a random number generator or random bit pattern generator 802, according to an example embodiment of the present invention. In an embodiment, random bit pattern generator 802 can generate a random number or bit pattern for the second key having a known fixed length, or alternatively, can generate a random number of any length, as dictated by the reader. Thus, in some embodiments, tags can have a flexible bit length second key, as determined by the reader. In this manner, the reader can cause the tag to respond with any numbers of bits, including bits the 1s, 10s, 100s, 1000s, and any other length ranges, until the reader decides to request no further bits.

[0100] Furthermore, in an embodiment, the second key generated by random bit pattern generator 802 can be stored in a second storage element 804, when

present. Alternatively, in an embodiment, the second key is not stored, and is transmitted by the tag bit-by-bit as it is generated by random bit pattern generator 802. Thus, in such an embodiment, second storage element 804 is not present. Such an embodiment is useful when a tag transmits a different second key each time it is negotiated, and/or transmits a second key with variable length. Any type of random bit pattern generator can be used for random bit pattern generator 802, including an oscillator, a combination of logic gates, or other type of random bit pattern generator known to persons skilled in the relevant art(s).

[0101] A tradeoff with using a dynamically generated number is that in order for the reader to know what item a tag is attached to, after reading the second key, the first key of the tag must be read. However, because the tag was already isolated using the secure second key, the reader can transmit a command to the tag to transmit the first key (e.g., identification number) to the reader, rather than the reader transmitting the first key to the tag, as during a normal binary traversal. Thus, only the response of the tag, such as a backscatter type response, will contain the first key.

[0102] The approach of (C) above solves several problems. For example, when negotiating using a bit to bit approach, such as in a binary tree traversal, information in the first key is essentially broadcast on the reader transmit channel (i.e., forward link), which is a relatively high powered channel (i.e., high power is required to activate the passive tag). Such a signal may be easily eavesdropped upon from a fairly long distance (hundreds of feet). After repeated scans of a tag population by readers, random noise, or inserted noise (spoofing), can eventually cause all or a significant portion of the first keys of the tags to be transmitted on the forward link. However, in an embodiment, the present invention provides that the first key is not transmitted by the reader in the forward link. Instead, the second key, which can be much shorter than the first key, and can be devoid of item related information (i.e., is non-correlated to the attached object), is transmitted by the reader in the forward link. If desired, the reader can then have

the singulated tag transmit its first key in the "backward" link (i.e., tag to reader). Because the responses of a tag are much lower power than transmissions of a reader, the responses are much more difficult for an unwanted third party to eavesdrop in on. Thus, even though the tag transmits the first key to the reader, this backward link transmission is much more difficult to detect, allowing for improved security over having the reader transmit the first key in the forward link.

[0103] Another problem solved by the present invention is related to the number of bits required to be communicated between readers and tags. According to the present invention, the number of bits negotiated between tag and reader (i.e., the second key) can be substantially less than the item identification number (i.e., first key). Once the reader has obtained the first key from the tag, the reader can address the tag using the second, shorter, key, until a new second key is generated by the tag. In embodiments, the reader can send a command to the tag to respond with a new second key. Alternatively, the tag can always respond with a newly generated second key, or can respond with a newly generated second key after every N interrogations, where N is greater than or equal to 1.

[0104] By addressing a tag with a second key that is shorter than the first key, communications can occur much faster. As described above, typically a tag only needs to be unique within the field of a reader, so really only needs a key much shorter than the first key. The first key can provide uniqueness worldwide and can be over 100 bits. Uniqueness in the field of the reader likely requires fewer bits. By resolving tag reads based on minimal number of bits according to the present invention, the speed of performance is increased on tags that need continued monitoring, such as in an automated inventory system. Higher system performance can result in faster overall inventory scans, which can detect inventory changes faster.

[0105] Item level information that is of security concern (i.e., first key information) is not transmitted as part of the tag negotiation process of the present invention because a non-correlated second key is instead used.

[0106] Thus, advantages of the present invention include providing the capability to read item identification numbers securely, from a reader transmit/broadcast perspective. Additionally, in static applications (such as inventory), much better efficiency can be obtained using the shorter second key, while keeping item identification numbers (i.e., first keys) private from competitors or other unwanted third parties.

[0107] FIG. 9A shows a flowchart 900 providing example steps for a tag to communicate with a RFID reader with improved security, according to an example embodiment of the present invention. In the example of flowchart 900, the example tag stores an identification number (i.e., a first key) which is defined by a first bit pattern. Other structural and operational embodiments will be apparent to persons skilled in the relevant art(s) based on the following discussion. The steps of FIG. 9A are described in detail below.

[0108] Flowchart 900 begins with step 902. In step 902, a first at least one bit is received from the reader. The first at least one bit causes the tag to respond to a binary traversal operation with a second bit pattern. The first at least one bit can be any bit or combination of bits to cause tags to respond with the second key. This can amount to a state transition by the tag, or other tag algorithm change.

[0109] In step 904, a binary traversal operation is engaged with the reader, wherein the tag responds during the binary traversal operation with the second bit pattern. Thus, as described above, the tag communicates with the reader, responding to the reader with bits of the second key. The tag can be singulated in this manner.

[0110] Steps 906, 908, 910, and 912 are optional, according to further example embodiments of the present invention.

[0111] In step 906, at least one bit is received from the reader to cause the first tag to transmit its identification number. For example, as described above, once the tag is singulated, the reader may desire to read the identification number, first key, of the tag, in order to identify the object to which the tag is attached. Thus,

the reader can use any mechanism to cause the tag to respond with bits of the first key.

[0112] In step 908, the identification number is transmitted.

[0113] In step 910, a command is received from the reader. For example, as described above, once the tag is singulated, the reader may desire to command the tag to execute any operation that the tag is capable of, such any command/operation as described elsewhere herein, or otherwise known.

[0114] In step 912, the command is executed.

[0115] FIG. 9B shows example steps for step 904. As shown in the embodiment of FIG. 9B, step 904 can include steps 914 and 916.

[0116] In step 914, a series of bits is received from the reader. For example, as described above, the reader transmits bits to the tag.

[0117] In step 916, each bit of the series of bits is responded to with a corresponding bit of the second bit pattern. For example, the tag compares each received bit with the previous transmitted bit of the tag's second key (or in alternative embodiments, compares each received bit with the next bit of the tag's second key). If they match, the tag transmits the next bit of the second key.

[0118] In an embodiment, step 904 can include the step where the next bit of the second bit pattern is read from storage in the tag. For example, the storage can be second storage element 702 or 804, which stores the second key.

[0119] In another embodiment, step 904 can include the step where the next bit of the second bit pattern is randomly generated. For example, the bit values can be generated by a random bit pattern generator, such as random bit pattern generator 802 shown in FIG. 8. The generated bit values can be stored in storage 804, or alternatively, are not stored, but are immediately transmitted by the tag to the reader in response to the binary traversal operation. Thus, in a subsequent binary traversal operation, the tag would newly generate each bit of the second bit pattern.

[0120] FIG. 10A shows a flowchart 1000 providing example steps for a reader to communicate with a population of RFID tags with improved security, according to an example embodiment of the present invention. In the example of flowchart 1000, each tag of the population of tags stores a corresponding identification number (i.e., a first key) which is defined by a first bit pattern. Other structural and operational embodiments will be apparent to persons skilled in the relevant art(s) based on the following discussion. The steps of FIG. 10A are described in detail below.

[0121] Flowchart 1000 begins with step 1002. In step 1002, a first at least one bit is transmitted to the population of tags to cause tags to respond to a binary traversal operation with a second bit pattern. The first at least one bit can be any bit or combination of bits to cause tags to respond with the second key.

[0122] In step 1004, a binary traversal operation is performed to singulate a first tag of the population of tags.

[0123] Steps 1006, 1008, and 1010 are optional, according to further example embodiments of the present invention.

[0124] In step 1006, the first tag is caused to transmit its identification number.

[0125] In step 1008, the identification number of the first tag is received.

[0126] In step 1010, a command is transmitted for execution by the first tag.

[0127] FIG. 10B shows example steps for step 904, according to an example embodiment of the present invention. As shown in the embodiment of FIG. 10B, step 1004 can include steps 1012 and 1014.

[0128] In step 1012, a series of bits is transmitted to the population of tags.

[0129] In step 1014, a corresponding bit of the second bit pattern is received from the first tag in response to each bit of the series of bits. Note that many tags of the population of tags may be responding to bits of the series of bits transmitted by the reader. However, eventually, only a single tag will respond, becoming the singulated tag.

[0130] In an embodiment, in step 1010, the reader transmits a predetermined number of bits. For example, the number of bits may be predetermined to be sufficient to identify tags within a communication range of the reader. For example, as described above, to negotiate 1024 tags, 10 bits are required for uniqueness. Thus, the reader may transmit 10 or more bits in the series of bits. Note that in embodiments, however, there is no limit on the number of bits a reader may transmit in the series of bits, including in the 1s, 10s, 100s, and 1000s of bits, to singulate a tag.

[0131] For example, in the example where the tag population includes 1024 tags, 16 bits may be chosen as the length of the second key for the tags. Thus, in this example, the reader could transmit 16 bits to likely singulate a tag. However, in this example, the reader could transmit fewer than 16 bits if it is predetermined that fewer than 16 bits will identify a single tag within communication range. Alternatively, the reader may desire to transmit bits additional to 16 bits to singulate a tag, in embodiments where tags are configured to have flexible bit lengths for the second key.

Further Embodiments

[0132] The systems and methods described above for improved security during RFID negotiations can be combined in any manner, as desired for a particular application. For example, in an embodiment, a reader may negotiate a population of tags. The tags may be instructed by the reader to respond with a second bit pattern during the negotiation that is not correlated with their identification number (e.g., their EPC number). The reader may negotiate the population of tags using a binary traversal. Once the reader singulates a tag, the reader can use the implied scroll function to cause the tag to send its identification number to the reader. Thus, this embodiment provides enhanced security because a non-correlated number is negotiated, and because the tag identification number is sent

to the reader on the "backward" link, which is lower power. Furthermore, such a singulation of a tag, and receipt of the tag's identification number can occur very rapidly. Because during the implied scroll, a reader does not transmit edges, and therefore the tag does not have to wait for edges, the identification number of the tag can be scrolled to the reader very rapidly. For instance, in an example embodiment, the tag can transmit its identification number (or other information) during an implied scroll three times faster than communications can occur during a binary traversal.

[0133] Further combinations of the embodiments described herein are also within the scope and spirit of the present invention, as would be understood by persons skilled in the relevant art(s) from the teachings herein.

Conclusion

[0134] While various embodiments of the present invention have been described above, it should be understood that they have been presented by way of example only, and not limitation. It will be apparent to persons skilled in the relevant art that various changes in form and detail can be made therein without departing from the spirit and scope of the invention. Thus, the breadth and scope of the present invention should not be limited by any of the above-described exemplary embodiments, but should be defined only in accordance with the following claims and their equivalents.

WHAT IS CLAIMED IS:

1. A method for a radio frequency identification (RFID) tag to communicate with a RFID reader, wherein the tag stores a corresponding identification number, wherein the identification number comprises a first bit pattern, comprising:

(a) receiving a first at least one bit from the reader to cause the tag to respond to a binary traversal operation with a second bit pattern;

(b) engaging in a binary traversal operation with the reader, including the steps of:

(1) receiving a series of bits from the reader, and

(2) responding to each bit of the series of bits with a corresponding bit of the second bit pattern.

2. The method of claim 1, wherein step (b) comprises:

reading the second bit pattern from storage in the tag.

3. The method of claim 1, wherein step (b) comprises:

randomly generating a bit value for each bit of the second bit pattern.

4. The method of claim 3, further comprising:

(c) storing the second bit pattern.

5. The method of claim 4, further comprising:

(d) engaging in a second binary traversal operation with the reader, including the steps of:

(1) receiving a second series of bits from the reader, and

(2) responding to each bit of the series of bits with a corresponding bit of the stored second bit pattern.

6. The method of claim 3, further comprising:

(d) engaging in a second binary traversal operation with the reader, including the steps of:

(1) receiving a second series of bits from the reader, and

(2) responding to each bit of the series of bits with a second randomly generated bit value.

7. The method of claim 1, further comprising:

(c) receiving at least one bit from the reader to cause the first tag to transmit its identification number; and

(d) transmitting the identification number.

8. The method of claim 1, further comprising:

(c) receiving a command from the reader; and

(d) executing the command.

9. A radio frequency identification (RFID) tag, comprising:

an antenna;

a modulator coupled to said antenna, wherein said modulator is configured to backscatter modulate bits received from said antenna with response bits;

a first storage that stores a first bit pattern that defines an identification number; and

a second storage that stores a second bit pattern that does not include bits identifying an item with which the RFID tag is associated;

wherein a first bit combination received from a reader causes said tag to respond to a binary traversal with the first bit pattern; and

wherein a second bit combination received from the reader causes said tag to respond to a binary traversal with the second bit pattern.

10. The RFID tag of claim 9, wherein said second bit pattern is a random bit pattern.

11. The RFID tag of claim 10, further comprising:
a random bit pattern generator that generates said second bit pattern.

12. The RFID tag of claim 11, wherein said random bit pattern generator comprises an oscillator.

13. The RFID tag of claim 9, wherein said second bit pattern is non-correlated with said first bit pattern.

14. The RFID tag of claim 9, wherein said second bit pattern is a fixed bit pattern.

15. The RFID tag of claim 9, wherein said second bit pattern includes bits corresponding to a location on wafer for an integrated circuit chip of the RFID tag.

16. The RFID tag of claim 9, wherein said second bit pattern includes bits corresponding to a time stamp.

17. The RFID tag of claim 9, wherein said second bit pattern includes a portion of the first bit pattern.

18. The RFID tag of claim 9, wherein said second bit pattern includes hashed bits from the first bit pattern.

19. A method for a radio frequency identification (RFID) tag to communicate with a RFID reader, wherein the tag stores a corresponding identification number, comprising:

(a) receiving a first at least one bit from the reader to cause the tag to respond to a binary traversal operation with a key;

(b) engaging in a binary traversal operation with the reader, including the steps of:

(1) receiving a series of bits from the reader, and

(2) responding to each bit of the series of bits with a randomly generated bit of the key.

20. A radio frequency identification (RFID) tag, comprising:

an antenna;

a modulator coupled to said antenna, wherein said modulator is configured to backscatter modulate bits received from said antenna with response bits;

a storage that stores a bit pattern that defines an identification number; and

a random bit pattern generator that generates said second bit pattern;

wherein a first bit combination received from a reader causes said tag to respond to a binary traversal with the first bit pattern; and

wherein a second bit combination received from the reader causes said tag to respond to a binary traversal with bits generated by said random bit pattern generator.

21. A method for a radio frequency identification (RFID) reader to communicate with a population of RFID tags, wherein each tag stores a corresponding identification number, wherein the identification number comprises a first bit pattern, comprising:

(a) transmitting a first at least one bit to the population of tags to cause tags to respond to a binary traversal operation with a second bit pattern;

(b) performing a binary traversal operation to singulate a first tag of the population of tags, including the step of:

(1) transmitting a series of bits to the population of tags, and

(2) receiving a corresponding bit of the second bit pattern from the first tag in response to each bit of the series of bits.

22. The method of claim 21, further comprising:

(c) after step (b), causing the first tag to transmit its identification number.

23. The method of claim 21, further comprising:

(c) after step (b), transmitting a command for execution by the first tag.

24. The method of claim 21, wherein the series of bits includes a number of bits predetermined to be sufficient to identify tags within a communication range of the reader, wherein step (1) comprises:

transmitting the predetermined number of bits to the population of tags.

25. A method in a radio frequency identification (RFID) system the includes at least one RFID reader that communicates with a population of RFID tags, wherein each RFID tag stores a corresponding identification number, comprising:

generating a key to identify an RFID tag of the population of RFID tags, wherein the key does not include bits identifying an item with which the RFID tag is associated;

operating a binary tree algorithm to at least identify the RFID tag in the population of RFIDs tags; and

receiving bits of the generated key from the RFID tag during the binary tree algorithm.

26. The method of claim 25, wherein said generating step includes the step of: selecting a number from a sequence of numbers to use as the key.

27. The method of claim 25, wherein said generating step includes the step of: using a randomly generated number as the key.

28. The method of claim 25, wherein said generating step includes the step of: dynamically generating a number prior to each traversal of the population of RFID tags to use as the key.

29. A method for a radio frequency identification (RFID) reader to communicate with a population of RFID tags, wherein each tag stores a corresponding identification number, wherein the identification number includes a first bit pattern, comprising:

(a) transmitting a first at least one bit to the population of tags to cause tags to respond to a binary traversal operation with a second bit pattern;

(b) performing a binary traversal operation to singulate a first tag of the population of tags;

(c) transmitting a substantially constant signal to the population of tags; and

(d) receiving a plurality of bits of the first bit pattern from the first tag during transmission of the substantially constant signal.

30. The method of claim 29, further comprising:

(e) terminating transmission of the substantially constant signal to the population of tags to stop the first tag from transmitting further bits of the first bit pattern.

31. The method of claim 30, further comprising:

(f) transmitting a second substantially constant signal to the population of tags;

(g) receiving a second plurality of bits of the first bit pattern from the first tag during transmission of the second substantially constant signal; and

(h) terminating transmission of the second substantially constant signal to the population of tags to stop the first tag from transmitting further bits of the first bit pattern.

32. The method of claim 31, further comprising:

(i) repeating steps (f)-(h) for subsequent substantially constant signals.

33. A method in a radio frequency identification (RFID) system the includes at least one RFID reader that communicates with a population of RFID tags, wherein each RFID tag stores a corresponding identification number, comprising:

(a) generating a bit to identify an RFID tag of the population of RFID tags, wherein the bit does not include bits identifying an item with which the RFID tag is associated;

(b) operating a binary tree algorithm to at least identify the RFID tag in the population of RFIDs tags;

(c) receiving the generated bit from the RFID tag during the binary tree algorithm; and

(d) repeating steps (a)-(c) until the RFID tag is singulated.

34. A method for a radio frequency identification (RFID) reader to communicate with a population of RFID tags, wherein each tag stores a corresponding identification number, wherein the identification number includes a first bit pattern, comprising:

(a) transmitting a first at least one bit to the population of tags to cause tags to respond to a binary traversal operation with the first bit pattern;

(b) transmitting a substantially constant signal to the population of tags; and

(c) receiving a plurality of bits of the first bit pattern from a first tag during transmission of the substantially constant signal.

35. The method of claim 34, further comprising:

(d) terminating transmission of the substantially constant signal to the population of tags to stop the first tag from transmitting further bits of the first bit pattern.

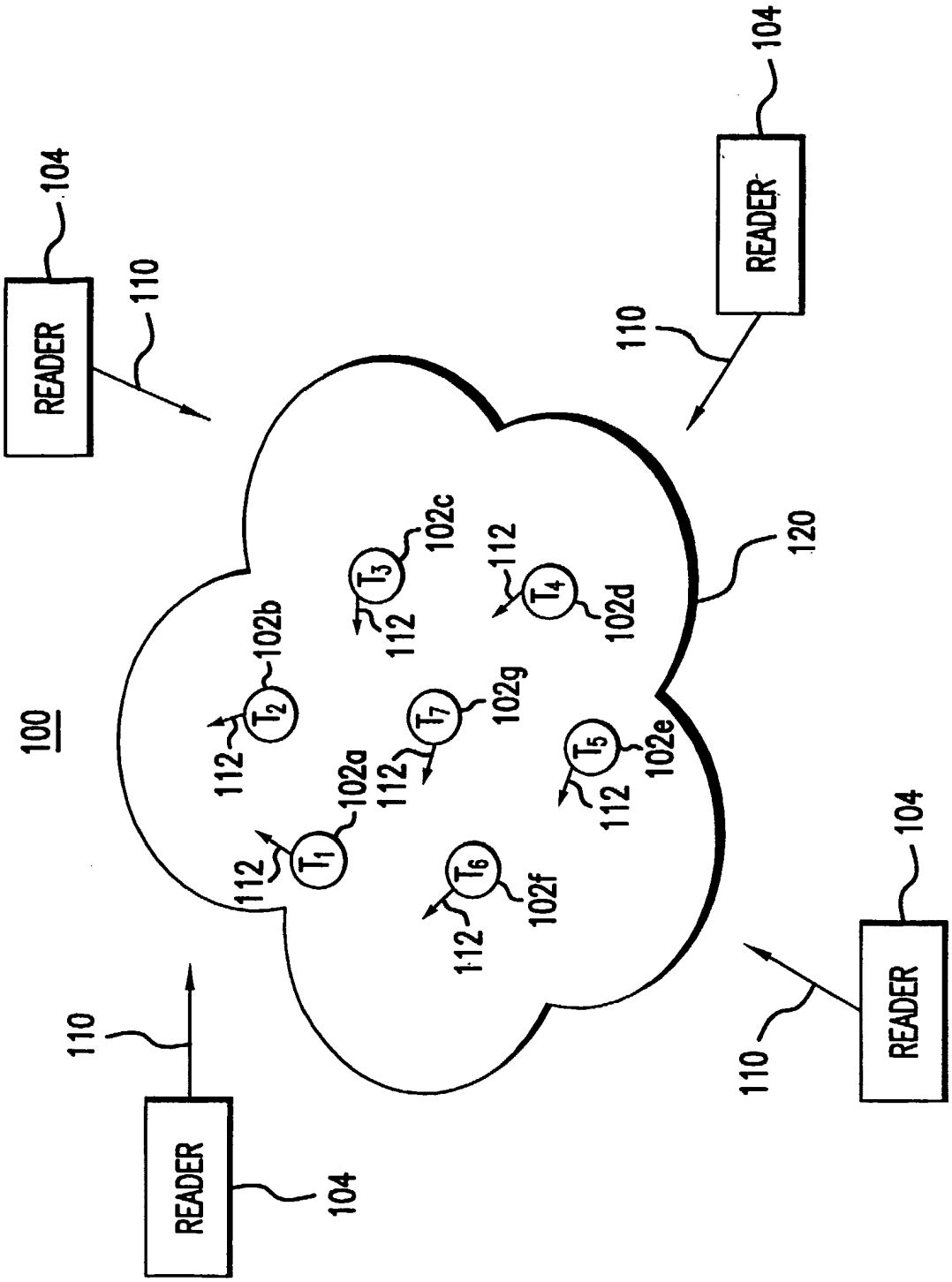

100
READER
104
110
READER
104
110
READER
104
110
READER
104
110
120
T_1
T_2
T_3
T_4
T_5
T_6
T_7
102a
102b
102c
102d
102e
102f
102g
112

FIG. 1

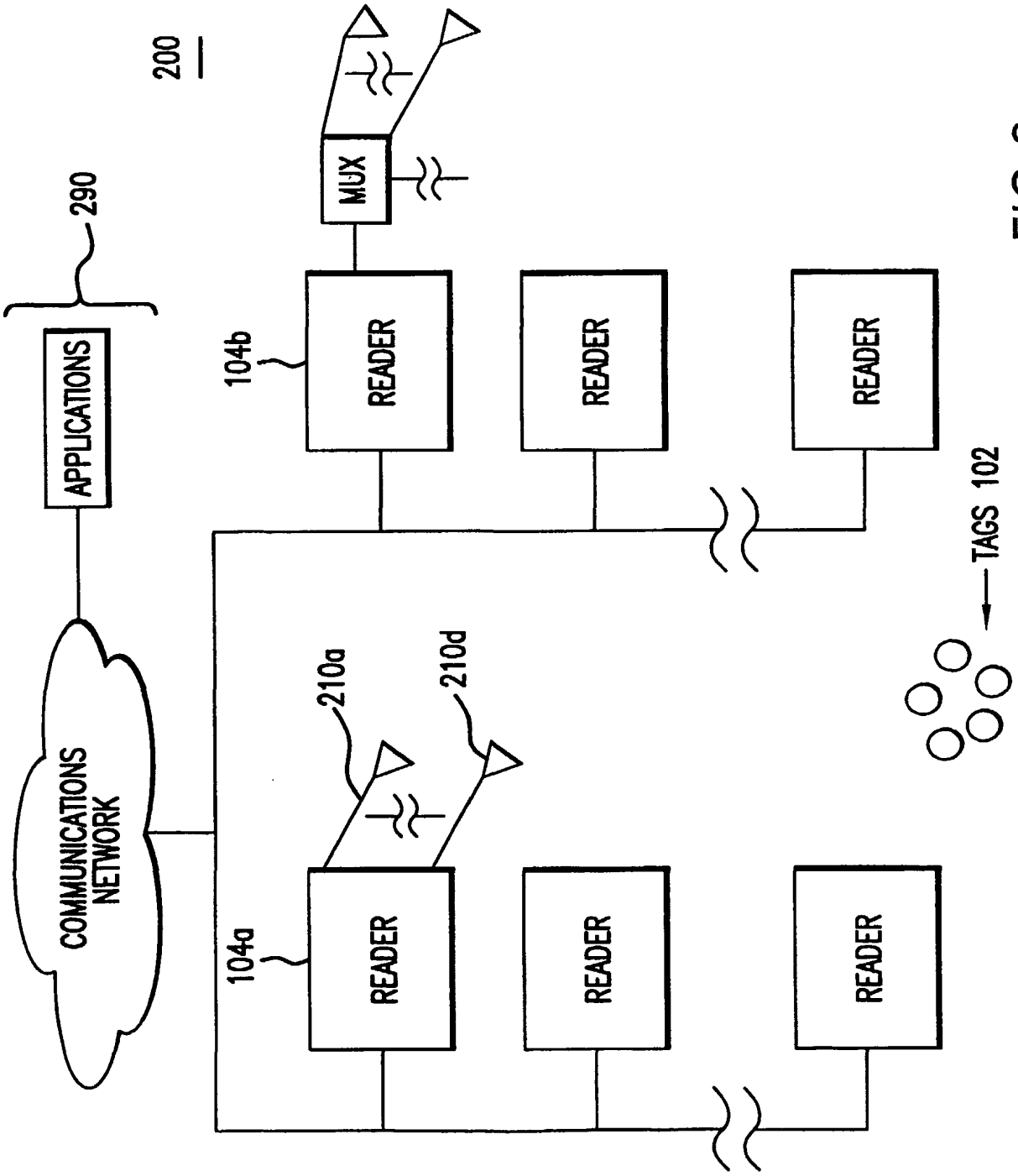

200
290
APPLICATIONS
COMMUNICATIONS NETWORK
MUX
104b
READER
READER
READER
210a
210d
104a
READER
READER
READER
TAGS 102

FIG. 2

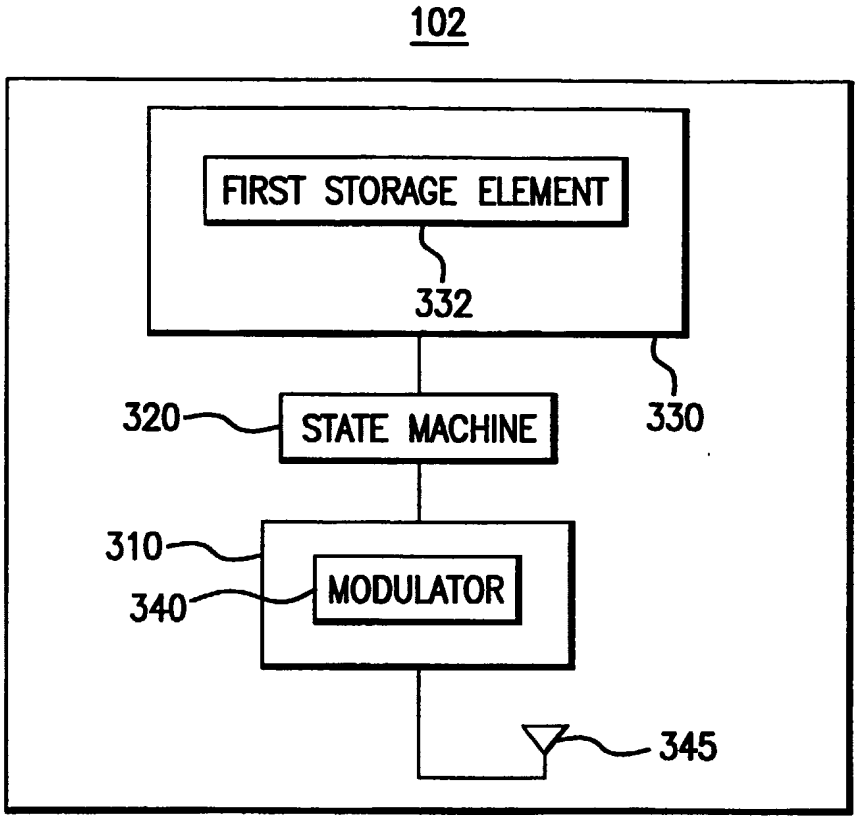

102
FIRST STORAGE ELEMENT
332
330
320
STATE MACHINE
310
340
MODULATOR
345

FIG.3A

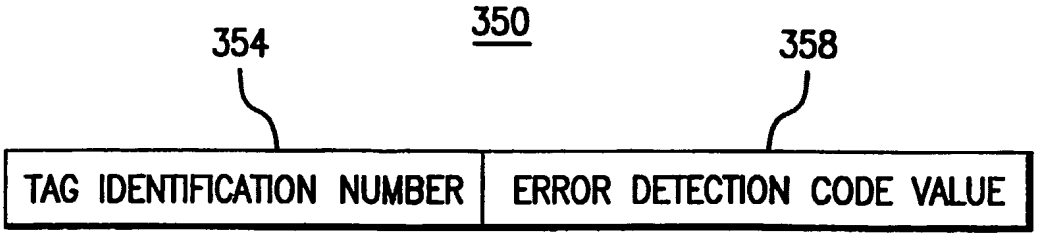

350
354
358
TAG IDENTIFICATION NUMBER
ERROR DETECTION CODE VALUE

FIG.3B

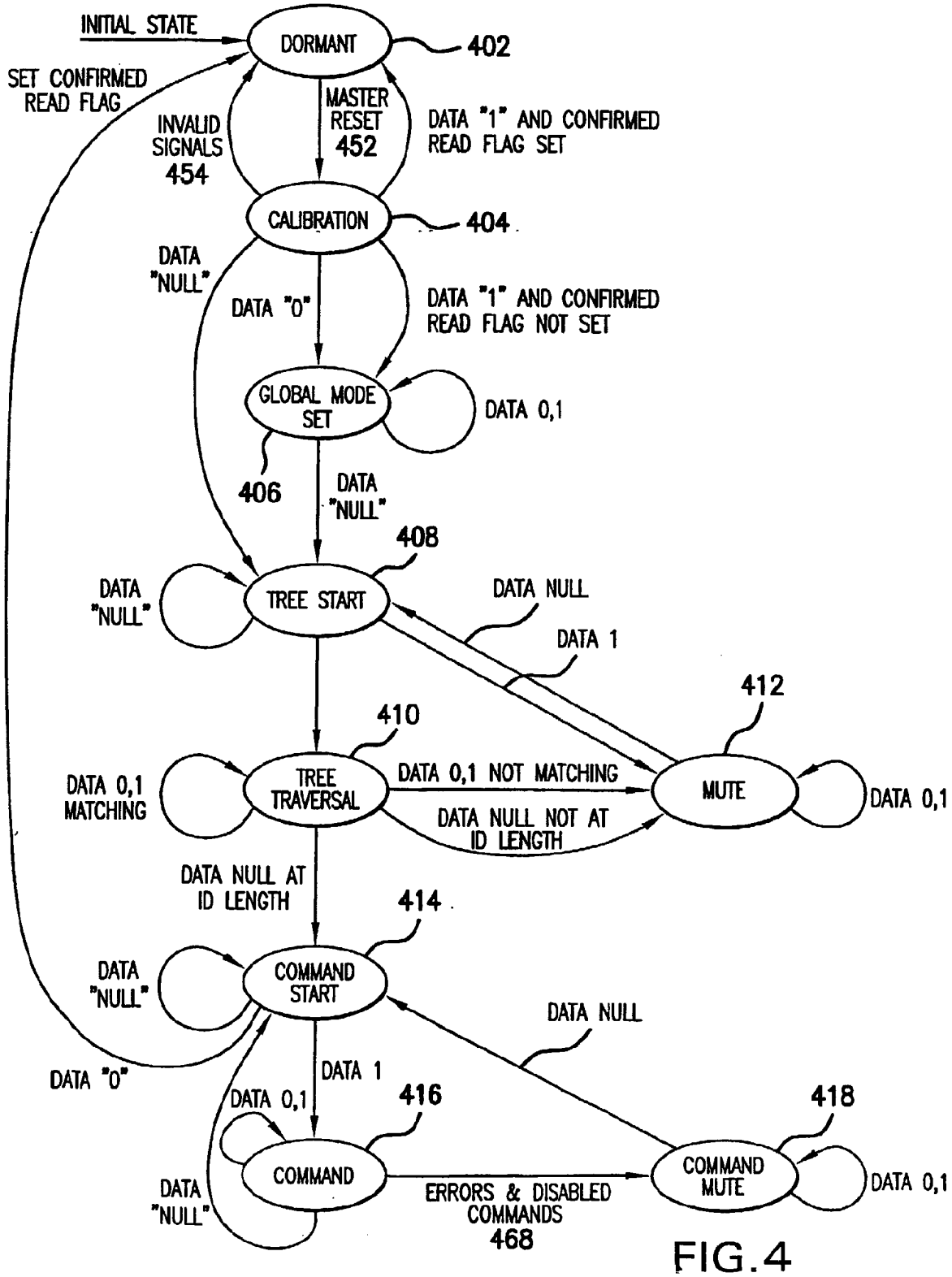


FIG.4

SAMSUNG EXHIBIT 1010, Page 226

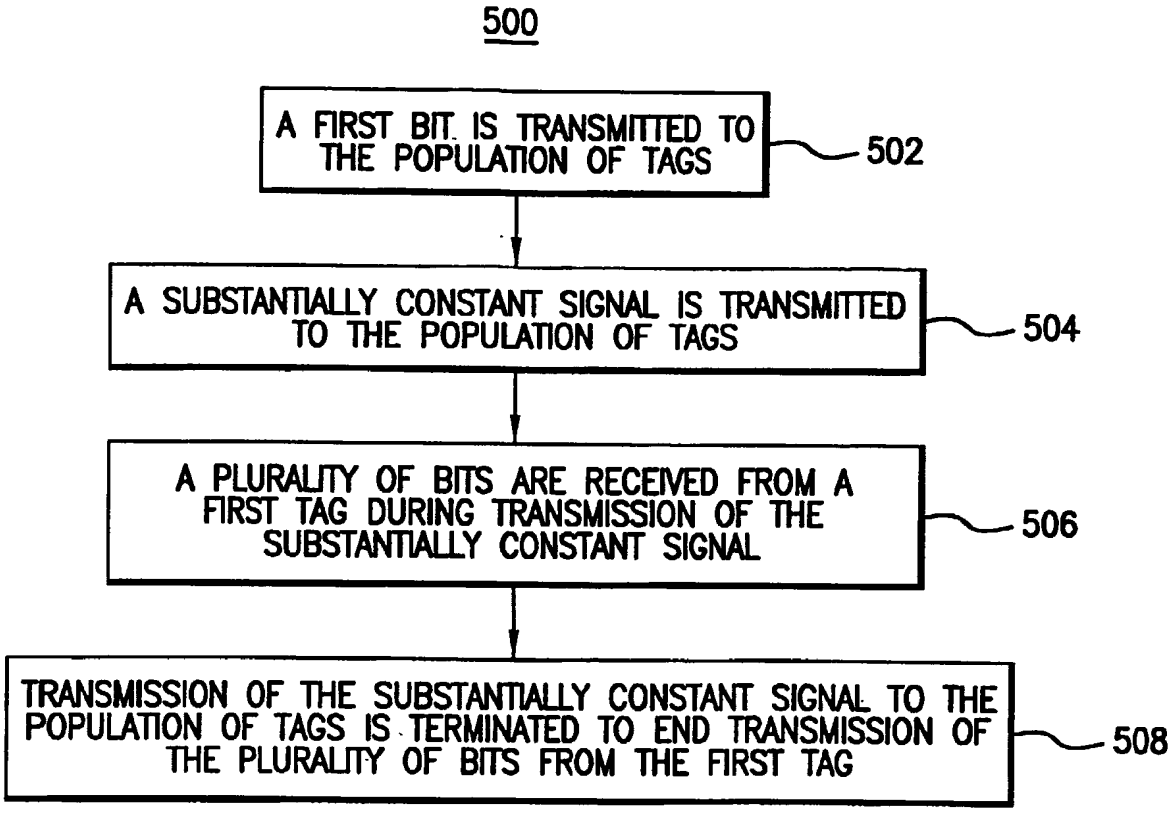


FIG.5

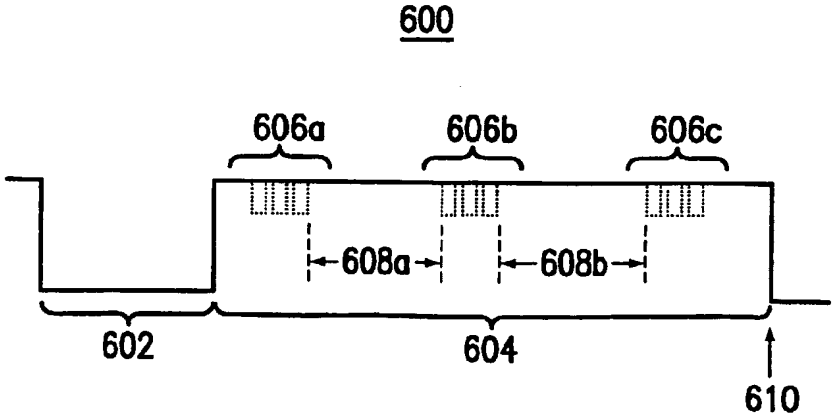


FIG.6

 SAMSUNG EXHIBIT 1010, Page 227

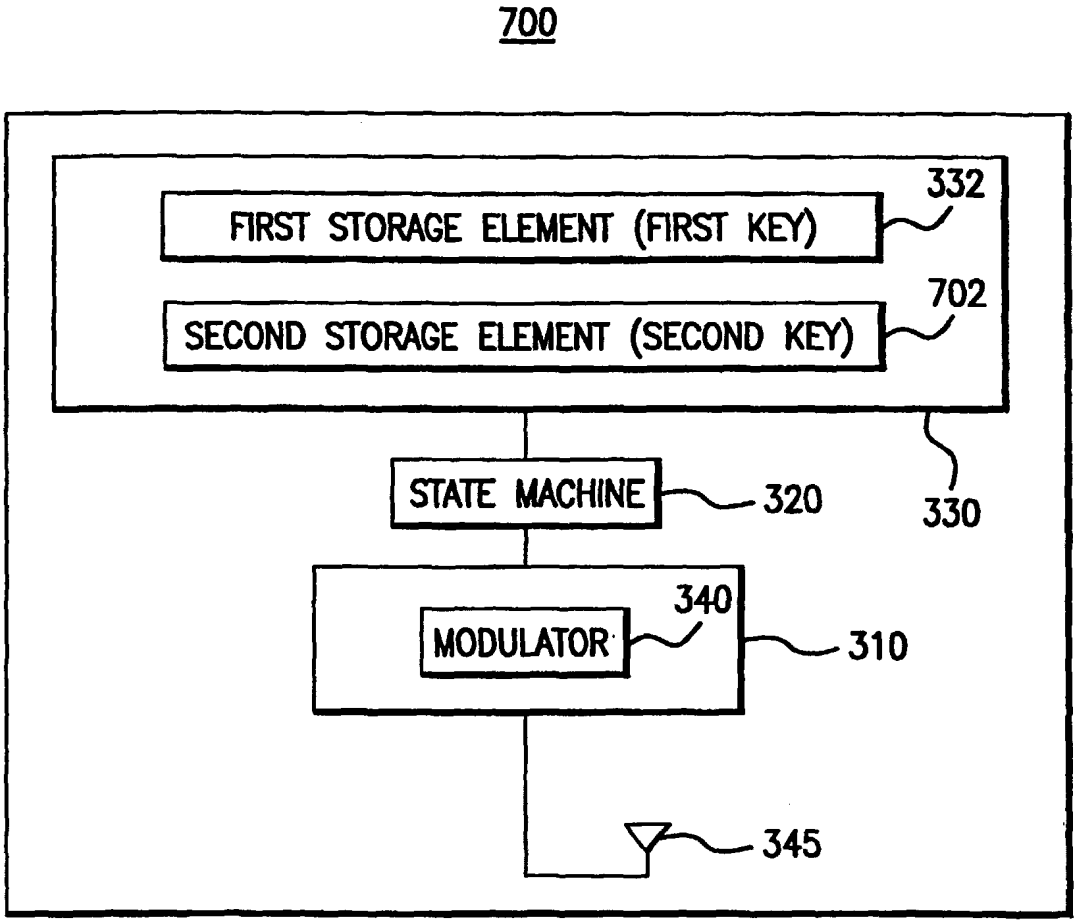


FIG.7

 SAMSUNG EXHIBIT 1010, Page 228

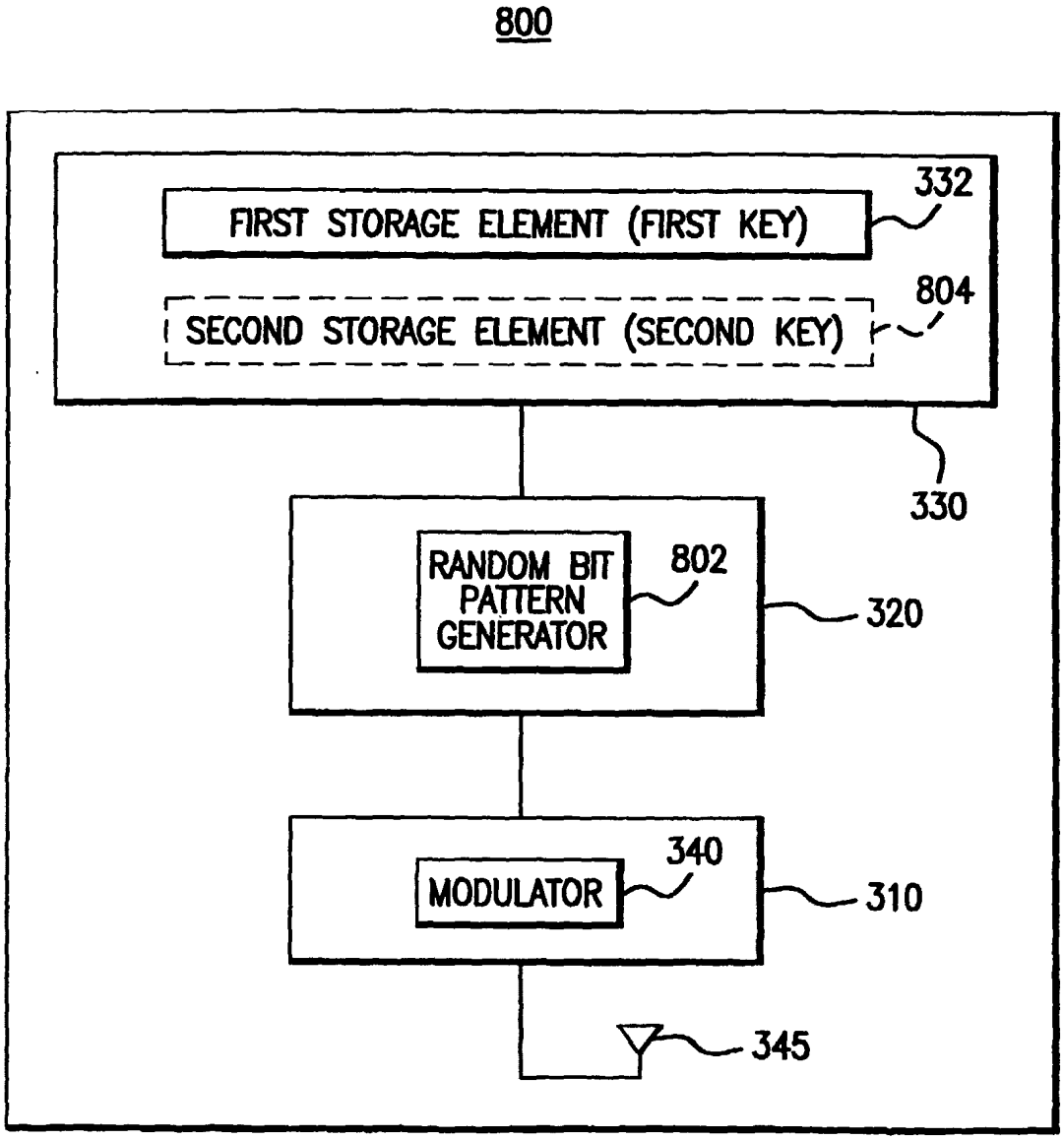

800
FIRST STORAGE ELEMENT (FIRST KEY)
332
SECOND STORAGE ELEMENT (SECOND KEY)
804
330
RANDOM BIT PATTERN GENERATOR
802
320
MODULATOR
340
310
345

FIG.8

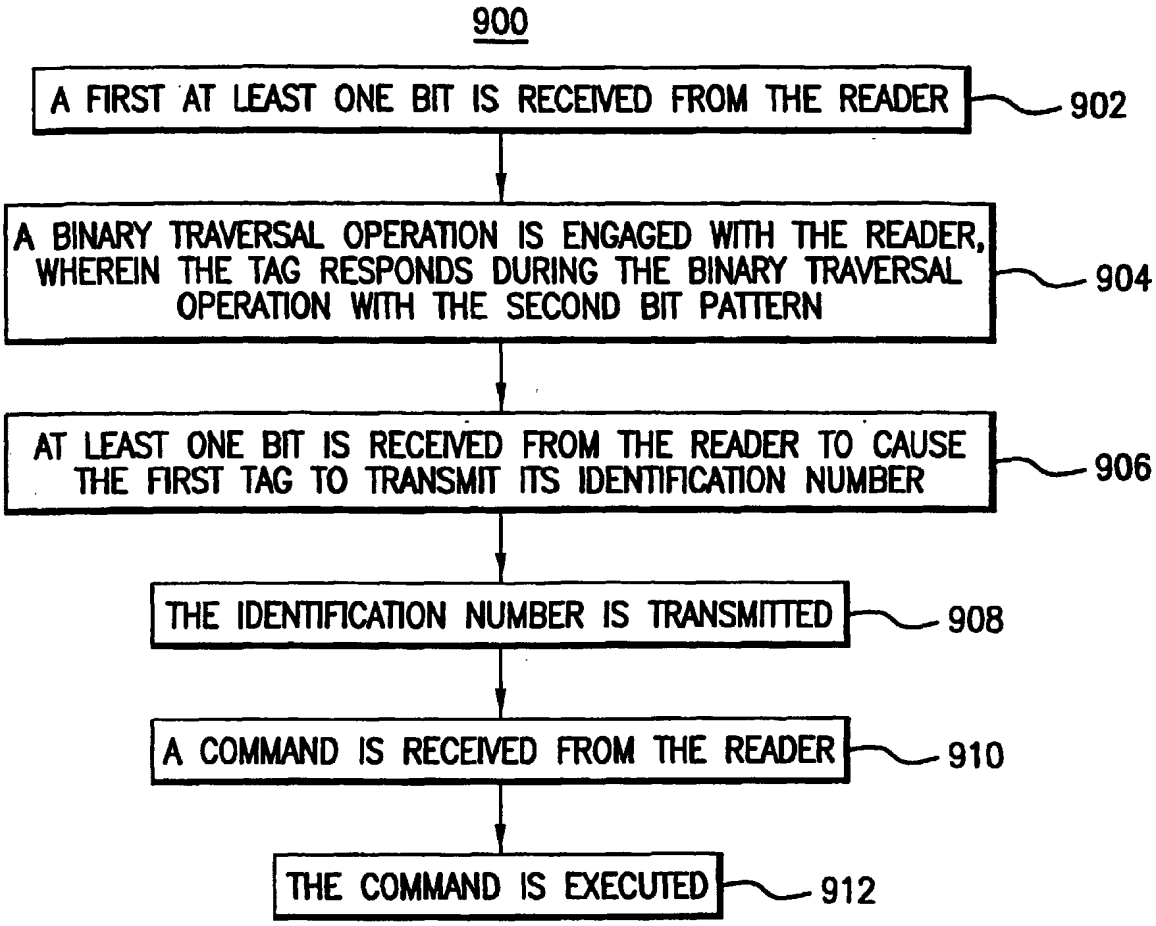

900
A FIRST AT LEAST ONE BIT IS RECEIVED FROM THE READER
902
A BINARY TRAVERSAL OPERATION IS ENGAGED WITH THE READER, WHEREIN THE TAG RESPONDS DURING THE BINARY TRAVERSAL OPERATION WITH THE SECOND BIT PATTERN
904
AT LEAST ONE BIT IS RECEIVED FROM THE READER TO CAUSE THE FIRST TAG TO TRANSMIT ITS IDENTIFICATION NUMBER
906
THE IDENTIFICATION NUMBER IS TRANSMITTED
908
A COMMAND IS RECEIVED FROM THE READER
910
THE COMMAND IS EXECUTED
912

FIG.9A

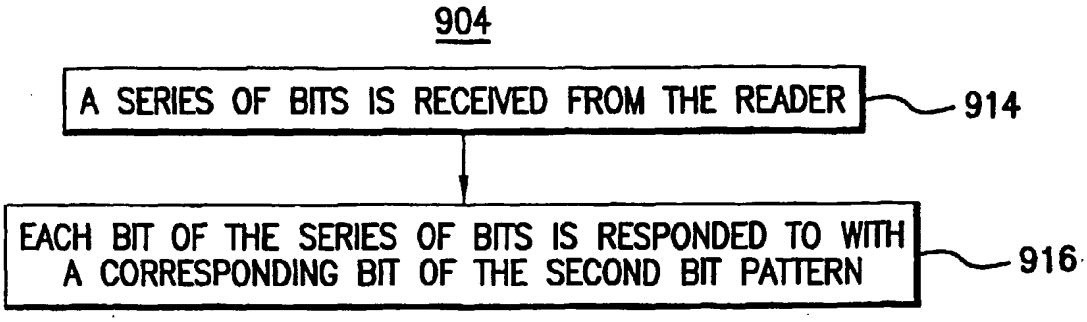

904
A SERIES OF BITS IS RECEIVED FROM THE READER
914
EACH BIT OF THE SERIES OF BITS IS RESPONDED TO WITH A CORRESPONDING BIT OF THE SECOND BIT PATTERN
916

FIG.9B

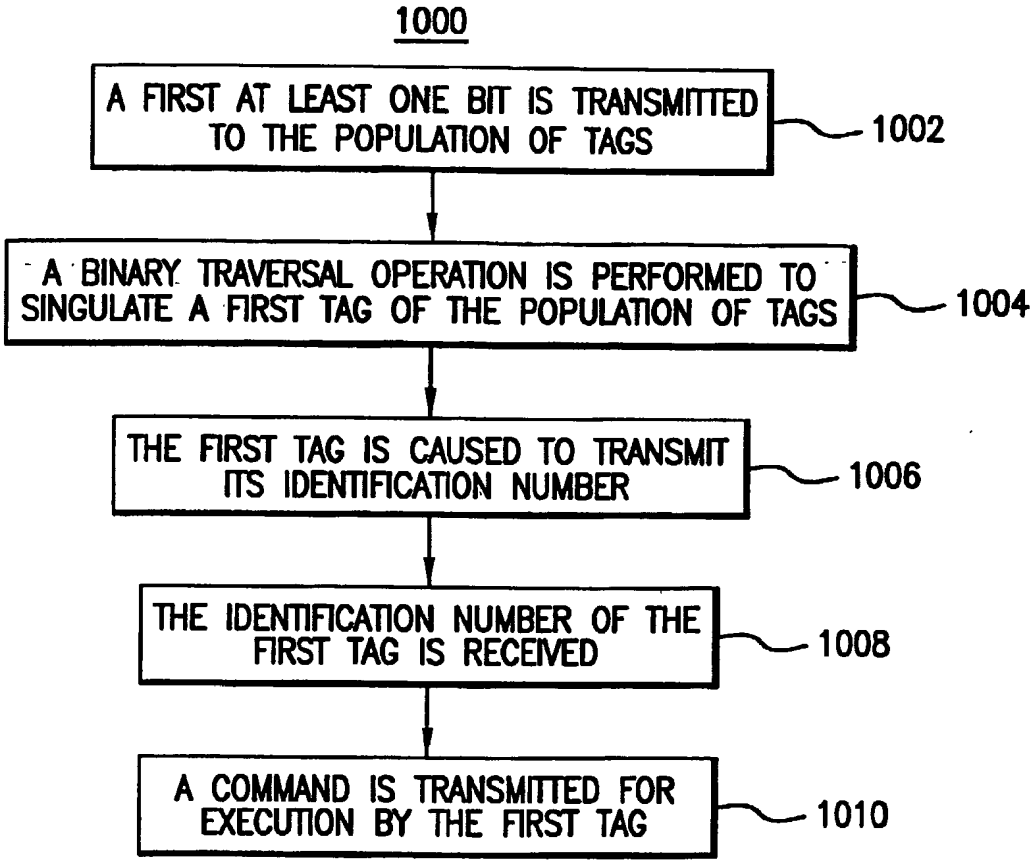


FIG.10A

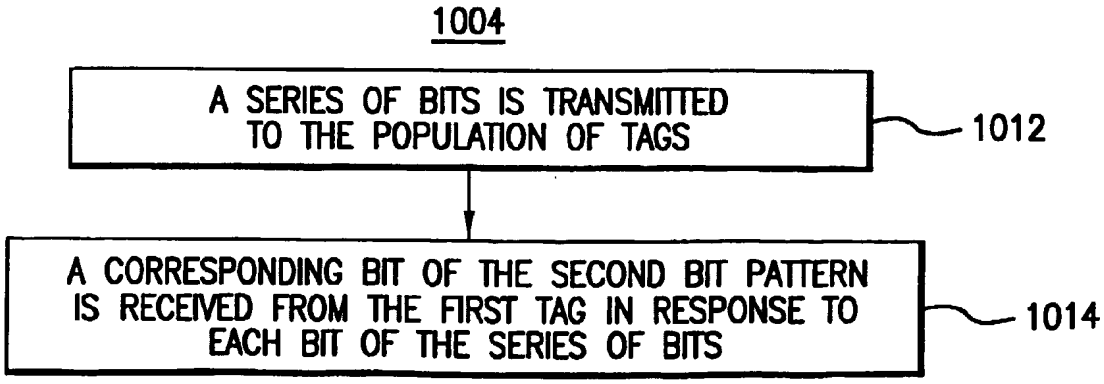


FIG.10B

 SAMSUNG EXHIBIT 1010, Page 231

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

(11) EP 1 075 781 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
30.01.2002 Bulletin 2002/05

(21) Application number: **99914309.2**

(22) Date of filing: **31.03.1999**

(51) Int Cl.[7]: **H05K 9/00**

(86) International application number:
PCT/US99/07088

(87) International publication number:
WO 99/57952 (11.11.1999 Gazette 1999/45)

(54) **EMI SHIELDING ENCLOSURES**

GEHÄUSE MIT ABSCHIRMUNG GEGEN ELEKTROMAGNETISCHE STÖRUNGEN

ENCEINTES DE PROTECTION CONTRE LES PERTURBATIONS ELECTROMAGNETIQUES (EMI)

(84) Designated Contracting States:
DE ES FI FR GB IT NL SE

(30) Priority: **01.05.1998 US 70994**

(43) Date of publication of application:
14.02.2001 Bulletin 2001/07

(73) Proprietor: **MINNESOTA MINING AND MANUFACTURING COMPANY**
St. Paul, Minnesota 55133-3427 (US)

(72) Inventors:
- **YENNI, Donald, M., Jr.**
Saint Paul, MN 55133-3427 (US)
- **DE SOUZA, José, P.**
Saint Paul, MN 55133-3427 (US)
- **BAKER, Mark, G.**
Saint Paul, MN 55133-3427 (US)

(74) Representative:
Hilleringmann, Jochen, Dipl.-Ing. et al
Patentanwälte von Kreisler-Selting-Werner,
Bahnhofsvorplatz 1 (Deichmannhaus)
50667 Köln (DE)

(56) References cited:

EP-A- 0 529 801	**EP-A- 0 805 619**
EP-A- 0 806 891	**US-A- 3 727 292**
US-A- 4 661 888	**US-A- 4 678 699**
US-A- 4 689 098	**US-A- 5 294 826**

Note: Within nine months from the publication of the mention of the grant of the European patent, any person may give notice to the European Patent Office of opposition to the European patent granted. Notice of opposition shall be filed in a written reasoned statement. It shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

Printed by Jouve, 75001 PARIS (FR)

Description

Background of the Invention

Field of the Invention

[0001] This invention relates to electronic assemblies surrounded by enclosures that prevent passage of electromagnetic or radio frequency interference (RFI). Enclosing structures combine shielding covers with ground planes associated with the electronic assemblies. Shielding covers derive from shaped composite sheets comprising nonwoven mats of randomly oriented, low melting, metal fibers. The invention further relates to means for attaching shielding covers to ground planes to provide completed shielding enclosures.

Description of the Related Art

[0002] Electronic assemblies, containing interference-sensitive or signal generating devices, require isolation by shielding covers and ground planes to protect the devices or prevent damage by the signals they emit. Shielding covers often include an electrically conducting element as part of a composite. A variety of composites containing both metal and polymeric materials are known for use in many varied applications. Composites may include metal in the form of continuous sheet, perforated sheets, mesh, woven screen or non-woven webs of randomly distributed fibers. Similarly, polymer structures, combined with the various forms of metal, may include films, sheets, perforated sheets, woven material or non-woven layers with random fiber distribution. Regardless of the metal/polymer composite used, it must act as a shield for electromagnetic and radio frequency waves. The interference caused by such waves in electronic devices is commonly referred to as electromagnetic interference (EMI) or radio frequency interference (RFI), hereinafter jointly referred to as EMI.

[0003] Effective EMI shielding requires the formation of a uniform conductive enclosure around the EMI-sensitive or EMI-emitting device. United States patent 5,294,826 (Marcantonio et al) discloses a combined heat dissipation and laminated shielding cover which absorbs energy by magnetic effects and electro-conductive effects to shield against electromagnetic interference. The laminated cover combines layers of metallic copper on either side of a magnetic layer.

[0004] From EP-A-0 806 891 there is known an EMI shielding enclosure for an electronic assembly comprising a ground plane, a shielding cover comprising a carrier sheet and a contact edge to form an electrical connection to the ground plane.

[0005] Suppression of radiated emissions from individual integrated circuits may involve the use of a shielded housing over an apparatus, e.g. a circuit board, that carries multiple integrated circuits. Such a housing is described in US 4,661,888 (Jewell et al). The housing of U.S. 4,661,888 and the cover of U.S. 5,294,826 require attachment to a ground plane using conventional methods such as soldering to a grounded contact point or connection through a conductive gasket or multiple machine screws. These methods include time-consuming, additional steps.

[0006] An EMI shielding layer, associated with the conductive enclosure, may be in the form of a continuous layer or a discontinuous grid, such as a metal mesh or nonwoven fibrous metal mass. A continuous layer, such as a metallic plate, is the most effective for EMI shielding because no gaps exist to allow passage of EMI. However, when using a discontinuous grid, any enclosure formation process that significantly increases the maximum void dimension in the shielding layer, sometimes called the "slot effect", could cause faulty EMI shielding performance of the shielding material. Void size increases in a variety of ways including, e.g. when the grid is stretched or by damage from tearing or other processes that can break the grid structure.

[0007] Previous disclosures reveal ways of producing and shaping sheet material to provide covers that have EMI shielding capability, typically using electrically conducting layers, which are required in many applications.

[0008] For example U.S. Patent No. 3 727 292 (Nicely), discloses a non-woven unitary metallic sheet which is fabricated by extruding a molten stream from a metallic melt into an atmosphere which reacts to form a stabilizing film about the periphery of the metal stream. The spun metal filaments are allowed to solidify, and then collected as a nonwoven fibrous mass. The mass of filaments is then compressed into a sheet-like form, and given strength by binding all or selected adjacent fibers together.

[0009] U.S. Patent No. 4 689 098 (Gaughan) discloses an EMI shielding sheet comprising a layer of nonwoven reinforcing fibers which supports a layer of metal whiskers or fibers formed from a ductile metal or metal alloy. The EMI shielding sheet is suitable for shaping of covers by stamping. Another stampable EMI shielding construction appears in U.S. Patent No. 4,678,699 (Kritchevsky et al). This patent notes that, "The shielding layer must be able to maintain its shielding effectiveness upon stamping." Kritchevsky further states that, "Holes formed upon tearing can dramatically reduce shielding." This statement refers to tearing of the shielding layer. Such statements reflect the fact that stamping processes tend to disrupt fibrous networks, breaking the fibers which, in the case of EMI shielding, results in poorer shielding effectiveness of the metal layers. There is no teaching of how to reduce fiber or filament breakage to a

SAMSUNG EXHIBIT 1010, Page 233

minimum during shaping.

[0010] Stamping is one method for forming shaped EMI shielding structures. This forming technology was developed in the metal industry for forming thin metal objects. It involves rapid, almost instantaneous application of mechanical force to distort a sheet into a shaped object. Stampable plastic/metal composite sheets may require heating, to soften the plastic surrounding the metal shielding layer, prior to stamping. This reduces the modulus of the plastic, allowing it to flow while the metal shielding composite responds to the high pressure, shaping force of the stamping press. The speed of this process demands high levels of ductility for the metal and high plasticity for the remainder of the composite, to absorb the applied force without rupture. This method, applied to sheet molding compound (SMC), provides automotive body panels and business machine housings using reinforced material comprising a non-woven, glass-fiber reinforcing layer, and a mat containing conductive fibers for EMI shielding, held together with a resin such as polyester. The SMC is a flat sheet prior to forming in compression dies of high tonnage presses. Material properties limit the use of SMC to simple, relatively shallow shapes. Conditions used for sharp draws, e.g. multiple rib formation in the shaped panel, may cause ripping of the shielding layer and reduction of EMI shielding performance.

[0011] As a substitute for stamping, the use of thermoforming or injection molding may be considered. Thermoforming, as it relates to the present invention, comprises heating a sheet and forming it into a desired shape. The process includes heating a thermoplastic composite sheet until it becomes soft and pliable, then using either air pressure or vacuum to deflect the softened sheet towards the surface of a mold until the sheet adopts the shape of the mold surface. Upon cooling, the sheet sets in the required shape allowing removal from the mold. Disclosures in JP 1990-276297 (Nakanishi) suggest the use of vacuum formable EMI shielding sheets, employing sandwich structures of brass filaments between plastic films. One embodiment uses a non-woven cloth of synthetic resin to reinforce the brass filaments. Reinforcement involves needle-punching of the metal fibers into the non-woven web. Application of plastic film, on both sides of the reinforced shielding layer, completes the vacuum formable sheet. Information from JP 1990-276297 includes no evidence of the condition of the EMI shielding layer after vacuum forming.

[0012] European patent EP 529801, commonly assigned with the instant application, discloses EMI shielding, add-on sheets, comprising carrier material with a metal fiber mat at least partially embedded in the carrier material. The add-on sheets provide EMI shielding covers to selected parts of a thermoformed structure. Successful use of these add-on sheets requires that they possess or develop porosity when thermoformed in contact with the thermoformable substrate blank to which they were applied. This reference addresses changes that can occur during thermoforming to impair the effectiveness of the EMI shield. These changes include breakage or beading of molten metal fibers and in extreme cases separation of the metal matrix into discontinuous islands which provide no EMI shielding. While observing a progression of damaging conditions there is no evidence of means for optimum stabilization of the EMI shield during thermoforming.

[0013] Depending on the melting point of the metal fibers, it is possible for fibers in an EMI shielding layer to melt, and rupture under the stress of stretching and shaping during thermoforming. If sufficient molten fibers break in close proximity to each other the liquid metal may flow to form a metal droplet by coalescence of multiple molten fibers. At some point in metal droplet development its size is sufficient to bleed through the surface of the EMI shielding layer. Continued flow of molten metal into a droplet produces a defect extending outside the plane of the shielding layer. Upon cooling the defect is clearly seen as a shiny protruding bead, bump or disc extending from, and disposed over the surface of the thermoformed structure. Formation of these spheroidal protrusions can adversely affect EMI shielding because the flow of molten metal, resulting in their formation, draws metal from an area surrounding the protrusion causing reduced shielding efficiency in that area. In addition, current conducting, solid spheroidal protrusions cause potential electrical shorting problems if they contact circuit elements or microdevices in the restricted space usually associated with housings for electronic assemblies. Solid protrusions can also interfere with injected resin flow when the shielding composite is an insert for injection molding.

[0014] Ideally, a shaped EMI shielding article employs an electrically conductive element, within its structure, to contain generated EMI or present a barrier to radiated EMI. At the same time the conductive element should not establish electrical contact with an electronic component, thereby causing a device to malfunction. However, effective EMI shielding enclosures require electrical continuity between a shaped EMI shield and a ground plane associated with, e.g. a printed circuit. To maintain electrical insulation of the shield, but allow access for electrical connection to the conductive element, commonly assigned patent EP 529,801 indicates the need for special connectors. Surprisingly, it was discovered that, by carefully controlling the thickness of insulation covering the electrically conducting shield, to less than 0.15 mm, the need for special connectors may be eliminated in favor of a simpler thermal bonding technique, also referred to herein as heat staking.

[0015] Several alternative solutions have been attempted to improve the effectiveness of conductive fiber based EMI shielding. The formation of pressure welds or sintered bonds between the fibers improves electrical conductivity, but reduces overall flexibility and extensibility of the welded mat. Composite metal-fiber/polymer sheets containing such sintered metal mats cannot be thermoformed without breaking many of the fibers themselves, the bonds between the fibers or both, thus reducing the shielding properties at higher stretch ratios required in thermoformed parts.

SAMSUNG EXHIBIT 1010, Page 234

[0016] With the increasing use of advanced, EMI-sensitive electronics, a need exists for improved materials for shaping into EMI shielding covers or housings that reliably protect electronic assemblies. Methods to shape EMI shielding covers rely upon the use of moldable composites. Many shapes limit stretching of the moldable composites to shallow drawn structural features. In other cases the shapes require composites with ability to retain shielding capabilities even when complex shapes demand localized elongation of 300-500%. This condition is possible using composite structures of the invention comprising a thermoplastic sheet of carrier material, supporting a layer of randomly distributed, low melting metal fibers stabilized against fiber rupture and development of bumps during forming, by means of a coating (fiber-coating) of a thermoplastic polymer. Composite sheets of the invention provide improved EMI shielding performance by maintaining the integrity of molten metal strands during thermal shaping to introduce shallow to deep drawn features into the composite sheet.

[0017] Prior art clearly reveals problems, associated with loss of EMI shielding, when the shielding layer loses its integrity through, e.g. tearing, excessive hole formation, fiber separation and increase in the number and size of gaps. While claiming EMI shielding effectiveness, in excess of 30dB, for a variety of formable sheets, prior art advances no teaching of properties tending to stabilize such sheets against the problems outlined above. Also there is no evidence of the variability of shielding performance of formed prior art structures. Accordingly, there is a need not only to provide effective EMI shielding but to control it in such a way that formed structures consistently show almost no evidence of undesirable features, such as tears, holes, breaks, and spheroidal protrusions such as beads, bumps and the like.

[0018] The current inventors discovered how to stabilize randomly oriented metallic fiber mats to maintain fiber continuity and conductivity to consistently provide thermoformed covers with maximum shielding capability. This contributes dual benefits of improved EMI shielding performance coupled with the potential for cost savings from reduced incidence of rejection of shielded structures after thermoforming. Additional cost savings and convenience accrues from the use of a heat staking method to connect shielding covers to conductive ground planes.

Summary of the Invention

[0019] The present invention discloses EMI shielding enclosures, for surrounding electronic assemblies, components used to form the enclosures, and a method for combining the components. One embodiment combines an EMI shielding cover with a ground plane associated with a printed circuit used to interconnect the devices of the electronic assembly. The shielding cover originally exists as a composite, thermoformable planar structure combining a non-porous carrier sheet with a mat or grid of randomly oriented, low melting metal fibers. The metal fibers are substantially surrounded by a fiber-coat material, which may be coated prior to or after attachment of the metal fibers to the non-porous sheet.

[0020] The shielding cover of the invention is a shaped article formed by thermoforming of a planar sheet, including an EMI shield. The article comprises a non-porous carrier sheet, a fibrous metal mat adjacent the carrier sheet such that the metal fibers, forming the metal mat, are essentially free of defects in the form of spheroidal protrusions, and a thermoplastic fiber coat, less than 0.15 mm thick, substantially surrounding the fibers. The fiber-coat may be sprayed onto the mat or, as a pliable, sometimes heated layer, may be pressed into the fibrous metal mat to substantially surround the metal fibers, and such procedure may take place before or after attachment to the carrier material.

[0021] All components of the composite planar structure melt or soften at temperatures lower than the temperature of thermoforming. At thermoforming temperatures, the viscosity of the softened fiber-coat material is higher than the viscosity of the molten metal of the metal fiber mat. The EMI shielding sheet exhibits improved performance, particularly when formed into deep-drawn shapes with pockets having stretch ratios up to 500%.

[0022] The resulting composite sheet material may itself be thermoformed or may be an integral portion of an injection molded structure when placed, as a planar sheet, or pre-form, into the molding cavity prior to resin injection.

[0023] All of the various embodiments of the invention require coating of the strands of the fibrous metal mat. This leads directly to the improvements associated with the invention including reduction or prevention of flaking of the metal fibers during handling and essential absence, at thermoforming temperatures, of fiber rupture that readily results in spheroidal protrusions by coalescence of molten metal from adjacent fibers. Lack of disruption of the fibrous metal mat means improved retention of EMI shielding for composite sheets of the invention. Presence of the coating over the metal fibers further results in shielding covers being electrically insulated.

[0024] It is desirable to establish electrical connection between cover and ground plane when forming EMI shielding enclosures. Such connection is preferably readily achievable. In accordance with this requirement, the invention teaches the formation of reliable electrical connection between cover and ground plane via control of thickness of the insulating fiber coat to facilitate direct attachment, during heating, using a method described herein as heat staking.

[0025] As used herein, these terms have the following meanings.

1. The terms "fiber-coat" and "fiber-coat matrix" are synonymous as used herein to refer to that coating or material which substantially surrounds the fibers of the metal mat, providing stabilization thereto, to reduce flow of molten metal during thermoforming.

SAMSUNG EXHIBIT 1010, Page 235

2. The term "carrier sheet" means a layer which is attached, by various means, including mechanical means, heat attachment, adhesive attachment or the like, to the metal mat and fiber-coat. The term "carrier material" is synonymous.
3. The term "melting point" as applied to a metal or metal alloy means that point at which the metal begins to become molten, i.e., the melt onset. The metal or metal alloy may not be completely melted at this point.
4. The term "softening point" of a polymer is associated with its glass transition temperature above which the polymer becomes soft and pliable.
5. The term "slot effect" refers to the phenomenon that the amount of EMI that passes through a given void is dependent on the length of the void's longest dimension and not on the total area of the void, such that a very long thin void may pass much more EMI through than a square void with smaller dimensions having many times the area of the thin void.
6. A "spheroidal protrusion" is a defect, exemplified by and synonymous with a bump or bead of exposed metal, projecting beyond the surface of an EMI shielding cover after thermoforming. Such defects occur by coalescence of molten metal produced on heating metal fibers to thermoforming temperatures. EMI shielding effectiveness decreases around the defect and the protrusion may cause short circuits by contact with circuit elements or micro-devices in the restricted space usually associated with electronic packages.
7. The terms "fibrous metal mat" and "metal fiber mat" are synonymous and mean a mat formed from metal filaments.
8. The term "contact surface" refers to the portion of the mat of randomly oriented metal fiber closest to the carrier sheet.
9. The term "contact edge" refers to the flange formed around the perimeter of the thermoformed EMI shielding cover to bond it over the conductive trace of the ground plane during heat staking.
10. The term "die profile edge" is a narrow, divided or continuous rail projecting from the heating block to provide localized heating around the contact edge.

[0026] All percentages, parts and ratios herein are by weight unless specifically noted otherwise.

Description of the Drawings

[0027] Fig. 1 is an exploded, perspective view showing alignment of parts for heat staking an EMI shielding cover to the ground plane of the printed circuit of an electronic assembly.
[0028] Fig. 2 is a cross sectional view showing positioning of the heating block of a staking tool to attach an EMI shielding cover to the printed circuit of an electronic assembly.
[0029] Fig. 2a is a detail view of a section from Fig. 2 showing the profile edge of the heating block.

Detailed Description of the Invention

[0030] Electromagnetic interference (EMI) shielding of electronic devices requires, in the majority of cases, a material that blocks the interference signals associated with the devices themselves or impinging from external sources that radiate potentially damaging electromagnetic waves. A suitable form of EMI shielding comprises an enclosure surrounding an electronic assembly. The enclosure of the current invention has several parts suitably connected to form an electro-conductive structure around the assembly. Required parts include a ground plane associated with the electronic assembly and an EMI shielding cover, electrically connected to the ground plane. The basic concept of combining a shielding cover with a ground plane to provide a shielding enclosure was disclosed previously. The distinguishing features of this invention reside in the shielding cover and its ease of attachment to the ground plane of a printed circuit. Effective shielding cover materials, in this case, must meet EMI shielding requirements while responding to shape formation using a variety of molding techniques. EMI shielding articles, for use as shielding covers herein comprise a carrier sheet, usually a thermoplastic polymer sheet, a conductive EMI shielding layer in the form of an electrically conductive, randomly oriented fibrous metal mat and a polymer fiber-coat substantially surrounding the fibers of the metal mat. The metal fibers comprise a low melting metal or metal alloy, melting in a temperature range from about 70°C to about 370°C. Within this temperature range, fibers in the fibrous metal mat become molten as required during thermoforming processes related to this invention.
[0031] In the absence of a fiber-coat around such molten metal, the influence of surface tension, creates a tendency for the metal to flow. This flow disrupts the filamentary form of the fibers. Consequently, unconstrained, a molten metal fiber is susceptible to interaction with other molten fibers to produce coalesced beads of metal that grow in size to a diameter of several millimeters. The process of coalescence redistributes EMI shielding material with the highest metal concentration close to the metal bead. Shielding material is thus lost from the area surrounding the bead which reduces the EMI shielding effectiveness of the metal mat in that area. Extreme cases of metal fiber coalescence exhibit uncon-

SAMSUNG EXHIBIT 1010, Page 236

nected islands of metal that grew until cessation of the flow of available molten metal. In these cases EMI shielding is minimal and usually unsatisfactory. Avoidance of coalescence provides the improvement, and consistency of performance, that distinguishes the present invention from other EMI shielding articles.

[0032] Redistribution of EMI shielding material may be substantially eliminated by constraining molten metal fibers in a form as similar as possible to that of the solid fibers. This may be accomplished by substantially surrounding the fibers with the fiber-coat material, which limits the ability of the fibers to form coalescing metal droplets. As the fiber-coat and metal fiber mat change shape during thermoforming, the fiber-coat matrix stabilizes the molten metal fiber and limits its flow. Thus, growth of metal droplets, to a level where they would bleed through the fiber-coat causing bare metal spheroidal protrusions, is much less likely to occur. Reduction of EMI shielding and short circuiting of electronic devices became relatively insignificant problems for fiber-coat stabilized metal fiber mats. Suitable materials for the fiber-coat include thermoplastic, film forming polymers having melt viscosities that exceed the viscosity of molten metal fibers during thermoforming of the fibrous metal mat. While not wishing to be bound by theory, it is believed that the fiber-coat provides channels or passageways that maintain metal fibers in filamentary form while molten, during thermoforming. Application of the fiber-coat before thermoforming is accomplished by varied methods, depending on the nature of the materials involved. For example, a non-porous, thermoplastic sheet may be softened then combined with the mat of metal fibers by pressing the mat into the material until the fibers are substantially covered. Alternatively, the fibrous metal mat may be first coated with the thermoplastic fiber-coat by such mechanisms as softening of a solid coat, spraying of a liquid coat and the like, and then the coated mat may be attached to the carrier layer, by means of adhesive, or of forcing the layers together or other conventional means. The extent of burying of the coated metal fiber mat depends upon the thickness of the fiber-coat, and the form in which it is applied. Any of the composite sheets, previously described, may be molded directly without significant disruption of the EMI shielding layer, due to the non-porous nature of the carrier material. Where a thick article is desired, the carrier layer can be provided with added thicknesses of carrier, which may be of the same or different chemical composition.

[0033] A preferred embodiment of thermoformable EMI shielding sheets used for the invention comprises a carrier sheet of polycarbonate, supporting a metal fiber mat of low melting tin/bismuth alloy fibers coated with ethylene vinyl acetate fiber-coat applied using extrusion techniques. The structure, thus described, passes between heated nip rollers to cause diffusion of the fiber coat through the metal fiber mat towards the carrier sheet.

[0034] An alternative preferred embodiment of the invention comprises a carrier sheet attached to a metal fiber mat by a layer of thermoplastic fiber-coat material such as ethylene vinyl acetate. When compressed in a heated platen press the fiber coat migrates through the metal fiber mat to engulf, or at least substantially surround the metal fibers.

[0035] In a third preferred embodiment, the invention includes four layers comprising a carrier sheet, a first adhesive layer, a metal fiber mat and a second adhesive layer. Application of pressure, from a heated platen press, causes inward flow of adhesive, from both sides of the metal mat, while promoting firm attachment of the fiber mat to the carrier sheet. This embodiment may be further modified by including electrically conductive particles, in the adhesive, to facilitate electrically conductive pathways between shaped, shielding cover articles of the invention and ground planes associated with electronic assemblies. Conductive particles include but are not limited to, metallic powders, metallic granules, metallic beads, metallic flakes, metallic fibers, metal coated powders, metal coated granules, metal coated beads, metal coated flakes and metal coated fibers.

[0036] Each of the preferred embodiments, previously described, contains fibers that are substantially surrounded by a thermoplastic resin fiber coat. This aspect of the invention distinguishes it from prior art structures including metal fibers either sandwiched between layers of thermoplastic film or partially embedded in thermoplastic resin.

[0037] Examples of polymeric materials useful as fiber-coat materials include, but are not limited to those having a softening point below about 80°C, such as ethylene vinyl acetate copolymers, vinyl acetate, amorphous polyolefins, polyethylene, polypropylene, thermoplastic elastomers, hot melt adhesives, acrylic adhesives, pressure sensitive adhesives, polyurethane, styrene butadiene styrene copolymers, styrene ethylene propylene styrene copolymers, ethylene methyl acrylate copolymers, grafted polymers and copolymers, functionalized polymers and copolymers, including maleic anhydride, acrylic acid and epoxy modified polymer and copolymers, copolyesters, latex binders, EVA dispersions, paraffin wax, and the like, including blends, mixtures and alloys thereof. While typically the fiber-coat and carrier sheet or film material will differ to provide desired properties in the final article, they could be the same if desired.

[0038] Examples of polymeric materials useful as carrier materials include, but are not limited to those having a softening point below about 150°C, such as polycarbonate, acrylonitrile butadiene styrene copolymers (ABS), styrene acrylonitrile copolymers (SAN), polystyrene, polyvinyl chloride, polyether imide, polypropylene, polyethylene, polybutylene, polyamide, thermoplastic polyesters and co-polyesters like, for example, polyethylene terephthalate, polybutylene terephthalate and polyethylene naphthalate, polymethyl methacrylate, ethylene butyl acrylate copolymers, polyacrylonitrile, polyarylketones, polyethersulfone, polyphenylene sulfide, polyurethane, styrene butadiene styrene copolymers, styrene ethylene propylene styrene copolymers, vinyl acetate, thermoplastic elastomers, grafted polymers and copolymers, functionalized polymers and copolymers and the like, including blends, mixtures and alloys thereof.

[0039] These polymers and copolymers may also contain fillers such as glass microspheres, which are especially

SAMSUNG EXHIBIT 1010, Page 237

useful when acrylic adhesives are used, colorants, antioxidants, dyes, and the like in small percentages such as will not disturb the electrical performance or EMI shielding properties of the article.

[0040] A wide variety of metals and metal alloys may be used in EMI shielding sheets of the invention. A useful metal has a melting temperature in the range of 70°C to about 370°C depending on the carrier polymer. Metals having the appropriate melting temperatures must be selected by one skilled in the art so that the carrier polymer will not degrade at the thermoforming temperatures required for the article. Examples of relatively low melting metals for use in composites of the present invention include tin, lead, bismuth, cadmium, indium, gallium, zinc, mixtures thereof, and their alloys. The alloy group may be augmented by alloys containing metals with higher melting points, including such metals as antimony, aluminum, copper, silver, gold, nickel, cobalt, and iron. Those skilled in the art will also be able to select other alloys to fulfill the requisite melt temperature criterion.

[0041] Thermoforming procedures used with improved EMI shielding, composite sheets of the invention do not include high impact methods such as forcible stamping even if the stamping proceeds at elevated temperature. Instead, the preferred method employs a clamping frame that holds the composite sheet for exposure to heating devices or ovens located on either side of the sheet. After absorbing heat, sufficient to suitably soften the composite sheet, and moving the frame to effect a seal between the softened sheet and the mouth of a shaping mold, the application of vacuum to the mold draws the pliable, composite sheet into the mold until there is intimate contact between the sheet and the mold surface. While this method uses vacuum to draw the sheet into the mold, it is possible to use external air pressure to urge the sheet into the mold and into contact with the mold surface as before. Also, the female mold used in the example may be replaced by a male mold suitably designed for either pressure or vacuum forming.

[0042] Shaping, by thermoforming may result in significant stretching of selected sections of a composite sheet. Some aspects of a shaped article may require elevated temperature elongation of from about 300% to about 500% by the metal mat and the carrier material. This places a strain on the integrity of the metal fibers which lose EMI shielding capability if they rupture. However, in articles of the invention, the molten metal fiber, substantially surrounded by a thermoplastic fiber-coat shows almost no tendency to flow and form spheroidal projections. As the softened composite sheet is stretched, the molten metal fibers, stabilized by the fiber-coat matrix, retain continuity. Metal fiber-to-fiber contacts not only remain intact but, as the fiber-coat stretches they are fused together, to improve the performance of the EMI shield. The existence of multi-fiber junctions causes rigidity before thermoforming. This may cause disruption of the EMI shield during thermoforming. Conversely, the formation of multi-fiber junctions as a result of thermoforming enhances the conductivity and shielding capability of the shaped structures.

[0043] Remarkably, even with an insulating coating over fibers of the metal mat, electrical continuity between the EMI shielding layer and e.g., a ground plane of a printed circuit, may be established, while attaching the shielding cover to an electronic assembly, using common connection techniques, such as heat staking and sonic welding. This provides a significant advantage compared to earlier methods used to make electrical connection. Such methods, including high-temperature soldering to a ground point, bridging between separated cover and ground plane with a conductive, shielding gasket and multi-point securing of an enclosure with machine screws, are subject to additional process steps.

[0044] Any method may be used for electrical connection, between the EMI shielding cover and associated structures, provided it displaces polymer to expose bare metal fiber. As an example, at heat staking temperatures, the metal fibers exhibit increased hardness relative to the softened polymer fiber-coat. The hardness differential causes the metal fibers to migrate through the polymer fiber-coat, under the influence of applied force. With application of sufficient force the metal fibers exit the polymer fiber-coat becoming exposed at its surface and available for direct contact against substrates adjacent to the exposed metal fiber. This condition persists for the short time required for heat staking according to earlier disclosure. Effective electrical connection to shaped articles of the invention requires that the thickness of the fiber coat layer is less than 0.15 mm. Thickness control represents an important consideration to the surprising execution of electrical connection through an insulating fiber-coat. Using shaped covers, described herein, the connection to ground occurs simultaneously with application of the EMI shielding cover as a housing over an electronic assembly.

[0045] Figures 1 through 2a illustrate application of a shielding cover using a heat sealing process, referred to herein as heat staking. After placing the EMI shielding cover **12** in desired alignment over the electronic assembly, application of heat and pressure, through the heat staking tool **14**, bonds the shield to the conductive trace **16** of the printed circuit **18** of the electronic assembly. The conductive trace **16** is part of the ground plane of the printed circuit **18**. A completed, covered assembly includes the printed circuit **18**, supporting electronic components that are surrounded, and protected, by the shaped EMI shielding cover **12**. Bond formation occurs between the shielding cover **12** and printed circuit **18** by adhesion, via e.g. a hot melt polymer, along the contact edge **20** of the EMI shielding cover **12.** The fiber coat resin provides the bonding material at the contact edge **20**.

[0046] Successful electrical connection of the shielding cover **12,** to the assembly, requires displacement of the insulating, fiber coat resin, substantially surrounding metal fibers in the vicinity of the conductive trace **16** of the assembly. Removal of insulation allows contact between the bare fibers and the conductive trace **16** during the heat staking process.

SAMSUNG EXHIBIT 1010, Page 238

[0047] Heat staking attaches an EMI shielding cover **12** over a printed circuit **18** using a heat staking tool **14** to precisely heat at least a portion of the perimeter of the shielding cover close to the contact edge **20**. Alignment of the contact edge **20** with the conductive trace **16** of the printed circuit **18** usually occurs before applying heat. Precise application of heat requires design of the heat staking tool **14** according to the shape of the contact edge **20** of the shielding cover **12**. The heated portion of the tool, in contact with the shielding cover, describes a track, up to only a few millimeters wide, around the perimeter of the cover. Use of the term, "die profile edge" **22** allows further description of this portion of the staking tool **14**, which needs some modification for optimum shielding cover **12** attachment to the printed circuit 18. The modification appears as a groove or channel **24** machined into the profile edge 22. During heat staking of a shielding cover **12** to a printed circuit **18**, the profile edge **22** raises the temperature at the contact edge **20** causing the fiber coat to soften. Pressure, applied to the heat staking tool **14**, causes metal fibers, of the EMI shield **12**, to establish metal to metal contact with the conductive trace **16** of the printed circuit. Softened fiber coat, displaced by this process, flows away from the contact edge **20** with some collecting in the space provided by the groove **24** in the profile edge **22.** Absence of a profile edge groove **24** causes inconsistent electrical connection between the contact edge **20** and the conductive trace **16** with resulting variability in the electrical resistance of the connection.

[0048] The benefits of EMI shielding composite sheets of the invention may be extended to other applications following the discovery that the planar sheets or thermoformed preforms, made therefrom, can provide EMI shielding to injection molded articles. For this purpose, the EMI shielding structure, either in sheet form or thermoformed preform, is inserted in the mold prior to injecting the molding resin layer. This provides a layer of EMI shielding material as part of the injection molded structure.

[0049] The invention is further understood by reference to the following non-limiting examples.

Experimental - Composite Sheet Formation

[0050] Samples of EMI shielding material, made according to the following Examples 1C - 5, were evaluated by thermoforming to the same shape, under the same shaping conditions. In particular molded EMI shielding cover samples were inspected, after the thermoforming process, for evidence of bare metal, spheroidal protrusions, as surface defects and for EMI shielding effectiveness.

Metal Fiber Mat Preparation

[0051] Fabrication of a non-woven metallic sheet involves the steps of extruding a molten stream from a metallic melt, distributing the stream on a planar surface as a randomly oriented mat of metal fibers, taking care to avoid fusion between fibers at points of intersection and thereafter allowing the metal mat to cool.

Metal Fiber Mat A

[0052] Metal fiber mat A, contains randomly oriented metal fibers, formed as previously described. The fibers comprise tin/bismuth alloy fibers weighing about 650 g/M^2 and melting at 138°C.

Polymer Fiber Mat B

[0053] Fiber mat B, used in comparative Example I C, is a melt-blown, non-woven, polymer web formed using a 50: 50 blend of ethylene vinyl acetate copolymers VYNATHENE EY 902-30 (available from Quantum Chemical Corp.) and ESCORENE 7520 (available from Exxon Chemical Co.). The resulting melt-blown web weighs about 160 g/M^2.

Comparative Example 1C

[0054] Metal fiber mat A was formed directly on a surface of polymer fiber mat B to provide a composite combining a metal fiber layer with a blown microfiber polymer layer. The composite was protected on either side by several sheets of silicone release paper and pressed for 5 seconds in a platen press operating at a temperature of about 70°C, under a load of 341-454 kg to partially drive the metal fibers into the polymer layer. Multiple layers of release paper protected the metal fibers from sintering and distortion, both of which may adversely affect the EMI shielding effectiveness of subsequently thermoformed structures.

[0055] The resulting composite structure of Example 1C was porous due to the combination of an unprotected, randomly oriented metal layer with a melt blown polymer web. Porous structures cannot be thermoformed, as described below, because air passes through the sheets preventing deflection of the softened sheet during application of vacuum or air pressure. Therefore, this comparative sample was combined with a continuous sheet of 0.25 mm polycarbonate prior to the thermoforming operation. Inspection of the metal fiber mat after thermoforming revealed surface defects

SAMSUNG EXHIBIT 1010, Page 239

of spheroidal protrusions, as shiny bare metal beads unprotected by electrically insulating fiber-coat material. In this example the metal fibers were not substantially surrounded by a fiber-coat.

Example 2C

[0056] Fiber mat A was formed directly on one surface of a sheet of 0.25 mm thick polycarbonate (GE #8B35 VIM - from GE Plastics-Structured Products). A film of 0.15 mm thick ethylene vinyl acetate (BYNEL E 418 - available from E.I. DuPont de Nemours), extruded at 235°C over the metal fibers, provided a sandwich composite which then passed through a pair of heated nip rollers. The chromed steel roller, next to the BYNEL E 418 layer, operated at a surface temperature of 113°C with a silicone release liner interposed to prevent sticking of the layer to the roller surface. A rubber roller, controlled at 96°C abutted the surface of the polycarbonate sheet. At the prevailing temperatures of the rollers, there was insufficient polymer flow to substantially surround the metal fibers. The appearance of the laminate provided evidence of air entrapment between the layers of film and the fiber mat. A thermoformed sample, of the sandwich composite, revealed evidence of bleeding of molten metal to form spheroidal protrusions outside the ethylene vinyl acetate layer.

Example 3

[0057] Fiber mat A was formed directly on a surface of a sheet of 0.25 mm thick polycarbonate (LEXAN 8010MC from GE Plastics-Structured Products). A 0.20 mm thick film of ethylene vinyl acetate (BYNEL E 418 available from E.I. DuPont de Nemours), extruded at 235°C over the top of the metal fibers, sealed them between polymer layers. The resulting composite then passed through a gap of about 0.50 mm formed by nip rollers operating at 121°C. A silicone release cover, over the roller contacting the BYNEL side of the composite, prevented sticking at the interface.

Example 4

[0058] A sheet of 0.25 mm thick polycarbonate (LEXAN 8010MC from GE Plastics-Structured Products) was coated with ethylene vinyl acetate (BYNEL E 418 available from E.I. DuPont de Nemours) to a thickness of 0.10 mm, using extrusion coating at 235°C. The next step of composite preparation involved formation of metal fiber mat A against the layer of ethylene vinyl acetate. A 0.10 mm thick film of ethylene vinyl acetate (BYNEL E 418 available from E.I. DuPont de Nemours), extruded at 235°C over the top of the metal fibers, then sealed them between layers of ethylene vinyl acetate. The resulting composite then passed through a gap of about 0.50 mm between a steel roller and a back-up rubber roller, forming nip rollers, operating at 113°C. A silicone release cover, over the steel roller contacting the BYNEL side of the composite, prevented sticking at the interface.

Example 5

[0059] A 0.64 mm thick film of ethylene vinyl acetate (DUPONT ELVAX 350) was extruded at 177°C onto metal fiber mat A, which was supported by a silicone belt. The two materials were joined by passing them through chrome plated steel nip rollers. A 20 cm x 20 cm sample of the resulting composite was placed metal fiber side up onto a 30 cm x 30 cm sheet of 0.26 mm thick sheet of LEXAN 8010MC polycarbonate (obtained from GE Plastics-Structured Products). This composite was pressed together in a platen press heated to 100°C at 455 kg for 10 seconds. The resulting composite comprises a polycarbonate carrier base, an intermediate layer of Elvax 350 and a top layer of tin bismuth fibers substantially embedded into the surface of the Elvax 350.

Example 6

[0060] Two sheets of acrylic adhesive were prepared as follows: 3M acrylic adhesive RD20789 (available from 3M), was mixed with 1.2% by weight of 30 micron diameter silver coated glass spheres obtained from Potters Industries, Inc., Parsippany, NJ. This mixture was coated onto a sheet of release liner using a notched bar coater at a wet thickness of 0.26 mm. After drying the adhesive layer sheets, one was laminated onto a 0.13 mm thick sheet of LEXAN 8010MC polycarbonate (obtained from GE Plastics-Structured Products) measuring 30 cm x 30 cm, by placing the adhesive side of one of the sheets against the polycarbonate, pressing it down from the release liner side and then peeling off the release liner to transfer the adhesive layer to the polycarbonate sheet. A layer of Mat A was then placed on top of the adhesive layer. The second adhesive layer was then applied to metal fiber mat A, as described previously, producing a metal layer sandwiched between layers of conductive adhesive. This composite was placed between multiple sheets of release liner to pad the material prior to pressing in a platen press set at 455 kg load for 20 seconds at 100°C.

SAMSUNG EXHIBIT 1010, Page 240

The Process of Thermoforming

[0061] Thermoforming, especially associated with the present invention, refers to the process that combines a shaping mold, heat and either pressure or vacuum to change a planar sheet of softened, thermoplastic material into a contoured structure which, on cooling, substantially replicates the shape of the mold. Equipment for the basic forming method includes parallel acting frames, to hold the thermoplastic sheet; heaters above and/or below the sheet-stock to be softened; molds, either male or female, to provide the shape against which the softened sheet will be thermoformed; and equipment for increasing or reducing air pressure to deflect the softened sheetstock for shaping.

Thermoformed Sample Preparation

[0062] Composite sheets of the invention had a planar structure before shaping in a thermoformer having a centrally positioned clamping system to hold a sheet between heaters positioned above and below the clamping station. Heating of a composite sheet may use either one of the heaters or both together. Examples 1C-6 used only the lower heater operating at a temperature of 538°C. Sheets were exposed to this temperature for about 0.5 minute.

[0063] Each of the composite sheets of Examples 2C, 3, 4 and 5 already included a layer of 0.25 mm thick polycarbonate while Example 6 included a 0.13 mm polycarbonate.

[0064] After softening, a sheet was positioned in close proximity to the shaping mold by moving the clamping structure. The thermoformed sample, used for evaluation, was a cylindrical bowl having a flat, circular base of 17.6 cm diameter with a circular wall extending 4.1 cm vertically from the base. With the sheet and clamping structure suitably positioned to form an air-tight seal with the upper edge of the circular wall of the mold, vacuum was applied to draw the sheet into the mold until the surface of the sheet was in close contact with the mold wall. This shaping required significant stretching of the composite sheet between the upper edge of the circular wall and the juncture between the wall and the base. After cooling, the composite material adopted the shape of the cylindrical bowl.

[0065] Metal fiber stretching is at a maximum in the corner formed by the circular wall and the base portion of the bowl-shaped composite material. This portion is therefore most subject to fiber rupture and separation during thermoforming. When the fibers become molten, extension of the metal strands is limited only by the surface tension of the molten metal. Any means to preserve the molten metal in the form of a fiber will improve potential fiber elongation. This is demonstrated by the results of forming the composite sheets of Examples 1C-6, described below and presented in Table 1.

[0066] In thermoformed bowl preparation, there was a very significant difference between Comparative Examples 1C and 2C, using a metal mat with insufficient fibercoat, and the other examples involving metal mats either substantially embedded in a polymer layer or having a polymer overcoat applied. Evidence of poorer performance of Examples 1C and 2C was the appearance, during thermoforming of the composite sheets, of metal beads by the coalescence process previously described. As the metal beads grow, they gain volume by accepting the flow of molten metal out of surrounding fibers until they emerge as isolated spheroidal protrusions outside the profile of the thermoformed articles. Existence of multiple protrusions is harmful to EMI shielding effectiveness and increases the probability of short-circuiting an electronic device.

[0067] Examples 3-6 were free from spheroidal protrusions. This shows the improvement provided by protecting the metal mat by overcoating or substantially embedding it in a polymer fiber-coat matrix before heating and shaping. Table 1 shows the results of testing composite sheets of the invention to determine incidence of metal bead formation and EMI shielding efficiency. The consistently higher shielding performance, measured in decibels (dB), for the bead-free samples, clearly demonstrates the improvement associated with these EMI shielding covers.

[0068] Example 6, having an adhesive coating over the metal fiber mat, may be adhesively attached and is capable, where needed, of establishing electrical connection with a suitable ground plane. Housings thermoformed from Example 6, attached to conductive surfaces by pressure, provide connections with electrical resistance less than 100 milliohms between the metal fiber mat A and the conductive surface.

Table 1 -

Thermoformed Sheet Performance			
Example	Oven Dwell Time (minute)	EMI Shielding (dB)	Metal Bead Formation
Example 1C	0.46	20	7 beads
Example 2C	0.45	37	11 beads
Example 3	0.46	45	None
Example 4	0.46	50	None

SAMSUNG EXHIBIT 1010, Page 241

Table 1 - (continued)

Thermoformed Sheet Performance			
Example	Oven Dwell Time (minute)	EMI Shielding (dB)	Metal Bead Formation
Example 5	0.59	50	None
Example 6	0.46	50	None

Injection Molding of Composite Sheets and Thermoformed Preforms

Example 7

[0069] A polycarbonate sheet of about 0.13 mm thickness (LEXAN 8010MC polycarbonate from GE Plastics-Structured Products) was coated with a thin layer of polyethylene using a 10% of VYTEL PE 200 in methyl ethyl ketone, using a #5 Meyer bar. After oven-drying these sheets at 105°C for two minutes, a sample of metal fiber mat A was applied to the VYTEL PE 200 layer. The composite was protected on either side using multiple sheets of silicone release paper, then laminated for 10 seconds, using a heated platen press operating at about 340 Kgf and 127°C. Upon cooling, the resulting samples were overcoated by hand-held spray bottle, using a solution of 10% solids ADCOTE 37P295 wax dispersion in water to a wet coating weight from about 10 gms/100cm^2 to about 30 gms/100cm^2. The completed composite sheet was dried in an oven at a temperature of 105°C for about 10 minutes.

Injection Molding of Example 7

[0070] A pre-formed insert was made from the material of example 7 using the thermoforming equipment previously described. The top heater of the thermoformer was turned off and the bottom heater was set at 538°C. The sheet was heated before forming in the thermoforming oven for 0.23 minutes. The sheet of example 7 was formed into a substantially rectangular pre-form having dimensions of approximately 3.5 cm x 9.8 cm x 1.0 cm deep. This part was pre-formed to fit snugly inside an injection mold. The pre-form was then placed into one side of the injection mold (the side opposite the gate) which in turn was mounted in a 70 ton Arburg molding machine. The mold was closed and the cavity was injected with a full charge of Lexan 141R polycarbonate obtained from GE Plastics, having a melt temperature of 300°C. The injection rate was 20 cc/s, the mold temperature was 40°C, and the cool time was 15 s. The mold was opened after the part cycle was completed and the result was an injection molded part, of a molding resin, with a smooth inner surface including an electrically conductive network of tin bismuth alloy fibers having a surface resistance of less than 200 milliohms from corner to corner as measured using a Fluke Model 75 Multimeter obtained from John Fluke Mfg. Co. Inc.

Example 8

[0071] Fiber mat A was spray overcoated using a 5% solution of PETG (KODAR 6763 from Eastman Chemical Co.) in methylene chloride. Spray application of the overcoat by a Binks spray gun with a #63B nozzle gave a wet coating weight of between about 20.0 g and about 30.0 g per 100 cm^2. After drying at room temperature, the resulting fiber mats were heat laminated onto a 0.13 mm thick PETG (KODAR 6763) plastic sheet for 5 seconds using a heated platen press as in Example 6.

Injection Molding of Example 8

[0072] A pre-formed insert was made from the material of example 8 using the thermoforming equipment previously described. The top heater of the thermoformer was set at 316°C and the bottom heater was set at 260°C. The sheet was heated before forming in the thermoforming oven for 0.28 minutes. The sheet of example 8 was formed into a substantially rectangular pre-form having dimensions of approximately 3.5 cm x 9.8 cm x 1.0 cm deep. This part was pre-formed to fit snugly inside an injection mold. The pre-form was then placed into one side of the injection mold (the side opposite the gate) which in turn was mounted in a 70 ton Arburg molding machine. The mold was closed and the cavity was injected with a full charge of Vistolen P2000 polypropylene having a melt temperature of 240°C. The injection rate was 40 cc/s, the mold temperature was 40°C and the cool time was 30 s. The mold was opened after the part cycle was completed and the result was an injection molded, resin part with a smooth inner surface including an electrically conductive network of tin/bismuth alloy fibers having a surface resistance of less than 200 milliohms from comer to comer as measured using a Fluke Model 75 Multimeter obtained from John Fluke Mfg. Co. Inc.

SAMSUNG EXHIBIT 1010, Page 242

Example 9

[0073] Composite sheets were prepared as described in Example 7 except the overcoat of ADCOTE 37P295 was omitted. This was not needed since the material did not require thermoforming prior to molding.

Injection Molding of Example 9

[0074] The film composite of Example 9 was taped onto the female side of the injection mold. The mold was mounted in a 150 Ton Demag Ergo Tech 150610 injection molding machine. The mold was then closed around the film which resulted in an initial cold forming of the plastic/metal fiber composite. Cycoloy HF1120 ABS/Polycarbonate blend obtained from GE Plastics, having a melt temperature of 270°C, was then injected into the mold. The injection rate was 30 cc/s, the mold temperature was 40°C, and the cooling time was 15 s. The mold was opened after the part cycle was completed and the result was an injection molded part having dimensions of approximately 4.8 cm x 9.7 cm x 0.4 cm with a smooth inner surface including an electrically conductive network of tin bismuth alloy fibers having a surface resistance of less than 200 milliohms from comer to comer as measured using a Fluke Model 75 Multimeter obtained from John Fluke Mfg. Co. Inc.

Example 10

[0075] Composite sheets were prepared as described in Example 8 except the overcoat of PETG was omitted. This was not needed since the material did not require thermoforming prior to molding.

Injection Molding of Example 10

[0076] The film composite of Example 10 was taped onto the female side of the injection mold. The film was preheated on the mold using a hand held heat gun for approximately 15 seconds. The mold was then closed around the film which resulted in an initial cold forming of the plastic/metal fiber composite. The mold was closed and the cavity was injected with a full charge of Cycoloy HF1120 ABS/Polycarbonate blend obtained from GE Plastics, having a melt temperature of 270°C. The injection rate was 30 cc/s, the mold temperature was 70°C, and the cooling time was 15 s. The mold was opened after the part cycle was completed and the result was an injection molded part having dimensions of approximately 4.8 cm x 9.7 cm x 0.4 cm with a smooth inner surface including an electrically conductive network of tin bismuth alloy fibers having a surface resistance of less than 200 milliohms from comer to corner as measured using a Fluke Model 75 Multimeter obtained from John Fluke Mfg. Co. Inc.

Example 11

[0077] A polycarbonate sheet of about 0.13 mm thickness (LEXAN 8B35 polycarbonate from GE Plastics-Structured Products) was coated, by lamination, with a layer of ethylene methyl acrylate copolymer (EMAC SP2207 from Chevron Chemical Co. - Specialty Polymers), about 0.10 mm thick. The lamination step used a heated platen press operating at 22,000 Kgf pressure for about 20 s at 125°C.

[0078] Metal fiber mat A, was placed on the EMAC SP2207 layer. The composite was protected on either side using multiple sheets of silicone release paper, then laminated for 20 s, using a heated platen press operating at about 25,000 Kgf and 110°C.

Injection Molding of Example 11

[0079] A pre-formed insert was made from the material of example 11 using the thermoforming equipment previously described. The top heater of the thermoformer was turned off and the bottom heater was set at 538°C. The sheet was heated before forming in the thermoforming oven for about 0.3 minute. The sheet of example 11 was formed into a substantially rectangular pre-form having dimensions of approximately 4.8 cm x 9.7 cm x 0.4 cm deep. This part was pre-formed to fit snugly inside an injection mold. The pre-form was then placed into one side of the injection mold (the side opposite the gate) which in turn was mounted in a 70 ton Arburg Allrounder 700-230-305 ECO molding machine. The mold was closed and the cavity was injected with a full charge of LEXAN 940 polycarbonate, obtained from GE Plastics, having a melt temperature of 300°C. The injection rate was about 20 cc/s, the mold temperature was about 90°C, and the cooling time was about 15 s. The mold was opened after the part cycle was completed and the result was an injection molded part of molded resin formed over an electrically conductive network of tin bismuth alloy fibers having a surface resistivity of less than 200 milliohms from comer to corner as measured using a Fluke Model 75 Multimeter obtained from John Fluke Mfg. Co. Inc.

SAMSUNG EXHIBIT 1010, Page 243

[0080] A second sample of a preform of Example 10, made as described previously, was placed, as a preformed insert, in a mold attached to a 70 ton Arburg Allrounder 700-230-305 ECO injection molding machine. After closing, the mold cavity was filled by injection with a full charge of ABS-polycarbonate blend (Cycoloy C1200HF, obtained from GE Plastics) having a melt temperature of about 270°C. At a mold temperature of about 40°C the resin injection rate was about 20 cc/s followed by cooling for about 15 s. The injection molded part had the same performance as the molding produced with LEXAN 940.

Example 12

[0081] A polycarbonate sheet, about 0.13 mm thick, (LEXAN 8B35 available from GE Plastics - Structured Products) was coated on both sides, by laminating about 0.10 mm of ethylene methyl acrylate copolymer (EMAC SP2207 available from Chevron Chemical Co. - Specialty Polymers) using a platen press operating at about 22,000 Kgf for about 20 s and at a temperature of about 125°C.

[0082] Metal fiber mat A was placed against one of the layers of EMAC SP 2207 before placing the composite between multiple sheets of silicone release paper then applying pressure using a heated platen press at 25,000 Kgf for about 20 s. at about 110°C.

Injection Molding of Example 12

[0083] A pre-formed insert was made from composite sheets of Example 12 as previously described for Example 11. The preform was placed in a mold attached to a 70 ton Arburg Allrounder 700-230-305 ECO injection molding machine. After closing, the mold cavity was filled by injection with a full charge of high density polyethylene (Petrothene LM6187, available from Quantum Co.) having a melt temperature of about 210°C. With mold temperature held at room temperature, the resin injection rate was about 20 cc/s followed by cooling for about 20 s. The resulting part showed good adhesion between the injected polyethylene layer and the preformed insert and had a smooth inner surface including an electrically conductive network of tin busmuth alloy fibers with a surface resistivity less than 200 milliohms measured using a Fluke Model 75 Multimeter obtained from John Fluke Mfg. Co. Inc.

[0084] Examples presented herein are not intended as limiting of the invention, the scope of which is defined by the following claims.

Claims

1. An EMI shielding enclosure for an electronic assembly, comprising:

    a ground plane; and
    a shielding cover, formed by thermoforming a composite sheet, said cover comprising:

        a non-porous carrier sheet;
        a fibrous metal mat having an outer surface and a contact surface, said contact surface adjacent said carrier sheet, said metal mat comprising low melting metal fibers that melt during thermoforming of said shielding cover;
        a fiber-coat to insulate said metal fibers by substantially surrounding said fibers, said fiber-coat overlying said metal fibers at said outer surface of said mat by less than 0.15 mm, said fiber-coat substantially extending through said mat to said non-porous carrier sheet; and
        a contact edge to form an electrical connection to said ground plane, said electrical connection made by adhesion of said contact edge against said ground plane, at temperatures up to 200°C, said cover essentially free from spheroidal protrusions.

2. The shielding enclosure of claim 1 wherein said non-porous carrier sheet has a softening point below 150°C.

3. The shielding enclosure of claim 1 wherein said non-porous carrier sheet is a polymer selected from the group consisting of polycarbonate, acrylonitrile butadiene styrene copolymers (ABS), styrene acrylonitrile copolymers (SAN), polystyrene, polyvinyl chloride, polyether imide, polypropylene, polyethylene, polybutylene, polyamide, polyethylene terephthalate, polybutylene terephthalate and polyethylene naphthalate, polymethyl methacrylate, ethylene butyl acrylate copolymers, polyacrylonitrile, polyarylketones, polyethersulfone, polyphenylene sulfide, polyurethane, styrene butadiene styrene copolymers, styrene ethylene propylene styrene copolymers, and vinyl acetate.

SAMSUNG EXHIBIT 1010, Page 244

4. The shielding enclosure of claim 1 wherein said fiber coat is selected from the group consisting of thermoplastic polymers, hot melt adhesive polymers and pressure sensitive adhesive polymers.

5. The shielding enclosure of claim 4, wherein said thermoplastic polymers are selected from the group consisting of ethylene vinyl acetate copolymers, vinyl acetate, polyethylene, polypropylene, polyurethane, styrene butadiene styrene copolymers, styrene ethylene propylene styrene copolymers, ethylene methyl acrylate copolymers, copolymers including maleic anhydride and acrylic acid, and paraffn wax.

6. The shielding enclosure of claim 4, wherein said hot melt adhesive polymers are selected from the group consisting of ethylene vinyl acetate copolymers, vinyl acetate, polyethylene, polypropylene, polyurethane, styrene butadiene styrene copolymers, styrene ethylene propylene styrene copolymers, and ethylene methyl acrylate copolymers.

7. The shielding enclosure of claim 1 wherein said fiber coat adheres proximate said ground plane to secure said electrical connection between said contact edge and said ground plane.

8. The shielding enclosure of claim 1 wherein said fiber coat includes conductive particles selected from the group consisting of metallic powders, metallic granules, metallic beads, metallic flakes, metallic fibers, metal coated powders, metal coated granules, metal coated beads, metal coated flakes and metal coated fibers..

9. The shielding enclosure of claim 1 wherein said low melting metal fibers are selected from the group consisting of tin, lead, bismuth, cadmium, indium, gallium, zinc, mixtures thereof, alloys thereof, and alloys thereof containing at least one element selected from the group consisting of antimony, aluminum, copper, silver, gold, nickel, cobalt, and iron.

10. A method for forming an EMI shielding enclosure around an electronic assembly according to claim 1, comprising the steps of:

(a) providing an electronic assembly, having a ground plane including a conductive trace;
(b) providing a thermoformed shielding cover having a contact edge, said shielding cover further comprising

a non-porous carrier sheet;
a fibrous metal mat having an outer surface and a contact surface, said contact surface adjacent said carrier sheet, said metal mat comprising low melting metal fibers that melt during thermoforming of said shielding cover; and
a fiber-coat to insulate said metal fibers by substantially surrounding said fibers, said fiber-coat overlying said metal fibers at said outer surface of said mat by less than 0.15 mm, said fiber-coat substantially extending through said mat to said non-porous carrier sheet;
(c) aligning said contact edge with said conductive trace;
(d) adhering said contact edge against said conductive trace to form an electrical connection between said edge and said trace.

11. A shaped EMI shielding cover, essentially absent spheroidal protrusions, comprising:

a non-porous carrier sheet having first and second surfaces;
a fibrous metal mat having an outer surface and a contact surface, said contact surface adjacent said first surface of carrier sheet, said metal mat comprising low melting metal fibers that melt during thermoforming of said shielding cover; and
a fiber-coat to electrically insulate said metal fibers by substantially surrounding said fibers, said fiber-coat overlying said metal fibers at said outer surface of said mat by less than 0.15 mm, said fiber-coat substantially extending through said mat to said non-porous carrier sheet.

12. The shaped shielding cover of claim 11, further comprising a molding resin layer applied to said second surface of said carrier sheet.

Patentansprüche

1. Gehäuse zur Abschirmung von elektromagnetischen Interferenzen für eine elektronische Anordnung, mit:

SAMSUNG EXHIBIT 1010, Page 245

- einer Masseebene; und
- einer durch Thermoformen einer Verbundbahn gebildeten Abschirmabdeckung, wobei die Abdeckung aufweist:
- eine nicht poröse Trägerbahn;
- eine Metallfasermatte mit einer Außenfläche und einer Kontaktfläche, wobei die Kontaktfläche der Trägerschicht benachbart ist, wobei die Metallmatte Metallfasern mit niedrigem Schmelzpunkt aufweist, die während des Thermoformens der Abschirmabdeckung schmelzen;
- eine Faserbeschichtung, welche die Metallfasern im wesentlichen umgibt und so isoliert, wobei die Faserbeschichtung die Metallfasern auf der Außenfläche der Matte mit weniger als 0,15 mm überdeckt, und wobei sich die Faserbeschichtung im wesentlichen durch die Matte bis zur nicht porösen Trägerbahn erstreckt; und
- einen Kontaktrand zur Bildung einer elektrischen Verbindung mit der Masseebene, wobei die elektrische Verbindung durch Anhaften des Kontaktrands an der Masseebene bei einer Temperatur bis zu 200° C gebildet ist, wobei die Abdeckung im wesentlichen frei von kugelförmigen Vorsprüngen ist.

2. Abschirmgehäuse nach Anspruch 1, bei dem die nicht poröse Trägerbahn einen Erweichungspunkt unter 150° C hat.

3. Abschirmgehäuse nach Anspruch 1, bei dem die nicht poröse Trägerbahn aus einem Polymer besteht, das aus der folgenden Gruppe ausgewählt ist: Polycarbonat, Acryolonitril-Butadien-Styrol-Copolymere (ABS), Styrol-Acrylonitril-Copolymere (SAN), Polystyrol, Polyvinylchlorid, Polyetherimid, Polypropylen, Polyethylen, Polybutylen, Polyamid, Polyethylenterephthalat, Polybutylenterephthalat und Polyethylennaphthalat, Polymethylmetacrylat, Ethylenbutylacrylat-Copolymere, Polyacrylonitril, Polyarylketone, Polyethersulfon, Polyphenylensulfid, Polyurethan, Styrolbutadienstyrol-Copolymere, Styrolethylenpropylenstyrolcopolymere und Vinylacetat.

4. Abschirmgehäuse nach Anspruch 1, bei dem die Faserbeschichtung aus der folgenden Gruppe ausgewählt ist: thermoplastische Polymere, Heißschmelzkleberpolymere und Haftkleberpolymere.

5. Abschirmgehäuse nach Anspruch 4, bei dem die thermoplastischen Polymere aus derfolgenden Gruppe gewählt sind: Ethylenvinylacetat-Copolymere, Vinylacetat, Polyethylen, Polypropylen, Polyurethan, Styrolbutadienstyrol-Copolymere, Styrolethylenpropylenstyrol-Copolymere, Ethylenmethylacrylat-Copolymere, Copolymere mit Maleinsäureanhydrid und Acrylsäure, und Paraffinwachs.

6. Abschirmgehäuse nach Anspruch 4, bei dem die Heißschmelzkleberpolymere aus der folgenden Gruppe gewählt sind: Ethylenvinylacetat-Copolymere, Vinylacetat, Polyethylen, Polypropylen, Polyurethan, Styrolbutadienstyrol-Copolymere, Styrolethylenpropylenstyrol-Copolymere und Ethylenmethylacrylat-Copolymere.

7. Abschirmgehäuse nach Anspruch 1, bei dem die Faserbeschichtung nahe der Masseebene haftet, um die elektrische Verbindung zwischen dem Kontaktrand und der Masseplatte zu sichern.

8. Abschirmgehäuse nach Anspruch 1, bei dem die Faserbeschichtung leitfähige Partikel enthält, die aus der folgenden Gruppe ausgewählt sind: Metallpulver, Metallgranulate, Metallkügelchen, Metallspäne, Metallfasern, metallbeschichtete Pulver, metallbeschichtete Granulate, metallbeschichtete Kügelchen, metallbeschichtete Späne und metallbeschichtete Fasern.

9. Abschirmgehäuse nach Anspruch 1, bei dem die Metallfasern mit niedrigem Schmelzpunkt aus der folgenden Gruppe ausgewählt sind: Zinn, Blei, Wismut, Cadmium, Indium, Gallium, Zink, Mischungen derselben, Legierungen derselben und Legierungen, die wenigstens ein Element aufweisen, das aus der folgenden Gruppe ausgewählt ist: Antimon, Aluminium, Kupfer, Silber, Gold, Nickel, Kobalt und Eisen.

10. Verfahren zur Herstellung eines EMI-Abschirmgehäuses um eine elektronische Anordnung nach Anspruch 1, mit den folgenden Schritten:

(a) Vorsehen einer elektronischen Anordnung mit einer Masseebene, die eine Leiterbahn aufweist;

SAMSUNG EXHIBIT 1010, Page 246

(b) Vorsehen einer thermogeformten Abschirmabdeckung mit einem Kontaktrand, wobei die Abschirmabdekkung ferner aufweist:

- eine nicht poröse Trägerbahn;
- eine Metallfasermatte mit einer Außenfläche und einer Kontaktfläche, wobei die Kontaktfläche der Trägerschicht benachbart ist, wobei die Metallmatte Metallfasern mit niedrigem Schmelzpunkt aufweist, die während des Thermoformens der Abschirmabdeckung schmelzen;
- eine Faserbeschichtung, welche die Metallfasern im wesentlichen umgibt und so isoliert, wobei die Faserbeschichtung die Metallfasern auf der Außenfläche der Matte mit weniger als 0,15 mm überdeckt, und wobei sich die Faserbeschichtung im wesentlichen durch die Matte bis zur nicht porösen Trägerbahn erstreckt;

(c) Ausrichten des Kontaktrandes mit der Leiterbahn;

(d) Anhaften des Kontaktrandes an der Leiterbahn zur Bildung einer elektrischen Verbindung zwischen dem Rand und der Bahn.

11. Geformte EMI-Abschirmabdeckung, im wesentlichen ohne kugelförmige Vorsprünge, mit:

- einer nicht porösen Trägerbahn mit einer ersten und einer zweiten Fläche;
- eine Metallfasermatte mit einerAußenfläche und einer Kontaktfläche, wobei die Kontaktfläche der Trägerschicht benachbart ist, wobei die Metallmatte Metallfasern mit niedrigem Schmelzpunkt aufweist, die während des Thermoformens der Abschirmabdeckung schmelzen; und
- eine Faserbeschichtung, welche die Metallfasern im wesentlichen umgibt und so isoliert, wobei die Faserbeschichtung die Metallfasern auf der Außenfläche der Matte mit weniger als 0,15 mm überdeckt, und wobei sich die Faserbeschichtung im wesentlichen durch die Matte bis zur nicht porösen Trägerbahn erstreckt.

12. Geformte Abschirmabdeckung nach Anspruch 11, ferner mit einer auf der zweiten Fläche der Trägerbahn aufgebrachten Formharzschicht.

Revendications

1. Enceinte de blindage contre les EMI pour un ensemble électronique, comprenant :

un plan de masse ; et

un couvercle de blindage, formé par thermoformage d'une feuille composite, ledit couvercle comprenant :

une feuille de support non poreuse ;

une matrice de métal fibreux ayant une surface externe et une surface de contact, ladite surface de contact étant adjacente à ladite feuille de support, ladite matrice de métal comprenant des fibres métalliques à faible point de fusion qui fondent pendant le thermoformage dudit couvercle de blindage ;

un revêtement de fibre pour isoler lesdites fibres métalliques en entourant sensiblement lesdites fibres, ledit revêtement de fibre recouvrant lesdites fibres métalliques au niveau de ladite surface externe de ladite matrice par moins que 0,15 mm, ledit revêtement de fibre s'étendant sensiblement sur toute ladite matrice à travers ladite matrice vers ladite feuille de support non poreuse ; et

un bord de contact pour former une connexion électrique avec ledit plan de masse, ladite connexion électrique étant effectuée par adhésion dudit bord de contact contre ledit plan de masse à des températures allant jusqu'à 200° C, ledit couvercle étant essentiellement dépourvu de protubérances sous forme de sphère.

SAMSUNG EXHIBIT 1010, Page 247

2. Enceinte de blindage selon la revendication 1, dans laquelle ladite feuille de support non poreuse présente un point de ramollissement en dessous de 150° C.

3. Enceinte de blindage selon la revendication 1, dans laquelle ladite feuille de support non poreuse est un polymère choisi dans le groupe constitué du polycarbonate, des copolymères d'acrylonitrile butadiène styrène (ABS), des copolymères styrène acrylonitrile (SAN), du polystyrène, du chlorure de polyvinyle, du polyéther imide, du polypropylène, du polyéthylène, du polybutylène, du polyamide, du polyéthylène téréphtalate, du polybutylène téréphtalate et du polyéthylène naphtalate, du poly méthacrylate, de méthyle des copolymères d'éthylène acrylate de butyle, du polyacrylonitrile, des polyarylcétones, du polyéthersulfone, du sulfure de polyphénylène, du polyuréthane, des copolymères styrène butadiène styrène, des copolymères styrène éthylène propylène styrène et de l'acétate de vinyle.

4. Enceinte de blindage selon la revendication 1, dans laquelle ledit revêtement de fibre est choisi dans le groupe constitué des polymères thermoplastiques, des polymères adhésifs à fusion chaude et des polymères autoadhésifs.

5. Enceinte de blindage selon la revendication 4, dans laquelle lesdits polymères thermoplastiques sont choisis dans le groupe constitué des copolymères d'éthylène acétate de vinyle, de l'acétate de vinyle, du polyéthylène, du polypropylène, du polyuréthane, des copolymères styrène butadiène styrène, des copolymères styrène éthylène propylène styrène, des copolymères éthylène acrylate de méthyle, des copolymères incluant l'anhydride maléique et l'acide acrylique et de la cire de paraffine.

6. Enceinte de blindage selon la revendication 4, dans laquelle lesdits polymères adhésifs à fusion à chaud sont choisis dans le groupe constitué des copolymères éthylène acétate de vinyle, de l'acétate de vinyle, du polyéthylène, du polypropylène, du polyuréthane, des copolymères styrène butadiène styrène, des copolymères styrène éthylène propylène styrène, et des copolymères éthylène acrylate de méthyle.

7. Enceinte de blindage selon la revendication 1, dans laquelle ledit revêtement de fibre adhère à proximité dudit plan de masse pour assurer ladite connexion électrique entre ledit bord de contact et ledit plan de masse.

8. Enceinte de blindage selon la revendication 1, dans laquelle ledit revêtement de fibre inclut des particules conductrices choisies dans le groupe constitué des poudres métalliques, des granulés métalliques, des perles métalliques, des flocons métalliques, des fibres métalliques, des poudres revêtues de métal, des granulés revêtus de métal, des perles revêtues de métal, des flocons revêtus de métal et des fibres revêtues de métal.

9. Enceinte de blindage selon la revendication 1, dans laquelle les fibres métalliques à faible point de fusion sont choisies dans le groupe constitué de l'étain, du plomb, du bismuth, du cadmium, de l'indium, du gallium, du zinc, de leurs mélanges, de leurs alliages et de leurs alliages contenant au moins un élément choisi dans le groupe constitué de l'antimoine, de l'aluminium, du cuivre, de l'argent, de l'or, du nickel, du cobalt et du fer.

10. Procédé de formation d'une enceinte de blindage contre les EMI autour d'un ensemble électronique selon la revendication 1, comprenant les étapes consistant à :

(a) fournir un ensemble électronique ayant un plan de masse incluant une piste conductrice ;

(b) fournir un couvercle de blindage thermoformé ayant un bord de contact, ledit couvercle de blindage comprenant, en outre,

une feuille de support non poreuse ;

une matrice de métal fibreux ayant une surface externe et une surface de contact, ladite surface de contact étant adjacente à ladite feuille de support, ladite matrice de métal comprenant des fibres métalliques à faible point de fusion qui fondent pendant le thermoformagé dudit couvercle de blindage ; et

un revêtement de fibre pour isoler lesdites fibres métalliques en entourant sensiblement lesdites fibres, ledit revêtement de fibre recouvrant lesdites fibres métalliques au niveau de ladite surface externe de ladite matrice par moins que 0,15 mm, ledit revêtement de fibre s'étendant sensiblement à travers ladite matrice jusqu'à ladite feuille de support non poreuse ;

SAMSUNG EXHIBIT 1010, Page 248

(c) aligner ledit bord de contact avec ladite piste conductrice ;

(d) faire adhérer ledit bord de contact contre ladite piste conductrice pour former une connexion électrique entre ledit bord et ladite piste.

11. Couvercle de blindage contre les EMI façonné, essentiellement dépourvu de protubérances sous forme de sphère, comprenant :

une feuille de support non poreuse ayant des première et seconde surfaces ;

une matrice de métal fibreux ayant une surface externe et une surface de contact, ladite surface de contact étant adjacente à ladite première surface de la feuille de support, ladite matrice de métal comprenant des fibres métalliques à faible point de fusion qui fondent pendant le thermoformage dudit couvercle de blindage ; et

un revêtement de fibre pour isoler électriquement lesdites fibres métalliques en entourant sensiblement lesdites fibres, ledit revêtement de fibre recouvrant lesdites fibres métalliques au niveau de ladite surface externe de ladite matrice par moins que 0,15 mm, ledit revêtement de fibre s'étendant sensiblement à travers ladite matrice jusqu'à ladite feuille de support non poreuse.

12. Couvercle de blindage façonné selon la revendication 11, comprenant, en outre, une couche de résine de moulage appliquée à ladite seconde surface de ladite feuille de support.

SAMSUNG EXHIBIT 1010, Page 249

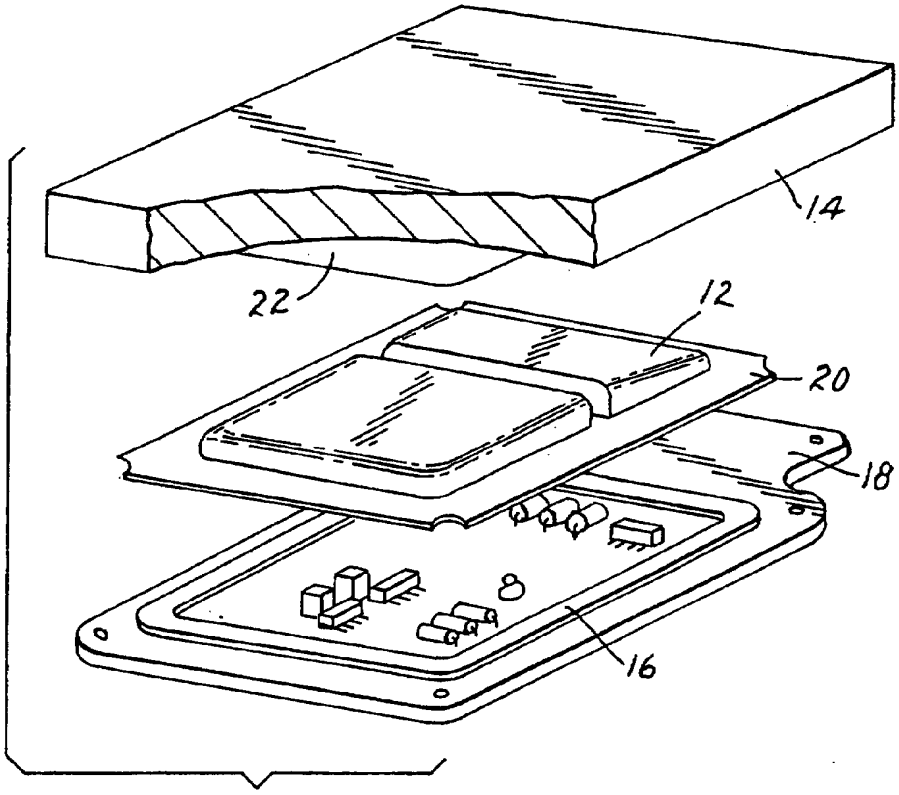


FIG. 1

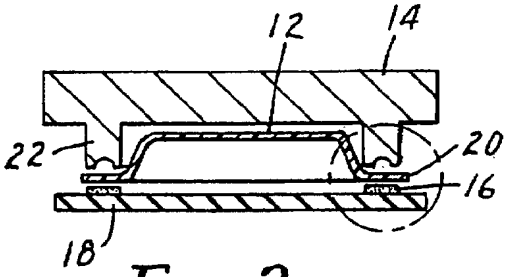


FIG. 2

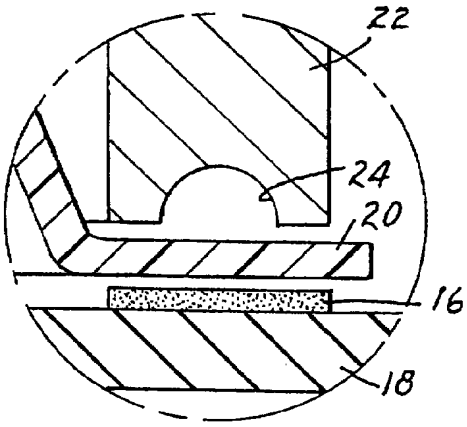


FIG. 2a

SAMSUNG EXHIBIT 1010, Page 250

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－348471

(43)公開日　平成11年(1999)12月21日

(51)Int.Cl.⁶	識別記号	ＦＩ	
Ｂ４２Ｄ　15/10	５２１	Ｂ４２Ｄ　15/10	５２１
Ｇ０６Ｋ　19/077		Ｇ０６Ｋ　19/00	Ｋ
19/10			Ｒ
19/00			Ｙ

審査請求　未請求　請求項の数３　ＯＬ　（全 ４ 頁）

(21)出願番号　特願平10－157148

(22)出願日　平成10年(1998)６月５日

(71)出願人　000001270
コニカ株式会社
東京都新宿区西新宿１丁目26番２号

(72)発明者　舟木　信介
東京都日野市さくら町１番地　コニカ株式会社内

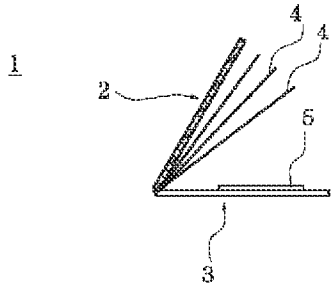
(72)発明者　野崎　裕美
東京都日野市さくら町１番地　コニカ株式会社内

(74)代理人　弁理士　鶴若　俊雄

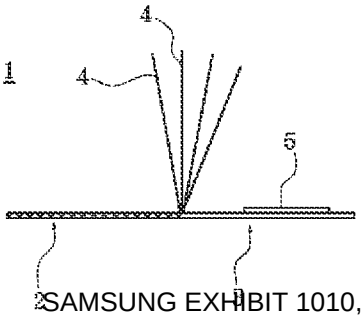
(54)【発明の名称】　冊子及びＩＣカードホルダ

(57)【要約】
【課題】外部からの盗聴電波よる偽造や変造をより一層有効に防止することが可能である。
【解決手段】冊子１は、非接触で外部と電波により情報の授受が可能なＩＣチップ、アンテナを有するＩＣユニット５及び／又はＩＣユニット５が設けられたＩＣカードＣＡを有し、少なくとも１頁４に電磁波を遮断もしくは通しにくいシールド部材を用いている。

(a)



(b)



1

【特許請求の範囲】

【請求項１】非接触で外部と電波により情報の授受が可能なＩＣチップ、アンテナを有するＩＣユニット及び／又はＩＣユニットが設けられたＩＣカードを有し、少なくとも１頁に電磁波を遮断もしくは通しにくいシールド部材を用いたことを特徴とする冊子。

【請求項２】前記頁に、表紙及び／又は裏表紙を含むことを特徴とする請求項１記載の冊子。

【請求項３】非接触で外部と電波により情報の授受が可能なＩＣチップ、アンテナを有するＩＣユニットが設けられたＩＣカードを保持するホルダを有し、このホルダが２つ折りになっており、前記ホルダの両面又は片面に電磁波を遮断もしくは微弱化する材料を少なくとも前記アンテナに対応した領域に被覆し、このホルダの２つ折りの内側に前記ＩＣカードを入れられるようにしたことを特徴とするＩＣカードホルダ。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、例えば、パスポート、預金通帳、社員証、学生証等の個人の身分を証明するに用いられるいわゆる冊子及びＩＣカードホルダに関する。

【０００２】

【従来の技術】パスポート、預金通帳、社員証や学生証等の個人の身分を証明するいわゆる冊子は、従来から用いられている。この冊子には非接触で外部と電波により情報の授受が可能なＩＣチップ、アンテナを有するＩＣユニット及び／又はＩＣユニットが設けられたＩＣカードが設けられ、またＩＣカードホルダにＩＣカードを入れるようにしたものがある。このＩＣカードには、例えば本人の住所、所属、個人コードＮｏ等本人の確認を行なうため、種々の個人情報がＩＣチップに記憶されている。

【０００３】

【発明が解決しようとする課題】このような冊子やＩＣカードホルダでは、冊子やＩＣカードホルダを開かないでもＩＣユニットの情報を外部より盗聴電波にて、知らないうちに読み出され、情報の改ざんが行なわれる危険性がある。

【０００４】この発明はかかる点に鑑みなされたもので、外部からの盗聴電波よる偽造や変造をより一層有効に防止することが可能な冊子及びＩＣカードホルダを提供することを目的としている。

【０００５】

【課題を解決するための手段】前記課題を解決し、かつ目的を達成するために、この発明は、以下のように構成した。

【０００６】請求項１記載の発明は、『非接触で外部と電波により情報の授受が可能なＩＣチップ、アンテナを有するＩＣユニット及び／又はＩＣユニットが設けられたＩＣカードを有し、少なくとも１頁に電磁波を遮断もしくは通しにくいシールド部材を用いたことを特徴とする冊子。』である。

2

【０００７】この請求項１記載の発明によれば、冊子の少なくとも１頁に電磁波を遮断もしくは通しにくいシールド部材を用いることで、冊子を閉じた状態ではＩＣユニットがシールドされ、冊子を持っている人、あるいは冊子を検査する人だけがＩＣユニットの情報の授受ができ、外部からの盗聴電波よる偽造や変造をより一層有効に防止することが可能である。

【０００８】請求項２記載の発明は、『前記頁に、表紙及び／又は裏表紙を含むことを特徴とする請求項１記載の冊子。』である。

【０００９】この請求項２記載の発明によれば、頁に、表紙及び／又は裏表紙を含み、この表紙及び／又は裏表紙に電磁波を遮断もしくは通しにくいシールド部材を用いることで、表紙及び／又は裏表紙を閉じた状態で偽造や変造をより一層有効に防止することが可能である。

【００１０】請求項３記載の発明は、『非接触で外部と電波により情報の授受が可能なＩＣチップ、アンテナを有するＩＣユニットが設けられたＩＣカードを保持するホルダを有し、このホルダが２つ折りになっており、前記ホルダの両面又は片面に電磁波を遮断もしくは微弱化する材料を少なくとも前記アンテナに対応した領域に被覆し、このホルダの２つ折りの内側に前記ＩＣカードを入れられるようにしたことを特徴とするＩＣカードホルダ。』である。

【００１１】この請求項３記載の発明によれば、ホルダの両面又は片面に電磁波を遮断もしくは微弱化する材料を少なくともアンテナに対応した領域に被覆し、このホルダの２つ折りの内側にＩＣカードを入れられるようにしたから、ホルダを閉じた状態ではＩＣカードがシールドされ、ＩＣカードホルダを持っている人、あるいはＩＣカードホルダを検査する人だけがＩＣユニットの情報の授受ができ、外部からの盗聴電波よる偽造や変造をより一層有効に防止することが可能である。

【００１２】

【発明の実施の形態】以下、この発明の冊子及びＩＣカードホルダを図面に基づいて詳細に説明する。

【００１３】図１はＩＣユニットを有する冊子を示す図である。冊子１は、パスポート、預金通帳、社員証、学生証等の個人の身分を証明するに用いられ、表紙２と、裏表紙３と、この表紙２と裏表紙３の間には複数の頁４が設けられている。裏表紙３の内側には、非接触で外部と電波により情報の授受が可能なＩＣチップ、アンテナを有するＩＣユニット５が設けられている。この情報として、例えば氏名、住所、所属等の個人に関する情報あるいは社名、学校名、発行日等の共通の事項等がある。

【００１４】表紙２は、電磁波を遮断もしくは通しにくいシールド部材を用い

SAMSUNG EXHIBIT 1010, Page 252

しては、アルミニウム、銅、鉄等の金属、パーマロイ等の合金、フェライト等が考えられる。

【００１５】この冊子１は、図１（ｂ）に示すように表紙２を開くことで裏表紙３の内側に設けられたＩＣユニット５の情報の読み書きの授受を行なう。このように表紙２に電磁波を遮断もしくは通しにくいシールド部材を用いており、表紙２を閉じた状態ではＩＣユニット５がシールドされ、冊子１を持っている人、あるいは冊子１を検査する人だけがＩＣユニット５の情報の授受ができ、外部からの盗聴電波よる偽造や変造をより一層有効に防止することが可能である。

【００１６】図２は他の実施の形態のＩＣユニットを有する冊子を示す図である。この実施の形態では、表紙２と裏表紙３の間には複数の頁４にＩＣユニット５が設けられている。また、表紙２及び裏表紙３が、電磁波を遮断もしくは通しにくいシールド部材を用いて形成されている。

【００１７】この冊子１は、図２（ｂ）に示すように表紙２及び裏表紙３を開くことで内側の頁４に設けられたＩＣユニット５の情報の読み書きの授受を行なう。このように表紙２及び裏表紙３に電磁波を遮断もしくは通しにくいシールド部材を用いており、表紙２及び裏表紙３を閉じた状態ではＩＣユニット５がシールドされ、冊子１を持っている人、あるいは冊子１を検査する人だけがＩＣユニット５の情報の授受ができ、外部からの盗聴電波よる偽造や変造をより一層有効に防止することが可能である。

【００１８】図１及び図２では、冊子１にＩＣユニット５が設けられているが、このＩＣユニット５に代えて図３に示すようなＩＣカードＣＡを設けることができる。ＩＣカードＣＡは、例えば社員証や学生証等の個人の身分を証明するものであり、個人の顔写真８のような画像情報と同時に、氏名、住所、所属等の個人に関する情報あるいは社名、学校名、発行日等の共通の事項９が文字情報として記載され、内部にＩＣチップ５ａ、アンテナ５ｂを有するＩＣユニット５が封入されている。

【００１９】図４はＩＣカードホルダを示す図である。この実施の形態のＩＣカードホルダ１０は、非接触で外部と電波により情報の授受が可能なＩＣチップ、アンテナを有するＩＣユニット５が設けられたＩＣカードＣＡを保持するホルダ１１，１２を有している。このホルダ１１，１２が２つ折りになっており、ホルダ１１，１２の両面に電磁波を遮断もしくは微弱化する材料を少なくともＩＣユニット５のアンテナに対応した領域に被覆し、このホルダ１２の内側にカード押え１３が設けられている。

【００２０】ホルダ１２の内側とカード押え１３の間にＩＣカードＣＡを収納可能であり、ホルダ１１，１２の２つ折りの内側にＩＣカードＣＡを入れられるようにしている。

【００２１】このようにホルダ１１，１２の両面に電磁波を遮断もしくは微弱化する材料を少なくともＩＣユニット５のアンテナに対応した領域に被覆し、ホルダ１１，１２の２つ折りの内側にＩＣカードＣＡを入れられるようにしたから、ホルダ１１，１２を閉じた状態ではＩＣカードＣＡがシールドされ、ＩＣカードホルダ１０を持っている人、あるいはＩＣカードホルダ１０を検査する人だけがＩＣユニット５の情報の授受ができ、外部からの盗聴電波よる偽造や変造をより一層有効に防止することが可能である。

【００２２】図５は他の実施の形態のＩＣカードホルダを示す図である。この実施の形態では、片面のホルダ１１のみに電磁波を遮断もしくは微弱化する材料を少なくともＩＣユニット５のアンテナに対応した領域に被覆し、ホルダ１２には電磁波を遮断もしくは微弱化する材料を設けていないので、ホルダ１１側からの盗聴電波よる偽造や変造をより一層有効に防止することが可能である。

【００２３】図６は自動情報読取装置を示す図である。

【００２４】自動情報読取装置２０は、情報読取ユニット２１及び開き機構２２を備えている。冊子１及びＩＣカードホルダ１０から情報を読み取る時には、自動的に冊子１及びＩＣカードホルダ１０を開き機構２２により開き、自動的に開けた後、ＩＣカード又はＩＣユニットのアンテナを有する側を先頭に搬送し、情報読取ユニット２１の上で停止させ、情報を読取、表示、電送等を行う。処理終了後は、逆方向に搬送し、取り出し口より排出する。

【００２５】また、自動情報読取装置２０全体をシールド箱に入れておけば読取中でも漏洩電波が傍受される恐れがない。

【００２６】

【発明の効果】前記したように、請求項１記載の発明では、冊子の少なくとも１頁に電磁波を遮断もしくは通しにくいシールド部材を用いることで、冊子を閉じた状態ではＩＣユニットがシールドされ、冊子を持っている人、あるいは冊子を検査する人だけがＩＣユニットの情報の授受ができ、外部からの盗聴電波よる偽造や変造をより一層有効に防止することが可能である。

【００２７】請求項２記載の発明では、頁に、表紙及び／又は裏表紙を含み、この表紙及び／又は裏表紙に電磁波を遮断もしくは通しにくいシールド部材を用いることで、表紙及び／又は裏表紙を閉じた状態で偽造や変造をより一層有効に防止することが可能である。

【００２８】請求項３記載の発明では、ホルダの両面又は片面に電磁波を遮断もしくは微弱化する材料を少なくともアンテナに対応した領域に被覆し、このホルダの２つ折りの内側にＩＣカードを入れられるようにしたから、ホルダを閉じた状態ではＩＣカードがシールドされ、ＩＣカードホルダ

ードホルダを検査する人だけがＩＣユニットの情報の授受ができ、外部からの盗聴電波よる偽造や変造をより一層有効に防止することが可能である。

【図面の簡単な説明】

【図１】ＩＣユニットを有する冊子を示す図である。

【図２】他の実施の形態のＩＣユニットを有する冊子を示す図である。

【図３】ＩＣカードを有する冊子を示す図である。

【図４】ＩＣカードホルダを示す図である。

【図５】他の実施の形態のＩＣカードホルダを示す図で ＊10

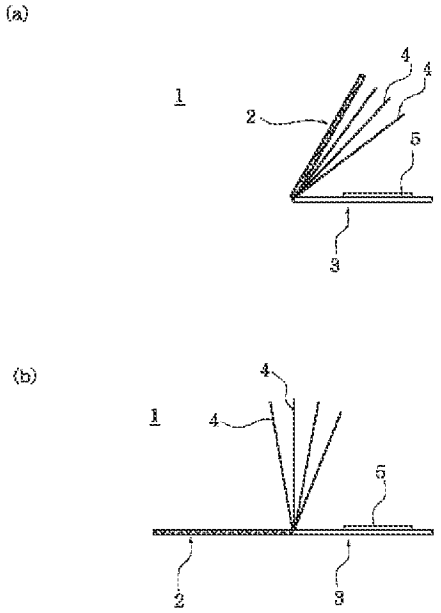
＊ある。

【図６】自動情報読取装置を示す図である。

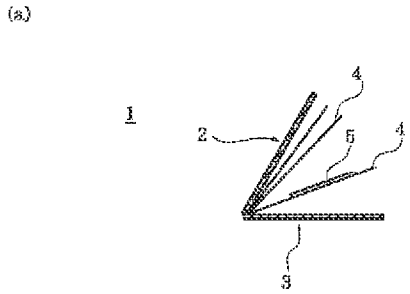
【符号の説明】

1　冊子
2　表紙
3　裏表紙
4　頁
5　ＩＣユニット
ＣＡ　ＩＣカード

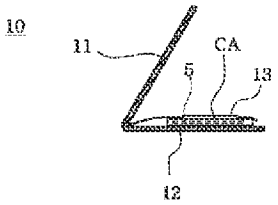
【図１】



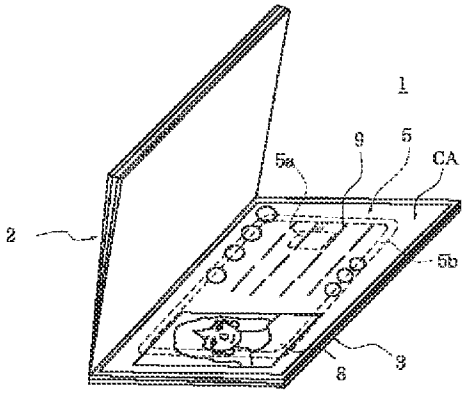
【図２】



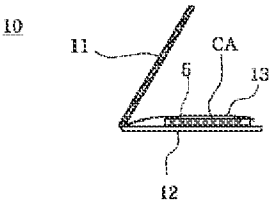
【図４】



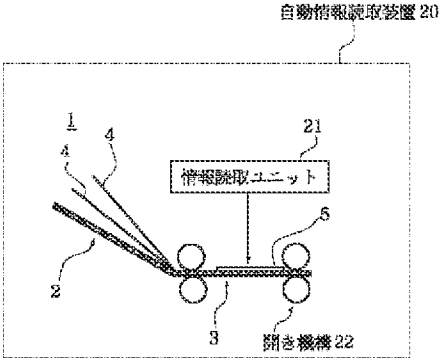
【図３】



【図５】



【図６】



Electronic Acknowledgement Receipt

EFS ID:	47273903
Application Number:	17952176
International Application Number:	
Confirmation Number:	8353
Title of Invention:	Methods of Using a Cellular Telephone
First Named Inventor/Applicant Name:	Steven Michael Colby
Customer Number:	43198
Filer:	Steven M. Colby/Susan Stewart
Filer Authorized By:	Steven M. Colby
Attorney Docket Number:	SMC-83-C12C3
Receipt Date:	26-DEC-2022
Filing Date:	23-SEP-2022
Time Stamp:	17:08:21
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)	IDS_C12C3_SB08.pdf	1039819 a96746abfab270004a2a2776610a3f89d2816576	no	14

Warnings:

Information:					
2	Foreign Reference	F1_EP0383059A1.pdf	474530 5f033aa7f9e0e5a64630c088f0535446d687faf8	no	9
Warnings:					
Information:					
3	Foreign Reference	F2_GB2397272A.pdf	1131027 91ca96c8427efa181285b2b5a75dc400743af5c3	no	28
Warnings:					
Information:					
4	Foreign Reference	F3_WO2004038644A2.pdf	2044594 89fbebcbfbdabb7eaaca8ece7b4d74a229afe390	no	52
Warnings:					
Information:					
5	Foreign Reference	F4_EP1075781B1.pdf	1398421 1947284dae276e6923d4e61efa8b269f7c36b9a5	no	19
Warnings:					
Information:					
6	Foreign Reference	F5_JP1999348471.pdf	194167 79fb3f0638bf623658bcb7686ad5ac37230632d7	no	4
Warnings:					
Information:					
7	Non Patent Literature	NPL1-1_NFC-phone-art.pdf	786482 ee37d5ad56273a35b98da01087d1ca65402670b8	no	2
Warnings:					
Information:					
8	Non Patent Literature	NPL1-2_NFC-phone-art-2.pdf	859158 fb52a298b08afe1be82935a8106976f4301da9b6	no	2
Warnings:					
Information:					

9	Non Patent Literature	NPL1-3_NFC-phone-art-3.pdf	1445044 04222316bccb68f2d30dc59ffcabc67141c5c3a5	no	7
Warnings:					
Information:					
10	Non Patent Literature	NPL1-4_ISO.PDF	412566 898234a8653f09c3236498cee565d82750f5a38d	no	18
Warnings:					
Information:					
11	Non Patent Literature	NPL1-5.PDF	1970848 adb9cc96d4afd07f561b508e6ef339dd6929d9d2	no	57
Warnings:					
Information:					
12	Non Patent Literature	NPL1-6_ISO.PDF	1399163 9107776eecca882334c26c289c8d3839a7f530fe	no	58
Warnings:					
Information:					
13	Non Patent Literature	NPL1-7_Ellis.pdf	563892 b29efb4341734568c98246890bc1f7e90804c548	no	26
Warnings:					
Information:					
14	Non Patent Literature	NPL1-8_TR_Biometric_Stds.pdf	6170518 b897938c3630c0ade402dfbd0806e9224115d159	no	60
Warnings:					
Information:					
15	Non Patent Literature	NPL1-10_Juels.PDF	4565383 99e061906d763483981a46988be61eed065f1b57	no	23
Warnings:					
Information:					

16	Non Patent Literature	NPL1-9_Shell.PDF	941166 a48ead320269d28e91f25c4bac6a26615eae8fdb	no	20
Warnings:					
Information:					
17	Non Patent Literature	NPL1-11_mifare.PDF	2107046 3342ace441b2ed12db0c486d63ab6a8078d91d1c	no	18
Warnings:					
Information:					
18	Non Patent Literature	NPL1-12_MR_Passports.PDF	21724804 d664e5fcf657025a73fc3e8888458d4c11e73c32	no	113
Warnings:					
Information:					
19	Non Patent Literature	NPL1-13_TR_Dev_Logical_Data.PDF	15438033 826fcc2d81dfe139013c4af5ccce08205675f5ed	no	92
Warnings:					
Information:					
20	Non Patent Literature	NPL1-14_Australia.PDF	995930 d92a3400eadaaff6c933029b0e96d476340b7a22	no	25
Warnings:					
Information:					
21	Non Patent Literature	NPL1-15_ICAOAnnex.PDF	712016 b7983d5df5c005adafe3500cd92acd664d3de141	no	27
Warnings:					
Information:					
22	Non Patent Literature	NPL1-16_MiFare_2.pdf	904663 2380170faf801ba1a2dcabbdb100505fa073bf2b	no	91
Warnings:					
Information:					

23	Non Patent Literature	NPL1-17_RFID_2.pdf	1689828 8150170a574f1006d46809d493277fb104d08873	no	105
Warnings:					
Information:					
24	Non Patent Literature	NPL1-18_Smart_Card_2.pdf	3395145 45eac8809925b99ed1ae360969ddbe39436267b6	no	137
Warnings:					
Information:					
25	Non Patent Literature	NPL1-19_Juels_2.pdf	1258153 d7123fd0e96eba3ad45a02cffc71f35165fe0b60	no	85
Warnings:					
Information:					
26	Non Patent Literature	NPL1-20_Juels-2_2.pdf	972589 00ebed1b8daee55431b95c20241423309c3e3dad	no	100
Warnings:					
Information:					
27	Non Patent Literature	NPL1-21_Knospe_2.pdf	500047 493866d199393b30e2a0a42dba47d6cf99f08564	no	13
Warnings:					
Information:					
28	Non Patent Literature	NPL1-22_Gao_2.pdf	2527406 b8cf7343d41bc9f54167cd89d81ef3a5c96c1a7f	no	111
Warnings:					
Information:					
29	Non Patent Literature	NPL1-23_Weis_2.pdf	929353 7bd1f78b927128fca5f6502e87f6165b6e03835d	no	50
Warnings:					
Information:					

30	Non Patent Literature	NPL1-24_EPC-Global_2.pdf	10196075 1205b8b5679d9a9b63ca0e64602c59bd0e3923f6	no	140
Warnings:					
Information:					
31	Non Patent Literature	NPL1-25_ICAO_2003_2.pdf	1069467 5248c23479ff842157fb26942167ba85151b5447	no	43
Warnings:					
Information:					
32	Non Patent Literature	NPL1-26_Morgantown_2.pdf	3251502 1cbad38c5c1305e7ac577a5e8e30df2f39e87fcd	no	92
Warnings:					
Information:					
33	Non Patent Literature	NPL1-27_Annex_2.pdf	671943 c7cddb7f0ede1d85c46fa45e18803c6fb345e171	no	94
Warnings:					
Information:					
34	Non Patent Literature	NPL1-28_Kinneging.PDF	10497399 195e249d4d6ae91da1c2674c427be05b19b31038	no	57
Warnings:					
Information:					
35	Non Patent Literature	NPL1-30-14443-1.pdf	1260631 bd5b48006a9b900aaf49bc9bd9f1f448f25b5fc5	no	10
Warnings:					
Information:					
36	Non Patent Literature	NPL1-31-14443-2.pdf	359781 2d749c6a7c4a6bb6e0cea266b81093396670f35a	no	18
Warnings:					
Information:					

37	Non Patent Literature	NPL1-33_LDS_OPT_Cap.pdf	5229140 1bdecb32b7a8a5d64cfdaa81bd87098d654339d6	no	92
Warnings:					
Information:					
38	Non Patent Literature	NPL1-34_TR_DevandSpec.pdf	1572249 4fca5c3b306beac3e194cdf1494661b7e6b67c85	no	60
Warnings:					
Information:					
39	Non Patent Literature	NPL1-38_Kuklinski.PDF	268299 2a829f883d644309146a9ca8de440f5d4c3a7185	no	4
Warnings:					
Information:					
40	Non Patent Literature	NPL1-39.PDF	868851 f8077b48fd653d9ca7f0fcdd99b4595bbff086ae	no	28
Warnings:					
Information:					
41	Non Patent Literature	NPL1-40.PDF	1013386 1941ddbca4c434547b91b3755aee0668b6d8ddd8	no	20
Warnings:					
Information:					
42	Non Patent Literature	NPL1-29_PKI2004_2.pdf	1350566 e65b27fa238f878f5b169cc5a6e7810f1f06bd81	no	71
Warnings:					
Information:					
43	Non Patent Literature	NPL1-36_ICAO-NTWG_Sept2003_2.pdf	1308751 92b71ecfe1bf3e52fce679c2af6746fe6b707506	no	14
Warnings:					
Information:					

44	Non Patent Literature	NPL1-37_USCFC_2.pdf	512558 55ddfa7cfd8f475c8cc0c6e9612a2f65a07af8fc	no	105
Warnings:					
Information:					
45	Non Patent Literature	NPL1-32-14443-3_2_compressed.pdf	2173119 d198281391cad04994d239975d45ad7cd610d291	no	58
Warnings:					
Information:					
46	Non Patent Literature	NPL1-35_Specs_Discr_Exp_2_compressed.pdf	5693348 00e9d9fd3ccb9f10eedbaeb8e3535520dc124641	no	113
Warnings:					
Information:					
47	Non Patent Literature	NPL1-41.PDF	878840 a27f743dda6f7f3cc39a9cd03e81dfdea30c0759	no	22
Warnings:					
Information:					
48	Non Patent Literature	NPL1-42.PDF	935908 a40c544facf483335381b45c941199e69ad189b0	no	20
Warnings:					
Information:					
49	Non Patent Literature	NPL1-43.PDF	962870 272b1fc260758d31d32ea4b620d04857a0271367	no	28
Warnings:					
Information:					
50	Non Patent Literature	NPL1-44.PDF	891643 c7e98e37bd8da08b7f9de6ce650a82023b92ec5d	no	22
Warnings:					
Information:					

51	Non Patent Literature	NPL1-45.PDF	1645476 9f9083cc04126d05eac3fc0722f2de5dc49d1f6b	no	20
Warnings:					
Information:					
52	Non Patent Literature	NPL1-46.PDF	754681 629bb86492ebe7ad4b7b993d64df9b84bbe0bb18	no	20
Warnings:					
Information:					
53	Non Patent Literature	NPL1-47.PDF	848408 9b06fc51a398b1c800cbf7b487867c97303092c5	no	20
Warnings:					
Information:					
54	Non Patent Literature	NPL1-48.PDF	1017097 0282a0bf530914f9de611160757386adbc16c577	no	20
Warnings:					
Information:					
			Total Files Size (in bytes):	133783779	

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

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES

PATENT AND TRADEMARK OFFICE

APPLICANT:	Mynette Technologies, Inc.
APPLICATION NO.:	17/952,176
CONFIRMATION NO.:	8353
FILING DATE:	23-SEP-2022
TITLE:	Methods of Using a Cellular Telephone
EXAMINER:	Unknown
ART UNIT:	2876
ATTY. DKT. NO.:	SMC-83-C12C3

Preliminary Amendment A

Prior to Examination of this application, please enter the following amendment.

Amendments to the claims begin on page 2.

Remarks begin on page 7.

SAMSUNG EXHIBIT 1010, Page 264

Listing of CLAIMS

1. (Currently Amended) A method of performing a financial transaction using a cellular telephone, the method comprising:

placing the cellular telephone within reading range of a wireless communication device, the cellular telephone being configured to communicate wirelessly using an inductive coupling and an RF antenna, wherein ~~the~~ communication ~~(verb)~~by the cellular telephone is responsive to a circuit including an electronic switch configured to change a state of the circuit, the circuit being configured to communicate responsive to the state of the circuit;

activating the electronic switch within the cellular telephone to change the state of the circuit, activation of the electronic switch being responsive to a biometric sensor included in the cellular telephone; and

communicating financial account information from the cellular telephone to the wireless communication device responsive to the state of the circuit to facilitate the financial transaction, the communication of the financial account information using the inductive coupling or the RF antenna.

2. (Cancelled) ~~The method of claim 1, wherein the cellular telephone includes the biometric sensor.~~

3. (Original) The method of claim 1, wherein the circuit is configured to facilitate the financial transaction responsive to the biometric sensor.

4. (Original) The method of claim 1, wherein the circuit is configured to approve the financial transaction responsive to the biometric sensor.

5. (Currently Amended) The method of claim 1, wherein the circuit is configured to communicate the financial account information responsive to the biometric sensor.

6. (Original) The method of claim 1, wherein the circuit is changed from a first ON state to a second ON state, responsive to the electronic switch, and wherein the circuit includes a memory configured to store the first and second ON states.

7. (Original) The method of claim 1, wherein the circuit is changed from a first ON state to a second ON state, responsive to the electronic switch, and wherein different

SAMSUNG EXHIBIT 1010, Page 265

amounts of personal information are communicated via the inductive coupling or RF antenna in the first ON state relative to the second ON state.

8. (Original) The method of claim 1, wherein the circuit is configured to store transaction logs.

9. (Original) The method of claim 1, wherein the circuit is configured for a user to select between a plurality of financial accounts for the financial transaction.

10. (Currently Amended) The method of claim 1, wherein the cellular telephone is configured for a user to enter an amount of the financial transaction, and further comprising entering ~~a personal identification number or a~~ the amount ~~password~~ to facilitate the financial transaction.

11. (Currently Amended) The method of claim 1, wherein the circuit is configured to communicate a financial~~n~~ account number via the inductive coupling or RF antenna to facilitate the financial transaction.

12. (Original) The method of claim 1, wherein the cellular telephone includes a user interface configured to enter a financial account number and includes memory configured to store the financial account number for use in the financial transaction.

13. (Currently Amended) The method of claim 1, wherein the cellular telephone is configured for a user to enter a personal identification number (PIN), communication of the financial account information via the inductive coupling or RF antenna being responsive to the personal identification number, and further comprising entering the personal identification number to facilitate the financial transaction.

14. (Cancelled) ~~The method of claim 1, wherein the cellular telephone includes a memory configured to store an encryption key used to facilitate the financial transaction.~~

15. (Original) The method of claim 1, wherein the cellular telephone includes a memory configured to store a key required to change the state of the circuit to facilitate the financial transaction.

16. (Currently Amended) The method of claim 1, wherein the cellular telephone is configured for mechanical insertion of an electronic key, the electronic key including a personal identification number, a signal communicated via the

inductive coupling or RF antenna to facilitate the financial transaction being responsive to entry of the personal identification number by a user.

17. (Currently Amended) The method of claim 1, wherein the cellular telephone is configured ~~for insertion of an electronic key, the electronic key including~~to store a financial~~s~~ account ~~identifier number~~ and the communication via the inductive coupling or RF antenna ~~being responsive to~~including the financial account ~~identifier~~number~~, the electronic key being configured to store a password or personal identification number~~.

18. (Currently Amended) The method of claim 1, wherein activating the electronic switch is responsive to data stored in memory of the cellular telephone and the data stored in the memory includes biometric data.

19. (Original) A method of performing a financial transaction using a cellular telephone, the method comprising:

placing the cellular telephone within reading range of a wireless communication device, the cellular telephone being configured to communicate wirelessly using an RF antenna, wherein the RF antenna is responsive to a circuit including an electronic switch configured to change a state of the circuit, the circuit being configured to communicate via the RF antenna responsive to the state of the circuit;

activating the electronic switch within the cellular telephone to change the state of the circuit, activation of the electronic switch being responsive to entry of a personal identification number; and

communicating financial account information from the cellular telephone to the wireless communication device responsive to the state of the circuit to facilitate the financial transaction, the communication of the financial account information using the RF antenna.

20. (Original) The method of claim 19, wherein the communication of the financial account information is responsive to a biometric sensor included in the cellular telephone.

21. (Original) The method of claim 19, further comprising approving the financial transaction using a biometric sensor.

22. (Cancelled) ~~The method of claim 19, further comprising approving the financial transaction using a mechanical switch.~~

23. (Currently Amended) The method of claim 19, wherein the cellular telephone includes a user interface configured for a user to enter a financial account number for use in the financial transaction. ~~and includes memory configured to store the financial account number for use in the financial transaction~~.

24. (Currently Amended) The method of claim 19, wherein the circuit is configured for a user to select between a plurality of financial accounts for the financial transaction.

25. (Original) The method of claim 19, wherein the circuit is changed from a first ON state to a second ON state, responsive to the electronic switch, and wherein different amounts of personal information are communicated via the RF antenna in the first ON state relative to the second ON state.

26. (Original) The method of claim 19, wherein the circuit is configured to store transaction logs.

27. (Currently Amended) The method of claim 19, wherein the circuit is configured to communicate a financial~~n~~ account number via the RF antenna to facilitate the financial transaction.

28. (Cancelled) ~~The method of claim 19, wherein the cellular telephone is configured for insertion of a memory, the memory including account information and a personal identification number, and a signal communicated via the RF antenna to facilitate the financial transaction being responsive to the account information and the personal identification number~~.

29. (Currently Amended) The method of claim 19, wherein the cellular telephone is configured for storing a password in memory of the cellular phone, the password being entered by a user of the cellular phone to engage in the transaction ~~insertion of an electronic key, the electronic key being configured to store a password, the communication via the RF antenna being responsive to the password.~~

30. (Currently Amended) The method of claim 19, wherein the cellular telephone is configured for insertion of an electronic key, the electronic key being configured

to store ~~a~~ the personal identification number, the communication via the RF antenna being responsive to the personal identification number.

31. (New) The method of claim 1, wherein the financial account information includes an account number corresponding to a financial account of a user of the cellular telephone.

32. (New) The method of claim 1, wherein the financial account information is stored in a memory on the cellular telephone, the financial account information corresponding to one of a plurality of financial accounts of a user of the cellular telephone, the method further comprising:

presenting a user interface to the user, the user interface being configured to allow the user to select a specific member of the plurality of financial accounts of the user for the financial transaction; and

wherein the step of communicating financial account information includes communicating financial account information corresponding to the selected specific member of the plurality of financial accounts.

33. (New) The method of claim 19, wherein the cellular telephone is configured for a user to enter an amount of the financial transaction.

34. (New) The method of claim 23, wherein the cellular telephone includes memory configured to store the financial account number, wherein the circuit is configured for the user to select between a plurality of financial accounts for the financial transaction; and further comprising selecting a specific member of the plurality of financial accounts for the financial transaction.

REMARKS

Claims 1, 3-13, 15-27, 29-34 are currently pending herein.

Claims 1, 5, 10, 11, 13, 16, 17, 18, 23, 27, 29 and 30 are currently amended.

Claims 2, 14, 22 and 28 are hereby cancelled.

Claims 31-34 are new.

The Applicant believes that no new matter is added in this amendment and that all claims are now in condition for allowance.

Respectfully submitted,

Date: December 23, 2022 /Steven M. Colby 50,250/

Dr. Steven M. Colby, JD, Ph.D.
(Reg. No. 50,250)
Partner, Rimon PC
CEO, Mynette Technologies, Inc.

Electronic Acknowledgement Receipt

EFS ID:	47272462
Application Number:	17952176
International Application Number:	
Confirmation Number:	8353
Title of Invention:	Methods of Using a Cellular Telephone
First Named Inventor/Applicant Name:	Steven Michael Colby
Customer Number:	43198
Filer:	Steven M. Colby
Filer Authorized By:	
Attorney Docket Number:	SMC-83-C12C3
Receipt Date:	23-DEC-2022
Filing Date:	23-SEP-2022
Time Stamp:	23:46:53
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		SMC-83-C12C3-Amendment-A-filing.pdf	136465 3ae3f69c7b17b2fc60b8e4fab3ed4866202a80b7	yes	7

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Preliminary Amendment	1	1
	Claims	2	6
	Applicant Arguments/Remarks Made in an Amendment	7	7

Warnings:	
Information:	
Total Files Size (in bytes):	136465

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.
17/952,176	09/23/2022	Steven Michael Colby	SMC-83-C12C3	8353

43198 7590 11/17/2022
Rimon Law, P.C. - SMC
Steven Colby
423 Washington Street, Suite 600
San Francisco, CA 94111

EXAMINER
CENTRAL, DOCKET

ART UNIT	PAPER NUMBER
OPAP	

NOTIFICATION DATE	DELIVERY MODE
11/17/2022	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.rimonlaw@clarivate.com
karen.hagerman@rimonlaw.com
steven.colby@rimonlaw.com

Decision Granting Request for Prioritized Examination (Track I)	**Application No.** 17/952,176	**Applicant(s)** Colby, Steven Michael	
	Examiner FIKIRTE A GEREMEW	**Art Unit** OMBL	**AIA (FITF) Status** No

1. THE REQUEST FILED 23 September 2022 IS **GRANTED** .

   The above-identified application has met the requirements for prioritized examination
   A. ☑ for an original nonprovisional application (Track I).
   B. ☐ for an application undergoing continued examination (RCE).

2. **The above-identified application will undergo prioritized examination**. The application will be accorded special status throughout its entire course of prosecution until one of the following occurs:

   A. filing a **petition for extension of time** to extend the time period for filing a reply;

   B. filing an **amendment to amend the application to contain more than four independent claims, more than thirty total claims** , or a multiple dependent claim;

   C. filing a **request for continued examination** ;

   D. filing a notice of appeal;

   E. filing a request for suspension of action;

   F. mailing of a notice of allowance;

   G. mailing of a final Office action;

   H. completion of examination as defined in 37 CFR 41.102; or

   I. abandonment of the application.

Telephone inquiries with regard to this decision should be directed to FIKIRTE GEREMEW at (703) 756-1930. In his/her absence, calls may be directed to Petition Help Desk at (571) 272-3282.

/FIKIRTE A GEREMEW/ PROGRAM SUPPORT ASSISTANT, OMBL	

U.S. Patent and Trademark Office
PTO-2298 (Rev. 02-2012)

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number
17/952,176

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	80		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	350		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	400		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	30 minus 20 =	* 10	x 50 =	500	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	2 minus 3 =	*	x =	0			
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			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	830		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
AMENDMENT A	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
AMENDMENT A	Application Size Fee (37 CFR 1.16(s))									
AMENDMENT A	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($)	ADDITIONAL FEE($)	OR	RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
AMENDMENT B	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
AMENDMENT B	Application Size Fee (37 CFR 1.16(s))									
AMENDMENT B	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	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
17/952,176	09/23/2022		1330	SMC-83-C12C3	30	2

CONFIRMATION NO. 8353

FILING RECEIPT

OC000000049942166

43198
Rimon Law, P.C. - SMC
Steven Colby
423 Washington Street, Suite 600
San Francisco, CA 94111

Date Mailed: 10/21/2022

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)

Steven Michael Colby, Verdi, NV;

Applicant(s)

Steven Michael Colby, Verdi, NV;

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 17/728,412 04/25/2022
which is a CON of 17/522,697 11/09/2021 PAT 11,347,949
which is a CON of 16/186,543 11/11/2018 PAT 11,170,185
which is a CIP of 15/418,726 01/28/2017 PAT 10,503,940
which is a CON of 14/660,825 03/17/2015 PAT 9,569,777
which is a CIP of 13/481,104 05/25/2012 ABN
which is a CON of 12/777,474 05/11/2010 ABN
and said 14/660,825 03/17/2015 is a CIP of 13/084,433 04/11/2011 ABN
which is a CON of 11/458,620 07/19/2006 PAT 7,924,156
which is a CIP of 11/382,052 05/07/2006 ABN
and is a CIP of 11/382,053 05/07/2006 ABN
and is a CIP of 11/382,054 05/08/2006 ABN
and is a CIP of 11/382,264 05/08/2006 ABN
and is a CIP of 11/382,265 05/08/2006 ABN
and is a CIP of 11/420,721 05/26/2006 ABN
and claims benefit of 60/700,884 07/19/2005

and claims benefit of 60/712,308 08/30/2005
and claims benefit of 60/715,641 09/10/2005
and claims benefit of 60/752,933 12/21/2005
and claims benefit of 60/758,751 01/13/2006
and claims benefit of 60/782,068 03/13/2006
and claims benefit of 60/744,154 04/03/2006
and claims benefit of 60/746,636 05/06/2006
and is a CIP of 11/382,050 05/07/2006 ABN
which claims benefit of 60/678,428 05/06/2005
and claims benefit of 60/685,331 05/27/2005
and said 14/660,825 03/17/2015 is a CIP of 14/468,110 08/25/2014 PAT 9,495,852
which is a CON of 12/577,209 10/12/2009 PAT 8,816,826
which is a CON of 11/468,026 08/29/2006 ABN
which claims benefit of 60/746,636 05/06/2006
and claims benefit of 60/744,154 04/03/2006
and claims benefit of 60/782,068 03/13/2006
and claims benefit of 60/758,751 01/13/2006
and claims benefit of 60/752,933 12/21/2005
and claims benefit of 60/715,641 09/10/2005
and claims benefit of 60/712,308 08/30/2005

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: 10/20/2022

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 17/952,176**

Projected Publication Date: Request for Non-Publication Acknowledged

Non-Publication Request: Yes

Early Publication Request: No
**** SMALL ENTITY ****
Title

Methods of Using a Cellular Telephone

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.

United States Patent and Trademark Office

Office of the Chief Financial Officer

Document Code:WFEE

User :Almaz Sahle

Sale Accounting Date:10/20/2022

Sale Item Reference Number	Effective Date
17952176	09/23/2022

Document Number	Fee Code	Fee Code Description	Amount Paid	Payment Method
I20220J022230482	2830	PROCESSING FEE, EXCEPT PROV. APPLS.	$70.00	Deposit Account

DocCode - SCORE

SCORE Placeholder Sheet for IFW Content

Application Number: 17952176 Document Date: 09/23/2022

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

- Drawing

At the time of document entry (noted above):

- USPTO employees may access SCORE content via DAV or via the SCORE web page.
- External customers may access SCORE content via PAIR using the Supplemental Content tab.

Form Revision Date: March 1, 2019

CERTIFICATION AND REQUEST FOR PRIORITIZED EXAMINATION UNDER 37 CFR 1.102(e) (Page 1 of 1)

First Named Inventor:	Steven M. Colby	Nonprovisional Application Number (if known):	
Title of Invention:	Methods of Using a Cellular Telephone		

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS PRIORITIZED EXAMINATION FOR THE ABOVE-IDENTIFIED APPLICATION.

1. The processing fee set forth in 37 CFR 1.17(i), the prioritized examination fee set forth in 37 CFR 1.17(c), and if not already paid, the publication fee set forth in 37 CFR 1.18(d) have been filed with the request. The basic filing fee, search fee, examination fee, and any required excess claims and application size fees are filed with the request or have been already been paid.

2. The application contains or is amended to contain no more than four independent claims and no more than thirty total claims, and no multiple dependent claims.

3. The applicable box is checked below:

I. ☑ Original Application (Track One) - Prioritized Examination under § 1.102(e)(1)

i. (a) The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a). This certification and request is being filed with the utility application via EFS-Web.

---OR---

(b) The application is an original nonprovisional plant application filed under 35 U.S.C. 111(a). This certification and request is being filed with the plant application in paper.

ii. An executed oath or declaration under 37 CFR 1.63 is filed with the application.

II. ☐ Request for Continued Examination - Prioritized Examination under § 1.102(e)(2)

i. A request for continued examination has been filed with, or prior to, this form.
ii. If the application is a utility application, this certification and request is being filed via EFS-Web.
iii. The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a), or is a national stage entry under 35 U.S.C. 371.
iv. This certification and request is being filed prior to the mailing of a first Office action responsive to the request for continued examination.
v. No prior request for continued examination has been granted prioritized examination status under 37 CFR 1.102(e)(2).

Signature /Steven M. Colby 50,250/	Date Sept. 22, 2022
Name (Print/Typed) Steven M. Colby	Practitioner Registration Number 50250

Note: *Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required in accordance with 37 CFR 1.33 and 11.18. Please see 37 CFR 1.4(d) for the form of the signature. If necessary, submit multiple forms for more than one signature, see below*.*

☐ *Total of_____ forms are submitted.

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.

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	Methods of Using a Cellular Telephone
First Named Inventor/Applicant Name:	Steven M. Colby
Filer:	Steven M. Colby
Attorney Docket Number:	SMC-83-C12C3

Filed as Small Entity

Filing Fees for Track I Prioritized Examination - Nonprovisional Application under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
UTILITY FILING FEE (ELECTRONIC FILING)	4011	1	80	80
UTILITY SEARCH FEE	2111	1	350	350
UTILITY EXAMINATION FEE	2311	1	400	400
REQUEST FOR PRIORITIZED EXAMINATION	2817	1	2100	2100
Pages:				
Claims:				
CLAIMS IN EXCESS OF 20	2202	10	50	500
Miscellaneous-Filing:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
PUBL. FEE- EARLY, VOLUNTARY, OR NORMAL	1504	1	0	0
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**3430**

Electronic Acknowledgement Receipt

EFS ID:	46686528
Application Number:	17952176
International Application Number:	
Confirmation Number:	8353
Title of Invention:	Methods of Using a Cellular Telephone
First Named Inventor/Applicant Name:	Steven M. Colby
Customer Number:	43198
Filer:	Steven M. Colby
Filer Authorized By:	
Attorney Docket Number:	SMC-83-C12C3
Receipt Date:	23-SEP-2022
Filing Date:	
Time Stamp:	21:59:18
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$3430
RAM confirmation Number	E20229MM06300080
Deposit Account	505992
Authorized User	Steven Colby

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

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Drawings-other than black and white line drawings	FigsPart1of2.pdf	118582 28258ab01743761927f4d4b98b989ac2217c62b6	no	15
Warnings:					
Information:					
2	Drawings-other than black and white line drawings	FigsPart2of2.pdf	220617 8bc8190fcff8181efd283cafae1a7637898707c6	no	20
Warnings:					
Information:					
3		SMC-83-C12C3-Spec-filing.pdf	269386 a9330b75fad8f4a0dfa68b38cdb6db761296f579	yes	67

Multipart Description/PDF files in .zip description

Document Description	Start	End
Specification	1	62
Claims	63	66
Abstract	67	67

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
Warnings:					
Information:					
4	Application Data Sheet	SMC-83-C12C3-ADS.pdf	1563536 f7fde17696af0083c6591f987512e353f6470673	no	10
Warnings:					
Information:					
5	Oath or Declaration filed	SMC-83-C12C3-Declaration.pdf	178158 a95846e9d1d8c792bb0275f016acb6649ee70921	no	2

Warnings:					
Information:					
6	Track One Request	sb0424.pdf	140099 611054825ceb72bf2153305fa9ed3b3a52b97d93	no	2
Warnings:					
Information:					
7	Fee Worksheet (SB06)	fee-info.pdf	51001 ba7a4cc4baf80e1697c4d0f51d96f445ac95a598	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	2541379		

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

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Methods of Using a Cellular Telephone

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is a continuation of US non-provisional patent application Ser. No. 17/728,412 filed April 25, 2022; this application is a continuation of US non-provisional patent application Ser. No. 17/697,923 filed March 18, 2022; which is a continuation of US non-provisional patent application Ser. No. 17/522,697 filed November 9, 2021; which in turn is a continuation of US non-provisional patent application Ser. No. 16/186,543 filed November 11, 2018, which in turn is a continuation-in-part of US non-provisional patent application Ser. No. 15/418,726 filed January 28, 2017; which, in turn, is a continuation of US non-provisional patent application Ser. No. 14/660,825 filed March 17, 2015, which in turn is:

a continuation in part of US non-provisional patent application Ser. No. 13/481,104 filed 5/25/2012; which is in turn is a continuation of 12/777,474 filed 5/11/2010, which in turn is a continuation of 11/350,309 filed February 7, 2006, now patent 7719425, and claims benefit of provisional patent applications:

60/678,428 filed 05/06/2005,
60/685,331 filed 05/27/2005,
60/700,884 filed 07/19/2005,
60/712,308 filed 08/30/2005,
60/715,641 filed 09/10/2005,
60/752,933 filed 12/21/2005, and
60/758,751 filed 01/13/2006;

a continuation in part of US non-provisional patent application Ser. No. 13/084,433 filed 04/11/2011 which in turn is a continuation of 11/458,620 filed 07/19/2006, now patent 7,924,156 which is a continuation in part of:

11/382,052 filed 05/07/2006,
11/382,053 filed 05/07/2006,
11/382,054 filed 05/08/2006,
11/382,264 filed 05/08/2006,
11/382,265 filed 05/08/2006, and

11/420,721 filed 05/26/2006,

and claims benefit of provisional patent applications:

60/700,884 filed 07/19/2005,

60/712,308 filed 08/30/2005,

60/715,641 filed 09/10/2005,

60/752,933 filed 12/21/2005,

60/758,751 filed 01/13/2006,

60/782,068 filed 03/13/2006,

60/744,154 filed 04/03/2006, and

60/746,636 filed 05/06/2006, and is

a continuation in part of 11/382,050 filed 05/07/2006, which claims benefit of provisional patent applications:

60/678,428 05//06/2005, and

60/685,331 05/27/2005; and

a continuation in part of US non-provisional patent application Ser. No. 14/468,110 filed 08/25/14, which is a continuation of 12/577,209 10/12/2009, now patent 8816826, which claims benefit of 11/468,026 filed August 29, 2006, 14/468,110 claims benefit of provisional patent applications:

60/700,884 filed 07/19/2005,

60/712,308 filed 08/30/2005,

60/715,641 filed 09/10/2005,

60/752,933 filed 12/21/2005,

60/758,751 filed 01/13/2006,

60/782,068 filed 03/13/2006,

60/744,154 filed 04/03/2006, and

60/746,636 filed 05/06/2006, and

is a continuation in part of

CIP 11/382,052 filed 05/07/2006,

CIP 11/382,053 filed 05/07/2006,

CIP 11/382,054 filed 05/08/2006,

CIP 11/382,264 filed 05/08/2006,

SAMSUNG EXHIBIT 1010, Page 290

CIP 11/382,265 filed 05/08/2006,

CIP 11/420,721 filed 05/26/2006, and

CIP 11/382,050 filed 05/07/2006 which claims benefit of provisional patent applications:

60/678,428 filed 05/06/2005, and

60/685,331 filed 05/27/2005.

[0002] The disclosures of the above provisional and nonprovisional patent applications are hereby incorporated herein by reference.

BACKGROUND OF THE INVENTION

[0003] *Field of the Invention*

[0004] The invention is in the fields of electronic passports, and more specifically in the field of electronic passports including shielding and/or switchable RFID tags.

[0005] *Description of Related Art*

[0006] Radio Frequency identity (RFID) tags are typically small, flexible, and low profile devices that can be affixed to items for electronic tracking and information storage purposes. An RFID tag can be read by an RFID reader when the RFID tag is brought within a certain vicinity of the reader that is broadcasting a radio frequency signal. In some cases, once within that vicinity, the RFID tag receives sufficient power from the radio frequency signal to permit it to transmit a return radio frequency signal using the received power. These RFID tags are referred to as passive RFID tags. In other cases the RFID tag has an independent power source for generating a return radio frequency signal. These RFID tags are referred to as active RFID tags. With either passive or active RFID tags, the return radio frequency signal may include an encoded copy of information stored within the RFID tag. As used herein, RFID tags include radio frequency contactless chips.

SUMMARY

[0007] The invention includes the use of shielding in relation to RFID tags. For example, some embodiments of the invention include shielded containers for storing devices including RFID tags. These devices can include identification devices such as passports, credit cards, or driver's licenses.

SAMSUNG EXHIBIT 1010, Page 291

[0008] Some embodiments of the invention include shielded containers and RFID tags, the RFID tags configured for use in determining a state of the container. For example, detection of an RFID tag can be used to determine if the container is open or closed. These embodiments are optionally used in event logging or security.

[0009] Some embodiments of the invention include shielding attached to identification devices. This shielding may, for example, be included in a clamshell configuration, as a shielding insert, or as part of a page or cover.

[0010] Various embodiments of the invention include a container comprising an RFID tag configured for determining if the container is open or closed, and radio frequency shielding configured to shield a signal from the RFID tag responsive to whether the container is open or closed.

[0011] Various embodiments of the invention include a vehicle comprising a receptacle attached to the vehicle and configured to receive an identification device including an RFID tag, and a radio frequency shielding attached to the receptacle and configured to shield the RFID tag when the identification device is placed within the receptacle.

[0012] Various embodiments of the invention include a purse comprising a receptacle configured to receive an identification device including an RFID tag, and a radio frequency shielding attached to the purse and configured to shield the RFID tag when the identification device is placed in the receptacle.

[0013] Various embodiments of the invention include a wallet comprising a receptacle configured to receive an identification device including an RFID tag, and a radio frequency shielding attached to the wallet and configured to shield the RFID tag when the identification device is placed in the receptacle.

[0014] Various embodiments of the invention include a shielded RFID device comprising an identity device including an RFID tag, and a cover physically attached to the device, the cover including a radio frequency shielding material configured to shield the RFID tag in a first position and to not shield the RFID tag in a second position.

[0015] Various embodiments of the invention include an identification device comprising a base including a surface configured to display identifying information, an RFID tag configured to transmit identifying information, and a cover including a radio

SAMSUNG EXHIBIT 1010, Page 292

frequency shielding material configured to shield the RFID tag when closed and to allow the RFID tag to communicate with a reader when open.

[0016] Various embodiments of the invention include a passport device comprising an RFID tag configured to transmit identifying information, a surface configured to visually display the identifying information, and an attached cover including a radio frequency shielding material configured to shield the RFID tag when the cover is closed, and configured to enable reading of the RFID tag when the cover is open.

[0017] Various embodiments of the invention include a passport device comprising a first cover part including identifying information on an inside surface, a second cover part separated from the first cover part by a fold, an RFID tag within the first cover or the second cover part, and a page between the first cover part and the second cover part, the page including shielding configured for shielding the RFID tag in a first position and not shielding the RFID tag in a second position.

[0018] Various embodiments of the invention include a driver's license device comprising an RFID tag configured to transmit identifying information, a surface configured to visually display the identifying information, and a cover including a radio frequency shielding material configured to shield the RFID tag in a first position, and configured to enable reading of the RFID tag in a second position.

[0019] Various embodiments of the invention include a credit card device comprising an RFID tag configured to transmit account information, an attached cover including radio frequency shielding and configured to move relative to the RFID tag, to shield the RFID tag in a first position, and not to shield the RFID that in a second position.

[0020] Various embodiments of the invention include a shielding device comprising a shielding material configured to be temporally attached to an identity device and to shield an RFID tag within the identity device, and an attachment mechanism configured for attaching the shielding material to the identity device.

[0021] Various embodiments of the invention include a passport reading system comprising an RFID reader, and a base disposed to form a slot between the base and the RFID reader, a width of the slot configured for passage of a passport in an open position such that shielding material within the passport does not interfere with communications between the RFID reader and an RFID tag included in the passport.

[0022] Various embodiments of the invention include a passport reading system comprising a first RFID reader, a second RFID reader, a third RFID reader, the first, second and third RFID readers surrounding a passport reading volume and being disposed such that at least one of the first, second and third RFID readers will be at a proper angle relative to an antenna of an RFID tag within a passport in the passport reading volume to read the RFID tag, and also disposed such that transmission between the RFID tag and the at least one of the first, second and third RFID readers is not prevented by shielding within the passport when the passport is open in the passport reading zone regardless of the angle of the shielding relative to the first, second and third readers.

[0023] Various embodiments of the invention include a system comprising a cover material configured for inclusion in a polarity of identity devices, a strip of shielding deposited on the cover material, a first RFID tag deposited on the cover material, a second RFID tag deposited on the cover material, and a cutting area configured to be cut in order to produce the plurality of identity devices, the cut including cutting of the strip of shielding and separation of the first RFID tag and the second RFID tag.

[0024] Various embodiments of the invention include a passport comprising an RFID tag configured to transmit identifying information, a surface configured to visually display the identifying information, and a cover including a first part and a second part separated by a fold, the first part including the RFID tag and the second part including a radio frequency shielding configured to shield the RFID tag when the cover is closed, and configured to allow reading of the RFID tag when the cover is open, the radio frequency shielding including metallic fibers disposed within the second part.

[0025] Various embodiments of the invention include a passport comprising a first cover part including identifying information including a photograph on an inside surface, a second cover part separated from the first cover part by a fold, an RFID tag within the first cover or the second cover part, and a page between the first cover part and the second cover part, the page including shielding configured for shielding the RFID tag in a first position and not shielding the RFID tag in a second position.

[0026] Various embodiments of the invention include a passport comprising a first cover part including an RFID tag disposed at least 5 mm from a fold, a second cover part

SAMSUNG EXHIBIT 1010, Page 294

separated from the first cover part by the fold and including shielding configured for shielding the RFID tag in a first position of the second cover part and not shielding the RFID tag in a second position of the cover part.

[0027] Various embodiments of the invention include a system comprising a cover material configured for inclusion in a polarity of identity devices, a strip of shielding deposited on the cover material, a first RFID tag deposited on the cover material, a second RFID tag deposited on the cover material, and a cutting area configured to be cut in order to produce the plurality of identity devices, the cut including cutting of the strip of shielding and separation of a location for depositing of the first RFID tag and a location for depositing of the second RFID tag.

[0028] Various embodiments of the invention include a method comprising depositing a radio frequency shielding material on a first part of a cover material, depositing at least a first radio frequency identity tag and a second radio frequency identity tag on a second part of the cover material, cutting the cover material through the radio frequency shielding, and creating a fold in the flexible material, the fold separating the first part of the cover material from the second part of the cover material.

[0029] Various embodiments of the invention include a remotely powered RFID (radio frequency identity) tag having an electronically controlled switch. This switch is optionally a remotely (wirelessly) controlled switch. In some embodiments, when the switch is in an off state, the RFID tag will not transmit and when the switch is in an on state the RFID tag will transmit in response to an RF (radio frequency) signal. In some embodiments, the switch includes multiple on states in which different information or signals are transmitted responsive to the state of the switch. The RFID tag includes a memory configured to store the states of the RFID tag and an integrated circuit configured to determine whether to transmit responsive to the stored state of the RFID tag and a received RF signal.

[0030] Various embodiments of the invention include switchable RFID devices. These switchable RFID devices can include identity documents such as passports or driver's licenses, financial cards such as credit or debit cards, remote controls, security devices, access devices, communication devices, or the like. In some embodiments, more than one switchable RFID tag is included in a single RFID device. In various

embodiments, one or more switches are used to change operation of an RFID tag from a responsive state to a non-responsive state, to change operation of an RFID tag from one responsive state to another responsive state, to enter data into an RFID device, to control an external device, or the like. In various embodiments, the switches are electronic, wireless, and/or mechanical.

[0031] Various embodiments of the invention includes an RFID tag comprising an antenna configured to receive data in a first RF signal, to receive energy from the first RF signal, and to transmit data in a second RF signal, the transmission of the second RF signal being powered by the energy received from the first RF signal; and an integrated circuit including an input configured to receive data from the antenna and to receive power resulting from the energy received from the antenna, an output configured to provide an RF signal to the antenna for transmission, a state memory configured to store an ON/OFF state of the RFID tag, a key memory configured for storing a key for changing the ON/OFF state stored in the state memory, and a switch logic configured to receive data from the input, to read the key from the key memory, to compare the received data with the read key, and to change the ON/OFF state stored in the state memory responsive to this comparison, the switch logic is further configured to determine whether or not to provide a second RF signal to the antenna for transmission, the determination being responsive to the ON/OFF state stored in the state memory.

[0032] Various embodiments of the invention include a method of changing an ON/OFF state of an RFID Tag, the method comprising receiving energy sufficient to power the RFID Tag through an RF antenna included in the RFID tag, receiving first data through the RF antenna, reading a key from a key memory, using an integrated circuit to compare the first data received through the RF antenna with the key read from the key memory, the integrated circuit powered by the received energy, and writing data to state memory responsive to the comparison, the data written to the state memory being configured to change the RFID tag from an OFF state in which the RFID tag will not transmit an RF signal to an ON state in which the RFID tag will transmit an RF signal.

[0033] Various embodiments of the invention includes a method of operating an RFID tag, the method comprising receiving energy sufficient to power the RFID tag

through an RF antenna included in the RFID tag, reading a state from state memory, sending an RF response through the RF antenna unless the read state is an OFF state.

[0034] Various embodiments of the invention includes a method of operating an RFID tag, the method comprising receiving energy sufficient to power the RFID tag through an RF antenna included in the RFID tag, reading a state from state memory, sending an RF response through the RF antenna if the read state is an ON state, and disabling the RF response through the RF antenna if the read state is an OFF state.

[0035] Various embodiments of the invention includes a method of operating an RFID tag, the method comprising receiving energy sufficient to power the RFID tag through an RF antenna included in the RFID tag, reading a state from state memory, sending an RF response through the RF antenna only if the read state is an ON state.

[0036] Various embodiments of the invention includes a multilayer identity document comprising a first outer layer, an electrical conductor configured to conduct a current, a spacer layer including an opening configured to contain a switch activator, the switch activator configured to make and break an electrical connection to the electrical connector, and an inner layer disposed such that the spacer layer and switch activator are between the first outer layer and the second outer layer, the inner layer being configured to be pressed to activate the switch activator.

[0037] Various embodiments of the invention includes a switchable RFID tag comprising an antenna configured to receive an RF transmission, an integrated circuit configured to generate a response transmission, and a switch configured to turn on and of the ability of the integrated circuit to generate the response transmission, the switch being disposed such that it is surrounded by the antenna.

[0038] Various embodiments of the invention includes a system comprising a plurality of switches configured for a user to enter data, logic configured to transmit a first wireless signal responsive to the entered data, and a circuit configured to receive energy from a received second wireless signal and to power the logic and the transmission of the system using the received energy.

[0039] Various embodiments of the invention includes a system comprising logic configured to transmit a first wireless signal in response to a received second wireless signal, a wireless I/O configured to receive the second wireless signal and to transmit the

first wireless signal, a memory configured to store an account number, the account number being included in the first wireless signal, a physical contact I/O configured for writing the account number to the memory, logic configured to allow writing of the account number to the memory if the account number is received via the physical contact I/O but if the account number is received via the wireless I/O, and a circuit configured to receive energy from the received second wireless signal and to power the logic and the transmission of the first wireless signal using the received energy.

[0040] Various embodiments of the invention includes a system comprising logic configured to transmit a first wireless signal in response to a received second wireless signal, a wireless I/O configured to receive the second wireless signal and to transmit the first wireless signal, the second wireless signal including an identification data associated with a reader, a memory configured to store a log of received identification data received from a plurality of readers, a physical contact I/O configured for uploading the log of received identification data from the memory, logic configured to allow uploading of the log of received identification data from the memory via the physical contact I/O but via the wireless I/O, and a circuit configured to receive energy from the received second wireless signal and to power the logic and the transmission of the first wireless signal using the received energy.

[0041] Various embodiments of the invention includes a method comprising mounting a plurality of RFID antenna and RFID tags on a support, mounting a the support on a first side of a spacer, the spacer including opening 140 and optionally including one or more cavity to receive the RFID tags, mounting a cover layer on a second side of the spacer, and cutting the support and spacer to generate a plurality of RFID enabled financial Cards.

[0042] Various embodiments of the invention include a method comprising mounting an RFID antenna and RFID tag on a support, mounting a spacer on the support, the spacer being compliant (soft) so that the RFID tag can enter a plane of the spacer to form a cavity, allowing the spacer to harden, and mounting a cover layer on the spacer.

[0043] Various embodiments of the invention include a method of assembling an identity device, the method comprising depositing an integrated circuit, antenna and

switch contacts on a support layer , and laminating the support layer, spacer and flexible membrane together, the spacer having a cavity in which the integrated circuit fits.

[0044] Various embodiments of the invention include a method of assembling an identity device, the method comprising depositing an integrated circuit, antenna and switch contacts on a support layer 150, depositing spacer 120 on the support layer, spacer 120 covering the integrated circuit, and depositing a flexible membrane on the support layer, the flexible membrane or the support layer optionally including an image of a user. The Spacer is optionally configured to create a hermetic seal around the integrated circuit and/or the RFID antenna.

[0045] Various embodiments of the invention include a method comprising programming data to non-volatile memory of an RFID tag in a programmable mode, and changing a state of a switch coupled to the RFID tag so as to change the RFID tag from the programmable mode to a non-programmable mode.

[0046] Various embodiments of the invention include an RFID tag comprising an antenna configured to transmit data, a power circuit configured to provide power, an integrated circuit configured to receive power from the power circuit, to provide the data to the antenna, the integrated circuit including a non-volatile memory configured to store the data and a logic circuit configured to determine a state of a switch, the switch being configured to control whether the volatile memory can or cannot be programmed.

[0047] Various embodiments of the invention include an integrated circuit comprising a first logic input configured for determining a state of a switch, a power input configured to receive power from a radio frequency antenna, the received power being sufficient for powering the integrated and transmitting a data output signal via the radio frequency antenna, and a data output configured for generating the data output responsive to the state of the switch as determined by the first logic input.

[0048] Various embodiments of the invention include an Identity Device comprising an RFID antenna configured to receive power from and communicate with an RFID reader, a circuit configured to receive power from the RFID Antenna, a tag configured to be powered by power received through the RFID antenna and to generate a signal for transmission between the RFID antenna and the RFID reader, and a switch configured to repeatedly turn on and turn off detectability or readability of the tag.

SAMSUNG EXHIBIT 1010, Page 299

[0049] Various embodiments of the invention include a locking mechanism comprising a RFID tag activation circuit configured to turn on a switchable RFID tag by operating a switch within the switchable RFID tag, an RFID reader configured to read the switchable RFID tag, and a lock configured to open responsive to the RFID reader.

[0050] Various embodiments of the invention include a method of operating an RFID tag, the method comprising activating a switch in order to turn on the detectability or readability of the RFID tag, the RFID tag powered by power received through an RFID antenna, and activating the switch in order to turn off the detectability or readability of the RFID tag. In some embodiments, the switch is configured to keep the readability of the RFID tag off until the switch is activated again. The switch optionally being included in an identity device.

[0051] Various embodiments of the invention include a method of operating a switchable RFID tag, the method comprising operating a switch to turn the RFID tag on, responsive to a first action of a user, receiving a signal at an RFID antenna, collecting power from the signal, using the collected power to power an integrated circuit, collecting data from the signal, processing the collected data using the integrated circuit, transmitting a signal generated by the integrated circuit in response to the collected data, using the RFID antenna, and operating the switch to turn the RFID tag off, responsive to a second action of a user.

[0052] Various embodiments of the invention include a switchable RFID tag comprising an RFID antenna configured to receive power from and communicate with an RFID reader, a tag configured to be powered by power received through the RFID antenna and to generate a signal for transmission between the RFID antenna and the RFID reader, and a switch configured to repeatedly turn on and turn off detectability or readability of the tag.

[0053] Various embodiments of the invention include a method of controlling an electronic device, the method comprising receiving a wireless RF signal from an RF transmitter, converting the received RF signal into electronic power, generating a wireless return signal using the electronic power, the wireless return signal configured to control the electronic device, placing a switch in a first position to turn on the generation of the wireless return signal, placing the switch in a second position to turn off the

generation of the wireless return signal, and returning the switch to the first position to turn on the generation of the wireless return signal.

[0054] Various embodiments of the invention include a method of controlling an electronic device, the method comprising receiving a wireless RF signal from an RF transmitter; converting the received RF signal into electronic power; repeatedly changing a switch from a first position to a second position; and generating a wireless return signal using the electronic power, the wireless return signal configured to control the electronic device and being responsive to whether the switch is in the first position and the second position.

[0055] Various embodiments of the invention include a system comprising an antenna configured to receive a wireless RF signal from an RF transmitter, a power circuit configured to convert the RF signal into electronic power, a circuit configured to receive the electronic power and to send a wireless response signal in response to the RF signal, and a first switch configured to repeatedly turn on and off a first operation of the circuit under control of a user.

[0056] Various embodiments of the invention include a method of receiving control instructions, the method comprising, generating a wireless RF signal, transmitting the wireless RF signal to a RF powered remote control device configured to send a wireless return signal responsive to the states of one or more switches, the return signal being generated and transmitted using power converted from the wireless RF signal, receiving the return signal, and determining the states of the one or more switches using the received return signal.

[0057] Various embodiments of the invention include a system comprising a RF transmitter configured to send a wireless RF signal, a controlled device, a RF powered remote control configured to be powered by the wireless RF signal and to send a wireless response signal to the controlled device responsive to a first switch, the first switch configured to be repeatedly turned on and off by a user.

[0058] Various embodiments of the invention include a method of operating an RFID tag, the method comprising receiving energy sufficient to power the RFID tag through an RF antenna included in the RFID tag, reading a state from state memory, and sending an RF response through the RF antenna unless the read state is an OFF state.

[0059] Various embodiments of the invention include a method of operating an RFID tag, the method comprising receiving energy sufficient to power the RFID tag through an RF antenna included in the RFID tag, reading a state from state memory, sending an RF response through the RF antenna if the read state is an ON state, and disabling the RF response through the RF antenna if the read state is an OFF state.

[0060] Various embodiments of the invention include a method of operating an RFID tag, the method comprising receiving energy sufficient to power the RFID tag through an RF antenna included in the RFID tag, reading a state from state memory, sending an RF response through the RF antenna only if the read state is an ON state.

[0061] Various embodiments of the invention include a communication device comprising: a 802.11 or cellular transmitter; a user interface configured for a user to enter data; and a switchable RFID tag including an active state and an inactive state and being configured to switch between the active state and the inactive state responsive to the data.

[0062] Various embodiments of the invention include communication device comprising: a 802.11 or cellular transmitter; a first slot configured to receive a first memory device having first data to be transmitted by a first RFID tag; a second slot configured to receive a second memory device having second data to be transmitted by the first RFID tag or a second RFID tag; and a user interface configured for a user to select whether to transmit the first data or the second data; the data optionally including financial account information or a digital key to a lock.

[0063] Various embodiments of the invention include a portable communication device such as a cellular telephone, a blackberry, a wireless personal digital assistant, or the like. The portable communication device includes an optionally switchable RFID tag configured to communicate with a local device via RFID technology as well as more distant devices using other RF technology such as Bluetooth, WiFi, WiMAX, 802.11 or cellular standards. The communication via the RFID tag is optionally at a different frequency than the communication using other technology. Two separate antennae are optionally used to communicate at these different frequencies. An electronically configurable antenna is optionally used to communicate at these different frequencies.

[0064] A user interface of the communication device is configured to control operation of the RFID tag. For example, the user interface may be used to turn on or off

SAMSUNG EXHIBIT 1010, Page 302

operation of the RFID tag, to enter security data into the RFID tag, to enter financial information (e.g., a credit or debit card number into the RFID tag, to enter an identifying number (e.g., telephone number) into the RFID Tag, or to enter account number into the RFID tag. The communication device may be configured for a user to enter the above data into the communication device using the user interface for later transmission (optionally encrypted) using the RFID Tag. For example, a user may enter a credit card number that is later transmitted in an encrypted form to an RFID reader.

[0065] In Various embodiments, the communication device is configured to receive one or more memory devices configured to store data such as financial or account information. For example, in some embodiments the communication device includes a plurality of slots configured to receive memory having credit card data stored thereupon. In these embodiments, the memory is used to provide the data to the communication device. A particular communication device is configurable to operate with respect to different financial accounts dependent on which particular memories have been inserted into the slots. Thus, a user may receive a first memory issued by a first bank and a second memory issued by a second bank, and install both the first memory and the second memory into the communication device. The user interface of the communication device may then be used to select which account (e.g., the first bank or second bank accounts) should be used for a particular transaction. For example, activating a first switch may result in a transaction being debited from a first account and activating a second switch may result in a transaction being debited from a second account. In some of these embodiments, the use of RFID is optional. For example, the transactions may be performed using cellular RF transmissions from a cellular telephone.

[0066] In some embodiments, the memory device may be configured to fit both a financial card including an RFID tag for transmission of data stored in the memory device, and also to fit within one of one or more slots within a cellular phone or similar communication device. In these embodiments, the memory device is optionally configured to act as a key allowing whatever device it is attached to to engage in a financial transaction.

[0067] In some embodiments, the memory devices are each packaged with an optionally switchable RFID tag. Thus, both the memory and the RFID tag are inserted

SAMSUNG EXHIBIT 1010, Page 303

into a slot of the communication device. The communication device need not include an RFID tag prior to insertion of a memory device. In some embodiments, the memory devices further include a separate antenna for use by the RFID tag. In alternative embodiments, the RFID tag is configured to use an antenna previously installed in the communication device.

[0068] Various embodiments of the invention include a memory device configured to be disposed within a financial card such as a credit card, to be removed from the credit card and to be inserted into the communication device. Thus, the memory device can be transferred from a credit card to the communication device. In some embodiments, transfer of the memory device includes transfer of an RFID tag. In some embodiments, transfer of the memory device includes transfer of an antenna for use by the RFID tag. In alternative embodiments the RFID tag is configured to use a first antenna included in the credit card and a second antenna included in the communication device, these antenna being separable from the memory device.

[0069] In some embodiments the user interface of the communication device is configured to enter an ID of an RFID reader in order to assure that a transaction takes place with the proper RFID reader. For example, in one embodiment several vending machines each include a numbered RFID reader. A user enters the number of a desired member of the several vending machines in order to be sure that the transaction doesn't accidentally occur with an adjacent vending machine.

[0070] In some embodiments, the user interface of the communication device is configured for entering an amount of a financial transaction, e.g., an amount of an electronic payment.

[0071] In some embodiments, the communication device is configured to use voice recognition to approve an RFID based financial transaction. For example, in some embodiments voice recognition authentication may be required before an RFID tag is activated.

[0072] Some embodiments of the invention include a cellular phone configured to use two or more communication modes: one mode for cellular operation and one mode, e.g., RFID, for short range financial transactions or lock operation. These modes may use different frequency ranges.

[0073] In some embodiments, a memory device inserted in a slot of the communication device is configured to operate a lock, optionally via RFID. The communication device may be configured to accept more than one memory device configured to activate a lock and/or engage in a financial transaction. In some embodiments, a memory device inserted in a slot of the communication device is configured as a remote control (e.g., as a car remote or a television remote).

[0074] In some embodiments, the user interface of the communication device is configured to receive an access code before the RFID tag is detectable. For example, prior to receiving the access code the RFID tag may be disabled from sending radio frequency signals.

[0075] In some embodiments, a power source of the communication device is used to power the RFID tag. In these embodiments the RFID tag does not need to generate power from a received inductive or RF signal. In some embodiments, the RFID tag is configured to receive power from the power source of the communication device when the communication device is ON, and to generate power from a received inductive or RF signal when the communication device is off. In some embodiments, the RFID tag is configured to receive power from the power source of the communication device when the communication device is ON, and to be unresponsive when the communication device is off. In some embodiments, the RFID tag is configured to receive power from the power source of the communication device when the communication device is ON or OFF. For example, in one embodiment the RFID tag is configured to draw power from the power source of the communication when an incoming signal is detected but to draw reduced or no power from the power source when no incoming signal is detected.

[0076] In some embodiments, the RFID tag is included in a replaceable battery cover of the communication device. Thus, the RFID tag may be changed by changing the battery cover. In some embodiments, the RFID tag or memory device is included in a replaceable antenna component of the communication device. In some embodiments the RFID tag or memory device is configured to fit into an audio plug of the communication device. In some embodiments, the memory device or RFID tag is configured to fit into a MiniSD slot of the communication device. In some embodiments, the memory device or RFID tag is configured to fit into the same interface as a power cord of the

SAMSUNG EXHIBIT 1010, Page 305

communication device. In some embodiments the communication device has a form factor that can be opened and closed (e.g., a clamshell cell phone) and operation of the RFID tag is responsive to whether the communication device is open or closed. For example, in one embodiment the RFID tag is inactive unless a cell phone is opened.

BRIEF DESCRIPTION OF DRAWINGS

[0077] FIG. 1 illustrates a container including a receptacle configured to store an ID incorporating an RFID tag, according to various embodiments of the invention.

[0078] FIG. 2 illustrates a container including an RFID tag or alternatively an RFID tag reader.

[0079] FIG. 3 illustrates various monitoring systems that employ illustrative embodiments of the container of FIG. 2.

[0080] FIG. 4 illustrates further details of an embodiment of the container of FIG. 2 that includes a monitored vial.

[0081] FIG. 5 illustrates another embodiment of a monitored vial that includes more than one compartment.

[0082] FIG. 6 illustrates an embodiment of the container of FIG. 2 wherein the container is a room.

[0083] FIG. 7 illustrates an access system based on an RFID tag, according to various embodiments of the invention.

[0084] FIG. 8 illustrates a clamshell ID including a base including an RFID tag and a cover connected to the base, according to various embodiments of the invention.

[0085] FIG. 9 illustrates a clamshell ID similar to that shown in FIG. 8 except that the base and cover are pivotally connected at a point rather than along an edge, according to various embodiments of the invention.

[0086] FIGs. 10A and 10B illustrate an ID similar to that shown in FIGs. 8 and 9 except that the cover is configured to fit into the base, according to various embodiments of the invention.

[0087] FIG. 11 illustrates further detail of some embodiments of a clamshell ID having a first cover and second cover separated by a fold.

[0088] FIG. 12 illustrates further embodiments of a clamshell ID including a first cover and second cover separated by a fold.

SAMSUNG EXHIBIT 1010, Page 306

[0089] FIG. 13 illustrates a clamshell ID wherein shielding is added to a page, according to various embodiments of the invention.

[0090] FIG. 14 illustrates an identification device, according to various embodiments of the invention.

[0091] FIG. 15 illustrates a method of allowing communication to an RFID tag, according to various embodiments of the invention.

[0092] FIG. 16 illustrates a method of modifying an RFID enabled identification device, according to various embodiments of the invention.

[0093] FIG. 17 illustrates a method of making an identity device including, according to various embodiments of the invention.

[0094] FIG. 18 is a block diagram illustrating a stage in the manufacture of an identification device, according to various embodiments of the invention.

[0095] FIG. 19 illustrates the method of manufacturing an identification device, according to various embodiments of the invention.

[0096] FIG. 20 illustrates an RFID reader system, according to various embodiments of the invention.

[0097] FIG. 21 illustrates an alternative RFID reader system, according to various embodiments of the invention.

[0098] FIG. 22 is a block diagram of a switchable RFID device, according to various embodiments of the invention;

[0099] FIGs. 23 and 24 illustrate some of many possible locations for a switch within a switchable RFID device, according to various embodiments of the invention;

[00100] FIG. 25A illustrates an OFF Position of a switch, according to various embodiments of the invention;

[00101] FIG. 25B illustrates an ON position of a switch, according to various embodiments of the invention;

[00102] FIGs. 26A and 26B illustrates a membrane switch, according to various embodiments of the invention;

[00103] FIG. 26C illustrates an embodiment of a membrane switch including a spring, according to various embodiments of the invention;

[00104] FIG. 26D illustrates a cross-sectional view of a membrane switch disposed within a switchable RFID Tag, according to various embodiments of the invention;

[00105] FIG. 27 illustrates a top view of a membrane switch, according to various embodiments of the invention;

[00106] FIG. 28 illustrates a switchable RFID tag in an identity document, according to various embodiments of the invention;

[00107] FIG. 29 illustrates the manufacture of instances of an identity document, according to various embodiments of the invention;

[00108] FIG. 30 illustrates an exploded view of an embodiment of a switchable RFID device including a driver's license, according to various embodiments of the invention;

[00109] FIG. 31 illustrates an embodiment of a switchable RFID device including a plurality of switches, according to various embodiments of the invention;

[00110] FIG. 32 illustrates various embodiments of an tag configured for use in embodiments of a switchable RFID device including a plurality of switches, according to various embodiments of the invention;

[00111] FIG. 33 illustrates an instance of a tag, according to various embodiments of the invention;

[00112] FIG. 34 illustrates a method according to various embodiments of the invention, according to various embodiments of the invention;

[00113] FIG. 35 illustrates a switchable RFID device configured to operate as a remote control, according to various embodiments of the invention;

[00114] FIG. 36 illustrates a multiswitch credit card, according to various embodiments of the invention;

[00115] FIGs. 37A-37C illustrate an antenna within a credit card, according to various embodiments of the invention;

[00116] FIG. 38 illustrates an RFID device including a conductor configured to set a state of an RFID tag, according to various embodiments of the invention.

[00117] FIG. 39 is a block diagram illustrating an RFID tag, according to various embodiments of the invention;

[00118] FIG. 40 is a flowchart illustrating a method of changing a state of the RFID tag illustrated in FIG. 22, according to various embodiments of the invention; and

[00119] FIG. 41 is a flowchart illustrating a method of operating the RFID tag illustrated in FIG.22, according to various embodiments of the invention.

DETAILED DESCRIPTION

[00120] Various embodiments of the present invention includes holders (e.g., containers) including radio frequency shielding materials to protect items, such as IDs (identification devices), incorporating RFID tags from being read. In some embodiments, a person can allow information within an RFID tag to be read by removing the item from the holder, while in other embodiments the holder is merely opened or removed to allow the RFID tag to be read. Replacing the item within the holder, or closing the holder, secures the item's RFID tag from unwanted readings from, or detection by, unknown or unauthorized RFID readers. It will be appreciated that items other than IDs, such as library books, consumer electronics, medications, and so forth, can also include, or be packaged with, RFID tags that a person may wish to shield from unauthorized RFID readers. Holders specifically tailored for such items, as well as general purpose holders such as wallets, purses and briefcases, can also include radio frequency shielding (also referred to herein as shielding) according to the present invention.

[00121] The holder can be in the general form of a container as an illustrative example, having two similar rectangular sides joined around three edges, being configured to be repeatedly opened and close, and optionally including a closure or flap along the fourth side. Such holders are well suited to the typical shape of most personal IDs such as passports, driver's licenses, green cards, credit and debit cards, medical information cards, insurance cards, medical alerts, student identification cards, security badges, immigration documents, or the like. Typically, the holder is configured to be repeatedly opened and closed to receive the ID.

[00122] The holder can also be a case such as a carrying-case for a cell phone or digital camera. The holder can also be a purse, suitcase, backpack, briefcase, satchel, glove compartment, a jewelry container, and the like. In some embodiments, the RF shielding is physically attached to the holder. The holder can alternatively include a checkbook holder, a wallet, a ticket holder, or a windshield visor pocket. Some embodiments of the invention are directed at articles of clothing in which one or more

pockets include an attached radio frequency shielding material. Additional embodiments are directed to key holders.

[00123] The desirability of RFID shielding for the objects listed above will be readily appreciated. Being able to read an RFID tag on a green card (an immigration document) without the owner of the green card giving consent or being aware that the green card is being read, for example, can enable less scrupulous individuals to engage in improper behaviors. Incorporating RFID shielding into a wallet, purse, or other type of holder would prevent an RFID tag on an item within the holder from being read unless the item is deliberately exposed to the RFID reader, for instance, by removing the item from the holder. In view of the problem of identity theft, such shielding is desirable for credit cards with RFID tags, social security cards with RFID tags, driver's licenses with RFID tags, and so forth.

[00124] In some instances the RFID tag is essentially a label that has been attached to an object for inventory or similar purposes. Library books can carry RFID tags, for example. Accordingly, providing RFID shielding for various carrying devices, such as purses, suitcases, book bags, briefcases, and satchels can prevent RFID tags in library books and other objects from being read without permission. In other instances the RFID tag is more integral with an object. Consumer electronics, electronic media, and so forth, can be manufactured to include RFID tags inside of housings, on printed circuit boards, and on electronic components, for example. Often, such devices have specially designed cases such as cell phone cases and camera cases. These cases can also comprise RFID shielding to prevent the RFID tags in the associated devices from being read without authorization.

[00125] In some embodiments, the holder is clear (e.g., transparent) so that the ID, such as a driver's license, can be readily seen without having to be removed from the holder. Many wallets include either a plastic sleeve or a leather pocket with a plastic window for this purpose. In some embodiments, of the invention in which at least part of the holder is transparent, the shielding in the transparent region needs to also be transparent. Certain electrically conductive polymers can serve as the RFID shielding material in these embodiments. Other transparent and non-transparent materials for RFID shielding are discussed further herein.

[00126] In some embodiments, the holder is designed to allow the ID to be easily and repeatedly removed and returned. For instance, some credit and debit cards have a smaller format (mini-cards) and can be stored in a matching case that can serve as a fob for keys. In some of these embodiments, the holder and the ID card are pivotally attached to one another so that the ID card can flip out from the holder, and in still further embodiments a spring mechanism aids in extending and retracting the ID card. Other cases of the present invention can comprise a clamshell configuration. Such ID card holders of the present invention include an RFID shielding material.

[00127] The present invention also provides for articles of clothing designed to include pockets that can shield RFID tags on objects within the pockets. In these embodiments the articles of clothing can be made from a cloth that includes a radio frequency shielding material, or the pocket can be lined with the radio frequency shielding material.

[00128] The present invention also provides for key holders comprising RFID shielding. The keys that are held by such key holders can be either mechanical or electronic, where mechanical is used herein to refer to keys meant to fit into mechanical locks such as car keys, house keys, and the like. Electronic keys refer to keys that carry an encoded password on a magnetic strip, a bar code, an RFID tag, or the like. Either type of key can include an RFID tag as either a further component of the locking mechanism or for completely unrelated reasons. An RFID tag on a key is part of the locking mechanism, for example, when the lock reads the RFID tag for some purpose, such as to read the key numbers from RFID tags on different keys in order to track which keys are being used in the lock.

[00129] Electronic keys are often placed on ID badges and other forms of identification. An RFID tag with such electronic keys may carry confidential information but be unrelated to the lock mechanism. In some embodiments, the key holder is retractable, and in some of these embodiments the key holder is spring-loaded to automatically retract the key into the key holder.

[00130] In the embodiments described herein, the holder, whether an container, case, article of clothing, or key holder, has some form of opening through which the ID or other object having an RFID tag can be transferred. In some embodiments, the holder also includes a closure for closing the opening. In some of these embodiments, the

closure can comprise a flap that closes over the opening. In other embodiments the closure is a zipper, Velcro, or related closure device. The closure can provide an electrical contact between opposing sides of the opening, in some instances.

[00131] In some embodiments, the RFID shielding material is incorporated into an ID. For example, a passport can include an RFID shielding material in the passport's cover so that an RFID tag within the passport can only be read when the passport is opened. Similarly, a driver's license can include a clamshell cover and base including an RFID shielding material, or a pivoting cover including an RFID shielding material.

[00132] The RFID shielding material can be provided in numerous different ways. The radio frequency shielding material can include a conductive material such as a metal or an electrically conductive plastic. The RFID shielding can be attached using adhesive. The radio frequency shielding material can include a mesh with a mesh size small enough to provide shielding against the radio frequency range used by RFID readers. The radio frequency shielding material can be laminated, either by laminating the RFID shielding material to another layer, such as a protective material layer, and/or by laminating together multiple layers of RFID shielding materials. In many embodiments the RFID shielding material is either flexible, transparent, or both. Examples of suitable RFID shielding materials include metal-coated elastomers such as aluminized Mylar and copper-coated plastic sheets and films. In some embodiments, the RFID shielding material is a semi-transparent mesh.

[00133] In some embodiments, the RFID shielding material is effective to form a Faraday cage around the ID, object, or key. Closing the closure can be effective to complete the Faraday cage, in some instances. In other embodiments the RFID shielding is used in selective locations in the holder. For example, where a nation's passport includes an RFID tag in a lower right-hand corner of the cover, passport holders designed for that nation's passports need only include RFID shielding above and/or below the location of the RFID tag when the passport is in the passport holder.

[00134] The RFID shielding shields an RFID tag from a reader in two ways. First, the RFID shielding greatly reduces the power being broadcast from the reader that reaches the RFID tag within the holder. This cuts the power available to the RFID tag to transmit information back. Secondly, even if the RFID tag receives enough power to transmit, the

signal sent from the RFID tag is also attenuated. Accordingly, it will be appreciated that the effectiveness of the RFID shielding can be varied considerably based on choices of radio frequency shielding materials and their thicknesses, mesh sizes, and so forth. In some embodiments, the radio frequency shielding material provides a reduction of input power to the RFID tag by between about 5db-30db, 10db-25db, 15db-20db, or more than 15, 25, 35 or 45 db.

[00135] In some embodiments, the container is configured to be repeatedly opened and closed to receive an item including an RFID tag. In some embodiments, the container includes a closure configured to enhance the shielding.

[00136] In some embodiments, the container configured to just fit a standard California driver's license. These embodiments may be characterized by inner dimensions of less then 3.5 inches, 3.75 inches, 4 inches or 4.5 inches height, and less than 2.25 inches, 2.5 inches or 2.75 inches in width. In some embodiments, the container is configured to just fit a U.S. passport or a passport issued by another country. These embodiments may be characterized by inner dimensions of less then 5 inches, 5.25 inches, 5.5 inches or 6 inches in height, and less than 3.5 inches, 3.75 inches, 4 inches or 4.5 inches in width.

[00137] FIG. 1 illustrates a Container 100 including a Receptacle 110 configured to store an ID 130 (identification device) incorporating an RFID Tag 140. The Container 100 and Receptacle 110 may include a wallet, purse, passport holder, key chain, ticket holder, pocket, sleeve, slot, opening, niche, compartment, lid & base, glove compartment, jewelry, suitcase, backpack, bag, carrier, carton, box, sack, carton, casing, shell, carapace, covering, sheath, or the like. Container 100 further includes attached Shielding 120 configured to attenuate the transmission of radio frequency signals to or from the RFID Tag 140. Receptacle 110 is configured to be repeatedly opened and repeatedly closed for insertion and removal of ID 130.

[00138] FIG. 2 illustrates an embodiment of a Container 200 including RFID Tag 140 or alternatively an RFID tag Reader 210. Container 200 is optionally an embodiment of the Container of FIG. 1, and visa-versa. Container 200 further includes Shielding 120 configured to attenuate the transmission of radio frequency signals to or from the RFID Tag 140 or Reader 210. The shielding effect of the Shielding 120 is optionally dependent

on a state of the Container 200. For example, in some embodiments, the Shielding 120 may be more efficient at attenuating RF transmission when Container 120 is closed than when it is open. As such, in some embodiments, the state of the Container 200 may be determined by a magnitude of a detected radio frequency signal between RFID Tag 140 and Reader 210 either of which may be within Container 200.

[00139] FIG. 3 illustrates various monitoring systems that employ illustrative embodiments of Container 200. These illustrative embodiments include a wall hanging (e.g., a Picture 320), a Refrigerator 325, a Jewelry Box 330, a Chest of Drawers 335, a Monitored Vial 340, a Filing Cabinet 345, and a Safe 350. In these embodiments, the monitoring systems further include RFID tag Reader 210 and optional Alarm and/or Log 310. Each of these examples of Container 200 include one or more RFID Tag 140 and Shielding 120 (whether shown or not) configured to modify the transmission of RFID signals from Reader 210 to RFID Tags 140 responsive to a state of the Container 200.

[00140] For example, the Picture 320 illustrated includes Shielding 120 (not shown) that surrounds the RFID Tag 140 while Picture 320 is mounted on Wall 330. Shielding 120 is configured such that the attenuation effect of the shielding will be reduced if Picture 320 is removed from Wall 330. For example, Shielding 120 may be disposed to form a Faraday cage around or interfere with the RFID Tag 140 (e.g. be on the back of the picture, optional standoffs, and/or wall) and if Picture 320 is removed from Wall 330 a resulting gap, or reduction in interference, will allow increased RFID signal transmission between the associated RFID Tag 140 and Reader 210. Picture 320 may alternatively be a statue or some other object designed to sit on a surface with an RFID tag between the object and the surface.

[00141] In a similar manner each of the Refrigerator 325, Jewelry Box 330, Chest 335, Monitored Vial 340, Filing Cabinet 345 and Safe 350 includes Shielding 120 configured such that a magnitude of an RFID tag signal received by Reader 210 is dependent on whether the particular container is open or not.

[00142] Reader 210 is configured to detect RFID signals from one or more of the RFID Tags 140 and to generate a responsive output signal. In some embodiments, this responsive output signal is a quantitative or qualitative indication of the state of one or more of the containers. The reader is optionally configured to distinguish the signals

received from each of the one or more RFID tags and, thus, identify which of the containers is open.

[00143] Alarm/Log unit 310 is optionally an alarm system or a logging system configured to activate an alarm or log an event responsive to the output signal of Reader 210. For example, in some embodiments, the Alarm/Log unit 310 is configured to activate an alarm when Picture 320 is removed from the wall or Safe 350 is opened. In some embodiments, the Alarm Log unit 310 is configured to log when Filing Cabinet 345, Chest 335 or Drawers or Refrigerator 325 is opened.

[00144] In alternative embodiments, Reader 210 may be placed within the container and RFID Tag 140 outside.

[00145] FIG. 4 illustrates further details of an embodiment of the Container of FIG. 2 that includes Monitored Vial 340. Monitored Vial 340 includes shielding in a Lid 410 and/or Base 420. When the Lid 410 and Base 420 are attached the shielding attenuates any signal from the enclosed RFID Tag 140. When Lid 410 is opened the attenuation is reduced. The RFID tag is optionally disposed on the underside of Lid 410. The illustrated embodiments are optionally used to monitor the use of medication or other material stored within Monitored Vial 340. The monitored vial is optionally an alternative form of Container 200 and optionally configured to store alternative types of goods. In some embodiments, Reader 210 of FIG. 3 is configured to log when Monitored Vial 340 is opened and closed. For example, if a user has a medication that should be taken at a specific time Reader 210 may be used to detect if Monitored Vial 340 is opened at these times and activate a reminder using Alarm/Log 310 if Monitored Vial 340 is not opened at a time medication should be taken.

[00146] FIG. 5 illustrates another embodiment of Monitored Vial 340 that includes more than one Compartment 510. Each Compartment 510 includes a separate RFID Tag 140 that may be separately identifiable using Reader 210. This embodiment may be used, for example, to monitor an activity that should occur at a variety of different times (e.g., times of day or days of the week.).

[00147] FIG. 6 illustrates an embodiment of the Container of FIG. 2 wherein Container 200 includes a Room 610. In these embodiments, radio frequency signals between RFID Tag 140 and Reader 210 may be used to determine if an opening to the

room is open. Room 610 includes Shielded Wall(s) 620 that block radio frequency signals between Tag 140 and Reader 210 when an Opening 630 is closed. When Opening 630 is open Tag 140 can be detected by Reader 210 and this stage can be logged by Alarm/Log 310. While the illustration shows Reader 210 within Room 610 and RFID Tag 140 outside, these positions are optionally exchanged. Room 610 is optionally a shipping container. RFID Tag 140 is optionally mounted on Opening 630 such that Tag 140 is brought within reading range of Reader 210 when Opening 630 is opened. Opening 630 can be, for example, a window or door.

[00148] FIG. 7 illustrates an access system based on an RFID Tag 140. RFID Tag 140 is optionally implanted within a Animal or Person 720 or attached to an animal collar. A Reader/Lock Control 710 is configured to detect a signal from RFID Tag 140 and to control a Lock 740 in response. Lock 740 controls the function of a Barrier 730, such as a door or gate. Reader/Lock Control 710 is optionally programmable to operate responsive to particular instances of RFID Tag 140.

[00149] The Reader/Lock Control 710 illustrated in FIG. 7 is optionally used in the following manner. RFID Tag 140 is placed within or attached to the Animal or Person 720. Reader/Lock Control 710 is placed in a programming mode. A serial number of the RFID Tag 140 is programmed into the Reader/Lock Control 710 either by digital data entry or communication, or by bringing the RFID Tag 140 within the reading range of the Reader/Lock Control 710, such that the serial number can be read from the RFID Tag 140. The Reader/Lock Control 710 in placed in a normal operation mode wherein it monitor's for the presence of the RFID Tag 140. The RFID Tag 140 is detected by the Reader/Lock Control 710. The serial number is read from the detected RFID Tag 140 by Reader/Lock Control 710. Reader/Lock Control 710 compares the read serial number with the serial number programmed into the Reader/Lock Control 710 while in the programming mode. If the read and programmed serial numbers agree Lock 740 is activated in response. Activation of Lock 730 controls (e.g., locks or unlocks) access through Barrier 730. After the detected RFID tag is no longer detected by the Reader/Lock Control 710, Reader/Lock Control 710 optionally reactivates Lock 740 to return it to a previous state.

[00150] FIG. 8 illustrates a Clamshell ID 810 (e.g. greencard (immigration card), passport, driver's license, transaction card, key card, national identity card, or the like). Transaction cards include credit cards, debit cards, check cards, payment cards, fare (e.g., transit) cards, or the like. Clamshell ID 810 includes an optional picture, a Base 830 including an RFID Tag 140, and a Cover 820 connected to Base 830 in a clamshell configuration, e.g., connected along an edge or Fold 840. Cover 820 and/or Base 830 include RFID shielding configured to attenuate radio frequency signals to or from RFID Tag 140 when Cover 820 is closed (e.g., shut), and to not attenuate, or attenuate to a lesser extent, radio frequency signals to or from RFID Tag 140 when Cover 820 is open. The shielding is optionally laminated into Base 830 and/or Cover 820. In some embodiments, Clamshell ID 810 includes shielding in both Base 830 and Cover 820. Base 820 can be the cover of a passport or other document. In some embodiments, Base 830 includes a plastic card.

[00151] In various embodiments, Clamshell ID 810 includes a passport, driver's license, credit card, etc. that includes RF shielding in one part (e.g., a page or cover) and an RFID tag in another part (e.g., a different page or cover). Not shown in FIG. 8 are pages that may be included between the covers (e.g., Base 830 and Cover 820). The RF shielding and RFID Tag 140 are configured such that, when Clamshell ID 810 is closed the shielding interferes with the RF pickup of the RFID tag to an extent sufficient for reading of RFID Tag 140 to be attenuated.

[00152] In some embodiments, Clamshell ID 810 can be closed in two ways. First, such that a picture and/or other identification information is displayed on the exposed surface of Base 830. Or, second, such that the picture and/or other identification information are covered by Cover 820. These two methods of closure are achieved by rotating Cover 820 and Base 830 relative to each other in different directions around Fold 840. In the first instance, the picture and/or other identification information can be used for identification while RFID Tag 140 is still shielded. Thus, Clamshell ID 810 can be used for identification (non-RFID) without unshielding RFID Tag 140.

[00153] When the Clamshell ID 810 is open, the shielding is less close to RFID Tag 140 and, thus, the interference of the shielding is reduced and RFID Tag 140 can be read. The shielding does not necessarily form a Faraday cage around RFID Tag 140 when

Clamshell ID 810 is closed. In some embodiments, shielding is not included in the part of Clamshell ID 810 that includes the RFID Tag 140. Clamshell ID 810 is optionally formed by laminating RFID Tag 140 and RF shielding between layers of Cover 820 or to a page disposed between Cover 820 and Base 830. Further visible information such as a name and/or photograph can be placed on any surface of the Clamshell ID. Thus, in some embodiments, this visible information is visible when the Clamshell ID is open or closed. In other embodiments, this visible information is visible only when the Clamshell ID is open.

[00154] FIG. 9 illustrates an ID 910 similar to that shown in FIG. 8 except that Base 830 and Cover 820 are pivotally connected at a Pivot Point 920 rather than in a clamshell configuration. Cover 820 is configured to rotate over Base 830 as shown. When Cover 820 covers the Base 830 the RFID Tag 140 is shielded. When Cover 820 is rotated away from Base 830 RFID Tag 140 is unshielded. In some embodiments, Cover 820 may have two sections between which Base 830 fits. Either Cover 820 and/or Base 830 can include the RF shielding.

[00155] FIG. 10A and 10B illustrate an ID similar to that shown in FIGs. 8 and 9 except that Cover 820 is configured to fit into Base 839, or visa versa . In the example shown, Cover 820 slides into and out of a slot in Base 830 and thus shields and exposes, respectively, RFID Tag 140. This embodiment may include an item to be worn such as a medical alert bracelet, an identity tag, a ring, clothing, glasses, or the like. For example, in the case of a medical alert bracelet, the bracelet includes an RFID tag (having medical information) that is only readable when a cover element of the bracelet is opened to expose the RFID tag to an RFID tag reader. When the cover is opened medical personal can read data from the RFID tag. When the cover is closed the medical information is shielded from being read by unauthorized persons and is thus kept confidential.

[00156] One embodiment of the invention includes the credit card (16) and case having sides (12) and (14) as illustrated in U.S. patent application Pub. 2004/0117514. In this embodiment, credit card (16) further (additionally) includes an RFID Tag 140 and sides (12) and/or (14) n further include RF shielding, or visa versa. The credit card may be replaced by an alternative type of ID device, e.g., a driver's license, debit card, or others discussed herein.

[00157] On embodiment of the invention includes the credit card (3) and holder (1) as illustrated in U.S. patent application Pub. 2005/0011776. In this embodiment, credit card (3) further includes an RFID Tag 140 and the holder (1) further includes RF shielding. The credit card may be replaced by an alternative type of ID device, e.g., a driver's license, debit card, or the like.

[00158] One embodiment of the invention includes the carrying case taught in U.S. patent application Pub. 2004/0256469, wherein the carrying case further includes RF shielding.

[00159] One embodiment of the invention includes the credit card and pivoting case described in U.S. patent application Pub. 2004/0237360, wherein an RFID tag is included in one part (e.g., the credit card) and shielding in another part (e.g., the case). Thus, when the credit card is pivoted into the case the RFID tag is shielded. One embodiment of the invention includes a credit card and case illustrated in FIG. 10 of U.S. patent application Pub. 2004/0237360. In this embodiment, the credit card includes an RFID Tag 140 and the case includes shielding. The credit card may be replaced by an alternative type of ID device, e.g., a driver's license, debit card, or the like.

[00160] One embodiment of the invention includes the security wallet illustrated in U.S. patent 4,744,497, wherein the security wallet further includes RFID shielding.

[00161] Various embodiments of the invention include the foldable transaction cards illustrated in US. Patent Applications Pubs. 2004/0169087 and 2004/0089724, wherein shielding is further included in one side of the fold while RFID Tag 140 is further included in the other side. RFID Tag 140 is shielded when the transaction card is folded closed and unshielded when it is open.

[00162] Various embodiments of the invention include the several different folding cards illustrated in U.S. Patent 5,700,037 and Application Pub. 2005/0205665. Wherein these cards further include RFID Tag 140 in one part and shielding in another part, such that in one fold position RFID Tag 140 is shielded by the shielding, and in another fold position RFID Tag 140 is un-shielded.

[00163] One embodiment of the invention includes the credit card case illustrated in U.S. patent application Pub. 2002/0117243. Where in the credit card case further

includes shielding configured to shield an rfid enabled credit card or other identification device.

[00164] FIG. 11 illustrates further detail of some embodiments of Clamshell ID 810, having a First Cover 1110 and a Second Cover 1120 separated by Fold 840. First Cover 1110 and a Second Cover 1120 may be, for example, Base 830 and Cover 820. Fold 840 can be a spine, hinge, crease, or the like. In alternative embodiments, First Cover 1110 and/or Second Cover 1120 can be embodied as a page or pages between covers of an identity document. Shielding 1130 is disposed as part of the second cover (e.g., or on or in an ID document cover or page). Shielding 1130 is optionally disposed away from fold 840 such that, when Clamshell ID 810 is open, the shielding as well separated from RFID Tag 140. In various embodiments, the separation between shielding 1130 and Fold 840 is greater than 5 mm, 10 mm, 15 mm, 20 mm, 25 mm or 30 mm. Likewise, RFID Tag 140 is optionally disposed away from Fold 830. In various embodiments, the separation between RFID Tag 140 (including antenna) and Fold 840 is greater than 5 mm, 10 mm, 15 mm, 20 mm, 25 mm or 30 mm. Alternatively, RFID Tag 140 and/or Shielding 1130 may be disposed to abut Fold 840.

[00165] FIG. 12 illustrates embodiments of Clamshell ID 810 including a First Cover 1210 and a Second Cover 1220 separated by Fold 830. These embodiments further include a Page 1230 disposed between First Cover 1210 and Second Cover 1220. Page 1230 includes RFID Tag 140 or Shielding 1130. For example, these embodiments of Clamshell ID 810 can include a passport including a photograph and identity information within an inside surface (facing toward Page 1230) of First Cover 1210, RFID Tag 140 within First Cover 1210 or Second Cover 1220, and Shielding 1130 within Page 1230. RFID Tag 140 can be shielded and un-shielded by moving Page 1230 close to or away from RFID Tag 140. In embodiments, wherein RFID Tag 140 is included in Second Cover 1220, RFID Tag 140 is shielded when Page 1230 is held close to Second Cover 1220. In this position is may be possible to view the photograph and identity information within the inside surface of First Cover 1210 without un-shielding RFID Tag 140. When Page 1230 is moved away from Second Cover 1220 then RFID Tag 140 is unshielded.

[00166] By including the RF Shielding 1130 with one of the one or more Page 1230, Clamshell ID 810 can be opened without necessarily removing Shielding 1130 from the

vicinity of RFID Tag 140. For example, if RFID Tag 140 is disposed within the back cover, and Clamshell ID 810 is opened such that the inside of the First Cover 1210 is visible, Page 1230 including Shielding 1130 could remain adjacent to Second Cover 1220 and thus limit communication with the RFID Tag 140. To allow communication with RFID Tag 130 Page 1230 including Shielding 1130 is turned such that it moves away from Second Cover 1220. The Shielding 1130 may be attached to Page 1230 or be included within Page 1230. For example, Shielding 1130 may be laminated within Page 1230, be sewn on Page 1230, be glued on Page 1230, be within the material of Page 1230, or otherwise be connected to Page 1230. In various embodiments, Shielding 1130 includes a wire mesh, metallic fibers, metallic particles, metallic thread, or the like. Shielding is optionally attached to a binding of Clamshell ID 810 as Page 1230. Page 1230 is optionally bound to Clamshell ID by stable, pin, wire, thread, adhesive, laminate, or the like.

[00167] FIG. 13 illustrates embodiments of Clamshell ID 810 wherein Shielding 1130 is added to Page 1230 following assembly of Clamshell ID. In these embodiments, Shielding 1130 is included in a Shielding Insert 1310. Shielding Insert 1310 optionally includes Adhesive 1320 or some other mechanism for attaching Shielding Insert 1310 to Page 1230. The attachment of Shielding Insert 1310 to Page 1230 can be permanent or temporary (e.g., Shielding Insert 1310 may be removable). In various embodiments, Shielding Insert 1310 includes a metal plate, wire mesh, metallic fibers, metallic particles, metallic thread, or other forms of shielding.

[00168] The size of Shielding Insert 1310 is optionally the same as or slightly smaller then a European Union Passport, a Japanese Passport, a Chinese Passport, a United States Passport, or the like. Alternatively, in various embodiments, Shielding Insert 1310 is configured in size such that it can be attached to Clamshell ID 810 at least greater than 5 mm, 10 mm, 15 mm, 20 mm, 25 mm or 30 mm from Fold 830. For example, Shielding Insert 1310 may be configured to attach to Page 1230 such that Shielding Insert 1310 extends from near an outer edge (opposite Fold 830) of Page 1230 to within 10 mm of Fold 830.

[00169] FIG. 14 illustrates embodiments of an Identification Device 1410, such as Clamshell ID 810. In these embodiments, Shielding Insert 1310 includes one or more

clips 1420, clamp, pin, slot, rivet, or other mechanism configured for, optionally temporary, attaching Shielding Insert 1310 to Identification Device 1410. In some embodiments Clip 1420 is replaced by a slot configured to receive that part of Identification Device 1410 including an RFID tag. Shielding Insert 1320 is optionally pivotally connected to Identification Device 1210. In the embodiments illustrated by FIG. 14, Fold 830, Second Cover 1220 and Page 1230 are optional. For example, Identification Device 1410 can be a single piece driver's license, credit card, etc. (without separate front and back covers) including RFID Tag 140. Shielding Insert 1310 is configured to be attached to First Cover 1210, Page 1230, and/or Second Cover 1220. In these embodiments Page 1230 need not include shielding. In some embodiments, Shielding Insert 1310 may be attached to that part of Identification Device 1410 that includes RFID Tag 140. In these embodiments, Shielding Insert 1310 is inserted to shield RFID Tag 140 and removed in order to un-shield RFID Tag 140. In some embodiments, Shielding Insert 1310 includes a flat metal plate configured to fit within a passport, e.g., a passport issued by the United States, a European Country, or an Asian Country. In these embodiments, the size of shielding insert may be similar to or slightly smaller than the dimensions of the passport. In some embodiments, Shielding Insert 1310 can include an attachment device, such as Clip 1420, on more than one side (face). As such, Shielding Insert 1310 may be configured to shield and RFID enabled driver's license on one side and an RFID enabled credit card on the other side. Shielding Insert 1310 is optionally approximately the size of a driver's license or credit card. In some embodiments, Shielding Insert 1310 has height and width dimensions similar to or smaller than a page between the front cove and the back cover. Shielding Insert 1310 is optionally thin and optionally flexible.

[00170] As illustrated in FIG. 15, some embodiments of the invention include a method of allowing communication to an RFID tag. The method includes a Step 1510 of opening a front cover of an identification device, such as Clamshell ID 810 or Identification Device 1410, in order to make information included on the inside of the front cover visible, an RF shielding page being kept in proximity of the back cover such that an RF tag within the back cover is unreadable. The RF shielding page can be for example an instance of Page 1230 or a page with Shielding Insert 1310 attached. The

method further includes a Step 1520 of visually presenting the information on the inside of the front cover. The information can include a name, citizenship, photograph, identification number, or the like. A step 1530 includes turning the shielding page away from the back cover such that the RFID tag becomes un-shielded and can communicate with a reader. The shielding page is a page, between the front cover and the back cover, that includes or is attached to RF shielding configured to limit communication with the RFID tag. In alternative embodiments of this method, the rolls of the front cover and back cover are reversed.

[00171] As illustrated in FIG. 16, some embodiments of the invention include a method of modifying an RFID enabled identification device, e.g., Identification Device 1410. This method includes, a Step 1610 of opening the identification device by turning a back cover away from a front cover; a Step 1620 of selecting a page disposed (optionally bound) between the front cover and the back cover; an optional Step 1630 of exposing an adhesive surface on an RF shielding insert, the RF shielding configured to limit RF communication between an RFID tag included in the identification device and a reader; and a Step 1640 of attaching the RF shielding insert to the selected page using the exposed adhesive. In alternative embodiments, the adhesive is optionally replaced by a clip, clamp, pin, slot, or other mechanism configured for temporary attachment to the identification device. The identification device is optionally a passport, driver's license, immigration document, national identity document, or other identification device discussed herein. The RF shielding insert is optionally sized (as discussed elsewhere herein) such that it is disposed at a distance from a fold in the identification device.

[00172] As illustrated by FIG. 17, one embodiment of the invention includes a method of making an identity device including: a Step 1710 of adding an RFID tag to a first cover layer; a Step 1720 of adding a second cover layer such that the RFID tag is disposed between the first cover layer and the second cover layer; and a Step 1730 of a attaching an RF shield to the combined first cover layer and second cover layer. The RF shield is optionally attached as a page configured to be disposed between to parts of the combined first cover layer and second cover layer when the combination is folded. The RF shield is optionally temporally attached to the combined first cover layer and second cover layer.

SAMSUNG EXHIBIT 1010, Page 323

[00173] FIG. 18 is a block diagram illustrating the manufacture of an identification device, such as a passport. At one stage in the manufacturing process Shielding 1130 is dispensed in the form of a strip. The strip is laid down over what will be several separate identification devices when the manufacturing is completed. A plurality of RFID Tags 140 are deposited. The assembled material, including shielding is cut along a Cutting Line 1820 (cutting area) to separate the locations where the RFID Tags 140 are deposited or to be deposited. As a result a plurality of identity documents are produced. The cut along Cutting Line 1820 occurs after Shielding 1130 is laid down. Pages are optionally added to the assembled material prior to cutting.

[00174] FIG. 19 illustrates the method of illustrating an identification device as shown in FIG. 18. In an Add Shielding Step 1910, shielding is added to an area of a cover that will become a first identification device and a second identification device. In an Add RFIDs Step 1920, a first RFID tag is added to that part of the cover that will become the first identification device and a second RFID tag is added to that part of the cover that will become the second identification device. In a Cut Step 1930, the cover is cut to separate that part that will become the first identification device and that part that will be come the second identification device. Cut Step 1930 includes cutting the shielding added in Add Shielding Step 1910.

[00175] FIG. 20 illustrates an RFID reader system configured to read Clamshell ID 810 e.g., an RFID enabled passport including shielding. Spacing between an RFID Reader 2010 and a Base 2020 is configured to form a Passport Slot 2030. RFID Reader 2010 is configured to read Clamshell ID 810. The height of Passport Slot 2030 is configured such that Clamshell ID 810 is sufficiently open when passed though Passport Slot 2030 between the RFID Reader 2010 and Base 2020. E.g., Passport Slot 2030 is configured such that, in order to pass through Passport Slot 2030 Clamshell ID 810 cannot be partially open such that shielding within Clamshell ID 810 could block the communication between RFID Reader 2010 and the RFID tag included in Clamshell ID 810. The width of the passport slot is optionally configured to assure that the shielding is not disposed between the RFID reader and the RFID tag.

[00176] FIG. 21 illustrates an RFID reader system including more than one RFID readers (RFID Reader 2010A, RFID Reader 1010B, and optionally RFID Reader1010C).

The more than one RFID readers are disposed such that any shielding within an ID is never within the line of sites between all of the one or more RFID readers and an RFID tag in a reading volume. And in addition, the more than one RFID readers are disposed such that the angle between an antenna of the RFID tag is at least one of the RFID readers is favorable for communicating between the RFID tag and RFID reader. Achieving both or these criteria may require three or more RFID readers. In alternative embodiments, this system may include fewer or more RFID readers than illustrated. The illustrated readers optionally surround a walk through reading volume.

[00177] FIG. 22 is a block diagram of a Switchable RFID Device 2200. In some embodiments, Switchable RFID Device 2200 is an identity device such as a passport, identity card, driver's license, immigration document (e.g., green card or visa), student identity card, library card, financial card (e.g., credit card, debit card or prepaid card), social security card, Military ID card, key, keycard or the like. Switchable RFID Device 2200 optionally includes Visible Indications 2220 such as a barcode, picture, image, name, address, text, and/or the like. Switchable RFID Device 2200 further includes one or more Switchable RFID Tag 2230. Switchable RFID Tag 2230 includes one or more RFID Antenna 2240, a Circuit 2250, one or more Tag 2260 and one or more Switch 2270. Switch 2270 is optionally disposed within Circuit 2250 or Tag 2260. RFID Antenna 2240 is configured for sending a radio frequency (RF) signal from Switchable RFID Device 2200 in response to a received signal. The received signal is optionally used to power Switchable RFID Tag 2230. In some embodiments, the received signal is an RF signal received by RFID Antenna 2240. In alternative embodiments, the received signal is received through an inductive coupling or a non-RF antenna within Circuit 2250. RFID Antenna 2240 is optionally a dipole antenna. RFID tags can operate in both low frequency (less than 100 MHz) and high frequency (greater than 100 MHz) modes. In low frequency systems, a field interacts with a coil which induces a current that is converted into a digital signal. In high frequency systems, the electric field of a propagating signal gives rise to a potential difference across the tag's dipole antenna, which results in a digital signal.

[00178] In some embodiments, Switchable RFID Tag 2230 is configured for a user to be able to repeatedly turn on and off the function (e.g., delectability or readability) of Tag

2260 using Switch 2270. Circuit 2250 typically further includes a diode, capacitor, transistor, and/or the like configured to receive power through RFID Antenna 2240 or an inductive coupling and to convey signals between RFID Antenna 2240 and Tag 2260. In some embodiments, Tag 2260 includes an integrated circuit.

[00179] Switchable RFID Tag 2230 is differentiated from circuits found in RFID tags of the prior art by at least the inclusion of Switch 2270. Switch 2270 is optical, thermal, magnetic, mechanical, wireless, and/or electronic. Switch 2270 is configured to be activated by a magnetic field, an electric field, a wireless signal, light, heat, mechanical force, and/or an electronic circuit external to Switchable RFID Device 2200. Switch 2270 is optionally a sliding switch, a flip switch, a rotating switch, membrane switch, pushbutton switch, or other mechanical switch known in the art of mechanical switches. In typical embodiments, Switch 2270 is configured for both turning on and turning off function of Tag 2260.

[00180] In various embodiments, Switch 2270 is normally open or normally closed, and the function of Tag 2260 can be normally on or normally off. For example, In some embodiments, Switch 2270 is a mechanical contact switch activated by applying pressure to an outside surface of Switchable RFID Device 2200. In some embodiments, when this pressure is applied the functionality of Tag 2260 will be turned on, and when this pressure is not applied the functionality of Tag 2260 will be off. In some embodiments, Switch 2270 is a mechanical contact switch activated using a magnetic field. In some embodiments, Switch 2270 is an electrical switch turned on or off by a circuit external to Switchable RFID Device 2200. For example, Switch 2270 may include two electrical contacts exposed at the exterior of Switchable RFID Tag 2230. When a conductance path, current and/or voltage is applied between these electrical contacts Switch 2270 is turned on, or in alternative embodiments, turned off.

[00181] In various embodiments, Switch 2270 functions by creating a short circuit. For example, Switch 2270 can be configured to turn off the function of Tag 2260 by short circuiting RFID Antenna 2240, a diode within Circuit 2250, a capacitor within Circuit 2250, a transistor within Circuit 2250, and/or a connection within Tag 2260.

[00182] In various embodiments, Switch 2270 functions by creating an open circuit. For example, Switch 2270 can be configured to create an open circuit between (or within) RFID Antenna 2240, Circuit 2250, and/or Tag 2260.

[00183] In some embodiments, Switchable RFID Device 2200 is configured to operate as a key and Switch 2270 is activated to turn on the functions of Tag 2260 by mechanical insertion of the key into a locking device. In these embodiments, the functions of Tag 2260 are typically off when the key is not inserted in the locking device. The locking device is configured to activate Switch 2270 using an electronic circuit, a mechanical force, or a magnetic field.

[00184] In alternative embodiments, an instance of Switch 2270 is included in Tag 2260 and/or Circuit 2250. Thus, Switchable RFID Tag 2230 may include a plurality of Switch 2270, one Switch 2270 in Circuit 2250 and one Switch 2270 in Tag 2260. As is described further herein, these instances of Switch 2270 may be configured to perform different functions.

[00185] FIG. 23 illustrates some of many possible locations for Switch 2270 within Switchable RFID Device 2200 where Switch 2270 creates an open circuit. FIG. 24 illustrates some of man possible locations for Switch 2270 within Switchable RFID Device 2200 wherein Switch 2270 creates a short circuit. The embodiments illustrated by FIGs. 23 and 24 include a Transistor 2310, a Diode 2320, and a Capacitor 2330. Possible positions for Switch 2270 are indicated by an "X."

[00186] In some embodiments, Switch 2270 is configured to partially limit the functionality of Tag 2260. Thus, Tag 2260 may be configured to respond with data indicating a first state when Switch 2270 is on and to respond with data indicating a second state when Switch 2270 is off. For example, Switch 2270 can be connected to logic circuits of Tag 2260 in such a way that Tag 2260 will transmit a limited amount of data when Switch 2270 is off and a less limited amount of data when Switch 2270 is on. For example, Tag 2260 may be configured to respond with data indicating the name of a person when Switch 2270 is off and to respond with the data including the name, an address, an account number and a telephone number when Switch 2270 is on. When Switch 2270 is connected to a circuit within Tag 2260, Switch 2270 (or a plurality thereof) is optionally configured to separately control detection of and readability of Tag

2260. Detection occurs when Tag 2260 sends any response signal, while readability is a function of the data that may be included in the contents of the response signal.

[00187] FIGs. 25A and 25B illustrate one embodiment of Switchable RFID Device 2200 in which Switch 2270 is a sliding switch disposed along an Edge 2520 of Switchable RFID Device 2200. FIG. 25A illustrates an OFF Position wherein an Electrical Connector 2510 between Circuit 2250 and Tag 2260 is in an open circuit state. In this state, Tag 2260 is not normally detectable or readable. FIG. 25B illustrates an ON position wherein Switch 2270 completes an electrical connection between Circuit 2250 and Tag 2260. In this position, Tag 2260 is detectable and readable. In this embodiment, Switch 2270 is configured to be moved between the on position and the off position, for example using a finger. In the on position, Switch 2270 optionally extends from Edge 2520 of Switchable RFID Device 2200. In the off position, Switch 2270 is optionally approximately flush with Edge 2520. Some embodiments of the invention include a switch configured to be approximately flush with an edge of a financial card (e.g., credit card or debit card) in at least one position. Some embodiments of the invention include a switch configured to be below an edge of a financial card in at least one position. Switch 2270 may be bistable or astable. Other features illustrated in FIGs. 25A and 25B are optional.

[00188] FIGs. 26A and 26B illustrates a Membrane Switch, generally designated 2600, (and surrounding area) for use in a switchable RFID device such as Switchable RFID Device 2200. Membrane Switch 2600 is optionally an embodiment of Switch 2270. Membrane Switch 2600 is shown in the OFF and ON positions, in FIGs. 26A and 26B respectively. The use of a finger to operate Membrane Switch 2600 is optional, other devices may be used to activate the switch. By bringing electrical conductors on a Surface 2630 and a Surface 2625 together, a switchable RFID tag is controlled, activated or deactivated. Typically, Surface 2625 and Surface 2630 are coated with an electrical conductor, such as copper. In some embodiments, a Support Layer 2610 is disposed at a First Surface 2615 of Switchable RFID Device 2200 and a Flexible Membrane 2620 is disposed at a Second Surface 2635 of Switchable RFID Device 2200. Thus, the Flexible Membrane 2620 includes both Surface 2625 and an outer surface, e.g., Surface 2635 of Switchable RFID Device 2200. In some embodiments, Surface 2635 extends beyond

Membrane Switch 2600 to Surrounding Areas 2650. As such Flexible Membrane 2620 is essentially flush with a surface of Switchable RFID Device 2200. Flexible membrane 2620 and Support Layer 2610 are separated by a Spacer 2640. In some embodiments, Spacer 2640 extends beyond the immediate vicinity if Membrane Switch 2600 to Surrounding Areas 2650. Spacer 2640 optionally extends essentially throughout Switchable RFID Device 2200. As such, Surface 2635 can be essentially smooth, e.g. does not include raised portions near Membrane Switch 2600. Support Layer 2610 is typically stiffer than Flexible Membrane 2620.

[00189] In various embodiments, Membrane Switch 2600 is included in an identity device such as a passport, driver's license, immigration card, key card, financial card, ID card, or the like. For example, in some embodiments, Membrane Switch 2600 is included within a passport or other identity device having a clamshell configuration. In these embodiments, Flexible Membrane 2620 is optionally disposed toward an interior of the identity device when the identity device is closed. In this position, Flexible Membrane 2620 is protected from inadvertent contact and typically can only be pressed after the identity device is opened.

[00190] In various embodiments, Membrane Switch 2600 is included in a financial card (e.g., a credit card, debit card or the like). In some of these embodiments, Flexible membrane 2620 is essentially flush with Surrounding Areas 2650 of the financial card including Surface 2625, as illustrated in FIGs. 26A and 26B. In this position Membrane Switch 2600 does not substantially stick out from First Surface 2625 of the financial card and is, thus, protected by Surrounding Areas 2650 from inadvertent activation. In some embodiments, Membrane Switch 2600 is recessed below First Surface 2635.

[00191] FIG. 26C illustrates an embodiment of Membrane Switch 2600 further including a Spring 2655. Spring 2655 may be considered a switch activator. Spring has an activation height at which the spring center will spring into contact with the Support Layer 2610 this activation height is typically below First Surface 2635.

[00192] FIG. 26D illustrates a cross-sectional view of Membrane Switch 2600 disposed within Switchable RFID Tag 2230. Tag 2260 is at least partially disposed within Spacer 540 and/or Support Layer 2610. Spacer 2640 and/or Support Layer 2610 optionally include a cavity configured to receive Tag 2260. In some embodiments, Tag

2260 is deposited on Support Layer 2610 before Spacer 2640 is deposited on Support Layer 2640. In these embodiments, Support Layer 2640 is formed around Tag 2260. In some embodiments, Spacer 2640 is configured to hermetically seal Tag 2260 and/or Membrane Switch 2600.

[00193] In various embodiments, an Opening 2670 within Membrane Switch 2600 is less than or equal to 2.0 mm, 1.5 mm, 1.75 mm, 1.25 mm, 1.0 mm, 0.75 mm, or 0.5 mm think as measured from Surface 2625 to Surface 2630.

[00194] The membrane switch illustrated in FIGs. 26A and 26C is optionally disposed such that Flexible Membrane 2620 is approximately flush with, or recessed in, First Surface 2635 of an identity device such as a driver's license or credit card. As such, Spacer 2640 prevents the membrane switch from being activated when a force is applied to the entire first surface. For example, when the identity device is placed within a wallet and the wallet is compressed.

[00195] Spacer 2640 optionally extends essentially throughout an identity device. For example, where Switchable RFID Device 2200 is a credit card, Spacer 2640 may extend to the outer edges of the credit card. Flexible Membrane 2620 optionally includes a picture of a user and/or an indication of the location of Opening 2670 in Spacer 2640. In some embodiments, Flexible Membrane 2620 is transparent and Spacer 2640 includes a picture of a user or a credit card number. In some embodiments, Spacer 2640 includes a cavity configured to fit an integrated circuit, the integrated circuit configured to operate as part of Tag 2260 and optionally mounted on Support Layer 2640. In some embodiments, Support Layer 2640 includes conductive traces configured to connect Tag 2260 to an RFID Antenna 2240. In some embodiments, Spacer 2640 is generally rectangular in shape, (e.g., in the shape of a financial card).

[00196] FIG. 27 illustrates a top view of Membrane Switch 2600 of FIG. 26C, according to various embodiments of the invention. In these embodiments, the shape of the Opening 2670 is configured to prevent Spring 2655 from rotating. A wide variety of alternative shapes may be used in alternative embodiments.

[00197] FIG. 28 illustrates Switchable RFID Tag 2230 in an embodiment wherein Switchable RFID Device 2200 includes an Identity Document 2800 having a clamshell configuration (e.g., a passport). Switchable RFID Tag 2230 may be included in a Cover

2840, a Cover 2830, or an interior page (not shown) of Identity Document 2800. Identity Document 2800 optionally includes Shielding 2810. Flexible Membrane 2620 is typically disposed such that it is on the interior of Identity Document 2800 when Identity Document 2800 is closed. See U.S. Patent 7,719,425 issued May 18, 2010 for further details of Identity Document 2800, according to some embodiments.

[00198] FIG. 29 illustrates the manufacture of instances of Identity Document 2800. At one stage in the manufacturing process, Shielding 2810 is dispensed in the form of a strip. The strip is laid down over what will be several separate instances of Identity Document 2800 (after when the manufacturing is completed). A plurality of Switchable RFID Tag 2230 are deposited, creating a device including several Switchable RFID Tag 2230. The assembled material, including Shielding 2810 is optionally cut to separate the locations where the instances of Switchable RFID tag 2230 are deposited or to be deposited. As a result a plurality of Identity Document 2800 are produced. Pages are optionally added to the assembled material prior to cutting. See U.S. non-provisional patent application 11/350,309 filed February 7, 2006 for further details, according to some embodiments.

[00199] In the above and other embodiments, Switchable RFID Tag 2230 is optionally disposed such that the switch mechanism is accessed from the inside of Cover 2830 or Cover 2840, the inside being the sides that face each other when Identity Document 2800 is closed. This orientation is optionally configured to reduce the probability of inadvertently activating Switch 2270 when Identity Document 2800 is closed. For example, in these embodiments, Flexible membrane 2610 may be to the inside (of the closed Identity Document 2800) and Support Layer 2610 may be to the outside. Support Layer 2610 optionally includes a stiffener in the region near Opening 2670.

[00200] FIG. 30 illustrates an exploded view of an embodiment of Switchable RFID Device 2200 including a Driver's License, generally designated 3000. In this view, for clarity, Spacer 2640 is removed and Flexible Membrane 2620 is separated from Tag 2260, RFID Antenna 2240, Circuit 2250 and Support Layer 2610. A location of Membrane Switch 2600 is indicated by Markings 3020 visible at Flexible Membrane 2620. Surface 2635 is of uniform level across the face of Driver's License 3000. As such, Switchable RFID Device 2200 can smoothly be placed in a wallet and Membrane

Switch 2600 is protected from inadvertent activation by Spacer 2640. Membrane Switch 2600 is optionally disposed at least partially within RFID Antenna 2240. A similar embodiment of Switchable RFID Device 2200 may include a credit card or similar financial device.

[00201] FIG. 31 illustrates an embodiment of Switchable RFID Device 2200 including a plurality of Switches, designated 3110, 3120 and 3130. These embodiments of Switchable RFID Device 2200 may include an identity device, financial device, credit card, debit card, remote control, product label, communication device, or the like. Any of Switches 3110, 3120, and 3130 are optional. Switch 3130 is configured for turning Switchable RFID Device 2200 ON and OFF. For example, as illustrated, Switch 3130 may be disposed in a connection between RFID Antenna 2240 and a Power Circuit 3140. Power Circuit 3140 is an embodiment of Circuit 2250 configured to generate electrical power from a received signal to power Tag 2260.

[00202] Switch 3110 and Switch 3120 are configured to control processing logic within Tag 2260. For example, in some embodiments, Switch 3110 and Switch 3120 are configured to provide Boolean (true/false) values to a logic circuit within Tag 2260. Some embodiments include further switches (e.g., 3, 4, 6, 8, 10 or more) configured to control processing logic.

[00203] In various embodiments, the processing logic within Tag 2260 can be configured to perform a wide variety of functions responsive to Switch 3110, Switch 3120, and any additional switches present. For example, in some embodiments, the processing logic is configured such that when Switch 3110 is activated a transaction amount is approved and when Switch 3120 is activated the transaction amount is disapproved. Alternatively, Switch 3110 and Switch 3120 may be part of a set of switches used to enter a PIN (personal identification number), an encryption key, an amount, an authorization code, an RFID reader identification number, an identification number associated with Switchable RFID Device 2200, a selection of a mode of Tag 2260, text, numbers, and/or other data.

[00204] In some embodiments, data sent by Tag 2260 using RFID Antenna 2240 is responsive to Switch 3110 and/or Switch 3120. For example, in some embodiments, Tag 2260 will send a different identification number depending on whether Switch 3110 or

SAMSUNG EXHIBIT 1010, Page 332

Switch 3120 is activated. In some embodiments, Tag 2260 is configured to allow a transaction up to a certain value if neither Switch 3110 nor Switch 3120 is activated, and progressively higher values if Switch 3110 or Switch 3120 is activated. In some embodiments, Tag 2260 is configured to require that Switch 3110 and Switch 3120 be activated in a specific combination, order and/or with a specific temporal pattern in order to perform some operation, e.g., a financial transaction.

[00205] While the embodiment of Switchable RFID Device 2200 illustrated in FIG. 31 includes one instance of Tag 2260, as discussed elsewhere herein, Switchable RFID Device 2200 optionally includes more than one instance of Tag 2260. When more than one instance of Tag 2260 is present, a separate instance of Switch 3130 may be disposed between RFID Antenna 2240 (or Circuit 2250) and each instance of Tag 2260. In this configuration, the instances of Switch 3130 may be used to select which instance of Tag 2260 to activate. Switch 3110 and/or Switch 3120 may, likewise, be configured to select, activate or control different instances of Tag 2260.

[00206] In some embodiments, Switchable RFID Device 2200 includes a Memory 3150. Memory 3150 is optionally programmable. For example, in some embodiments, Memory 3150 is programmable using data entered through instances of Switch 3110 and Switch 3120. In some embodiments, Memory 3150 is changed from a write state to a read only state, using Switch 3110. In various embodiments, Memory 3150 is configured to store data to be broadcast, encryption information, data keys, values to be used in conjunction with data entered suing Switch 3110, data for logic processing, identifying data, account data, mode data characterizing a mode of Switchable RFID Tag 2230, or the like. Memory 3150 can be volatile or non-volatile, FLASH, SDRAM, ROM, DDRAM, DRAM, or the like. Some embodiments of the invention include an automated device configured to actuate Switch 2270 in order to place Switchable RFID Tag 2230 in a programmable mode.

[00207] FIG. 32 illustrates various embodiments of Tag 2260 configured for use in embodiments of Switchable RFID Device 2200 including a plurality of switches. In the illustrated embodiments, Tag 2260 includes a First Logic Input 3210 and an optional Second Logic Input 3220, configured to be coupled to Switch 3110 and Switch 3120, respectively. First Logic Input 3210 and Second Logic Input 3220 are each configured to

SAMSUNG EXHIBIT 1010, Page 333

be responsive to a different switch. First Logic Input 3210 and Second Logic Input 3220 are configured to control the function of Tag 2260.

[00208] For example, in some embodiments, Tag 2260 is configured to output different data via a Data Input/Output 3240 depending on the state of Switch 3110 as determined by the First Logic Input 3210. Tag 2260 is optionally configured to output different data depending on whether a switch coupled to First Logic Input 3210 or a switch coupled to Second Logic Input 3220 is activated. In some embodiments, Tag 2260 is configured to send a signal via Antenna 2240 in response to a signal received and/or energy received via Antenna 2240. The sent signal is responsive to the states of Switches 3610-3612. For example, in some embodiments, Tag 2260 is configured to respond with a specific signal only when Switches 3610-3612 are activated in a specific order, combination, or temporal pattern. In some embodiments, Tag 2260 is configured to receive power via Antenna 2240, examine a state of Switches 3610-3612, and to send data via Antenna 2240 responsive to the examined state.

[00209] In some embodiments, the switches illustrated in FIG. 32 are membrane switches. In some embodiments, the switches illustrated in FIG. 32 are irreversible switches.

[00210] FIG. 33 illustrates an instance of Tag 2260, according to various embodiments of the invention. These embodiments include a plurality (e.g., 2, 3, 4, 8, 10, 12 or more) of switch inputs, such as First Logic Input 3210, Second Logic Input 3220 and Third Logic Input 3330. First Logic Input 3210, Second Logic Input 3220 and Third Logic Input 3330 are configured to receive inputs from Switch 3110, Switch 3120, Switch 3130, or the like, respectively. The state of connected switches (Switch 3110, Switch 3120, etc.) is monitored by an optional Switch State Monitor 3340 and a Processing Logic 3350. Switch State Monitor 3340 is optionally a multiplexer, latch, logic circuit, or the like.

[00211] In some embodiments, Processing Logic 3350 is configured to process data received through a Data Input From Antenna 3360, to receive power from a Power Input From Antenna 3230, and to generate data for output through a Data Output to Antenna 3370 responsive to the states of Switch 3110, Switch 3130, etc. The generated data is

optionally further responsive to data stored in Memory 3150 and/or data received from Data Input from Antenna 3360.

[00212] The data received from Memory 3150 can include codes required for Processing Logic 3350 to generate specific data for communication through Data Output to Antenna 3370. For example, in some embodiments, Tag 2260 is configured to output an RF signal only if data in Memory 3150 matches a state of Switches 3110 and 3120. In some embodiments, the state of switches is used to determine which of several different alternative RF signals to transmit. For example, if Switch 3110 is activated then a first signal is transmitted, if Switch 3120 is activated then a second signal is transmitted, and if no switches are depressed than no signal is transmitted or an third signal is transmitted. The first and second signals are optionally associated with different financial accounts and/or different functions.

[00213] Some embodiments of the invention include a multiswitch credit card including one or more instances of Tag 2260. This multiswitch credit card optionally is configured to be associated with more than one financial account and switches may be used to indicate which of the more than one financial account should be used for a transaction. In one example, the multiswitch credit card includes an instance of Tag 2260 configured for engaging in a financial transaction responsive to Switch 3110 and also configured to operate an electronic lock responsive to Switch 3120. Multiswitch credit card: Includes one or more switches; Includes RFID device- optionally passive; Single switch can be used to tum on and off RFID; Multiple switches can be used to enter an access code, such as PIN or password; the PIN or password may be encoded in an order of switch state change or a temporal relationship between switch state change, e.g., a temporal pattern; Multiple switches can be used to enter an ID number of an RFID reader. Multiple switches may be embodied in telephone device, such as a cellular phone; Multiple switches may be used to enter an access code based on combinations of switches as well as single switch activation. Single switch activation optionally includes. use of a temporal pattern of switch to generate a code. Switches could be used to indicate amount approval. Switches could be used to select an account. For example, activating a first switch may result in a transaction being debited from a first account and activating a second switch may result in a transaction being debited from a second account.

[00214] Cellular phone: Cellular phone configured to use two or more communication modes: one mode for cellular operation and one mode, e.g., RFID, for short range financial transactions or lock operation. These modes may use different frequency ranges. Keys (switches) within cellular phone turn on and off short-range transmissions within the short range mode. Keys within cellular phone configured to enter access code for use in short range mode. Short range mode is optionally passive RFID. For example, the presence of an RFID tag, within the cellular phone, may allow operation of a lock. The cellular phone is optionally configured to receive a plurality of RFID tags. These RFID tags are optionally responsive to switches (e.g., keys) on the cellular phone.

[00215] Some embodiments of the invention optionally include programming of Tag 2260 to make associations with the one or more financial account. This programming can include entering data within Memory 3150. Alternatively, Tag 2260 is configured to include a plurality of exchangeable Memory 3150. In these embodiments, Tag 2260 is programmed to operate with different financial accounts and/or functions by inserting different instances of Memory 3150 within Switchable RFID Tag 2230. The multiswitch credit card is, thus, optionally a multi account credit card.

[00216] Some embodiments of Switchable RFID Device 2200 are configured to include a plurality of Tag 2260. Each member of the plurality of Tag 2260 may be responsive to one or more switches. In some embodiments, Switchable RFID Device 2200 is configured to receive one or more replaceable instances of Tag 2260. In these embodiments, Switchable RFID Device 2200 may be programmed by replacing an instance of Tag 2260. Multiple instances of Tag 2260 optionally share one instance of RFID Antenna 2240 and/or one instance of Memory 3150.

[00217] FIG. 34 illustrates a method according to various embodiments of the invention. In these embodiments, power is received by Tag 2260 through an RF or inductive signal in a Receive Power Step 3410. The RF signal optionally includes data received in a Receive Data Step 3420. The state of one or more of Switches 3110, Switch 3120, etc. is then determined in a Determine Switch State 3430 Step. This state is used to determine an RF response, of any, in a Determine Response Step 3440. The RF response is then sent in a Send Response Step 3450.

[00218] FIG. 35 illustrates various embodiments of the invention in which Switchable RFID Device 2200 is configured as a RF Powered Remote 3500 configured to control

external devices. This RF Powered Remote 3500 optionally does not require an internal power source (e.g., is powered wirelessly). Power is received from an RF (radio frequency) signal via RFID Antenna 2240 and used to send a return signal, typically through the same instance of RFID Antenna 2240. RF Powered Remote 3500 uses one or more Switchable RFID Tag 2230 to activate and deactivate or modify the return signal. The one or more Switchable RFID Tag 2230 optionally share RFID Antenna 2240, power circuits, and/or processing logic. RF Powered Remote 3500 is typically a multifunction remote control.

[00219] RF Powered Remote 3500 is optionally used as part of a locking mechanism, such as in a vehicle lock or door lock. RF Powered Remote 3500 is optionally configured to control electronic equipment, such as a computing device, a video recording device, projector, a game, a stereo, or a television. RF Powered Remote 3500 is optionally configured to control a garage door opener.

[00220] As illustrated in FIG. 35, a Transmitter 3510 is configured to send an RF signal to provide power to RF Powered Remote 3500. This RF signal is received by RF Powered Remote 3500. When a switch (e.g. a First Switch 3520 or a Second Switch 3530), included in RF Powered Remote 3500, is in a first position the received power is used to send a return signal from RF Powered Remote 3500 to the device being controlled, e.g. a Controlled Device 3540. Transmitter 3510 is optionally included in Controlled Device 3540. When First Switch 3520 and/or Second Switch 3530 is in a second position the received power is not used to send the return signal from the remote, or is used to send a different return signal. The return signal may include audio, RF, infrared light, visible light, or the like. First Switch 3520 and Second Switch 3530 are optionally embodiments of Switch 3110, Switch 3120, or Switch 3130. In various embodiments, RF Powered Remote 3500 includes 1, 2, 3, 4 or more switches, such as First Switch 3520 and Second Switch 3530. Typically, different switches are configured to control different functions of Controlled Device 3540.

[00221] In some embodiments, First Switch 3520 and/or Second Switch 3530 are configured to control the collection of power from the RF signal. In some embodiments, First Switch 3520 and/or Second Switch 3530 are configured to prevent the power from flowing through an integrated circuit within the RF Powered Remote 3500. In some

embodiments, the First Switch 3520 and/or Second Switch 3530 are configured to decouple an instance of RFID Antenna 2240 within RF Powered Remote 3500. In some embodiments, the First Switch 3520 and/or Second Switch 3530 are configured to prevent data transmission from RF Powered Remote 3500. In some embodiments, First Switch 3520 and/or Second Switch 3530 are configured to control logic within an instance of Tag 2260 within RF Powered Remote 3500. In various embodiments, First Switch 3520 and/or Second Switch 3530 are normally on or normally off. In some embodiments, more than one switch is configured to control logic within the same integrated circuit.

[00222] The embodiments of RF Powered Remote 3500 illustrated in FIG. 14 include a Power Collection Circuit 3550 configured to convert the received RF signal to electrical power of the operation of one or more Tag 2260. RF Powered Remote 3500 is configured to power an integrated circuit, e.g., Tag 2260, and send a return signal using the electrical power produced by Power Collection Circuit 3550. The RF Powered Remote optionally receives all of its electrical power from the Power Collection Circuit 3550.

[00223] Depending on the state of First Switch 3520 and/or Switch 3530, Tag 2260 may cause the return signal to be transmitted using a Return Signal Generator 3560. Return Signal Generator 3560 is optionally included in Tag 2260. Return Signal Generator 3560 is optionally shared by a plurality of Tag 2260 within RF Powered Remote 3500. In some embodiments, Return Signal Generator 3560 includes an instance of RFID Antenna 2240.

[00224] First Switch 3520 and Second Switch 3530 each control Tag 2260, such that the return signal is responsive to the states of these, and optionally further, switches. For example, in some embodiments, if First Switch 3520 is on, then Tag 2260 will include a first data in the return signal, and if Second Switch 3530 is on, then Tag 2260 will include a second (typically different) data in the return signal.

[00225] The RF Transmitter 3510 and Controlled Device 3540 are optionally separate. For example, the RF transmitter may be included in an automobile and the controlled device may be a garage door.

[00226] In some embodiments, First Switch 3520 is activated by insertion of RF Powered Remote 3500 in part of a locking system.

[00227] In some embodiments, First Switch 3520 is coupled to a button configured for turning the volume of an electronic device up and/or Second Switch 3530 is coupled to a different button configured for changing a channel.

[00228] In some embodiments, RF Powered Remote 3500 is configured to unlock a car.

[00229] In various embodiments, RF Powered Remote 3500 includes a wireless keypad, a wireless computer mouse, a wireless keyboard, a wireless microphone, a key, a telephone, an identity document, or the like.

[00230] In some embodiments, RF Powered Remote 3500 is included in a hermetically sealed and/or waterproof housing. Because the RF powered remote is remotely powered, there is no necessity for a battery compartment or power plug.

[00231] First Switch 3520 and Second Switch 3530 may include a push-button switch, a membrane switch, a sliding switch, a magnetic switch, or any of the many other switches known in the art to make and break electrical connections. First Switch 3520 is optionally part of a roller, wheel or dial that makes and breaks an electrical connection as it is turned. First Switch 3520 and Second Switch 3530 are optionally embodiments of Switch 2270.

[00232] In some embodiments, a single instance of RF Transmitter 3510 is configured to power a plurality of Tag 2260. Each of this plurality of Tag 2260 is optionally configured to control a separate electronic device or operate different functions in a single electronic device. The plurality Tags 2260 optionally included in the same RF Powered Remote 3500.

[00233] In some illustrative embodiments, an instance of RF Transmitter 3510 is disposed within a vehicle dashboard and a plurality of Tag 2260 are disposed within a steering wheel of the vehicle or rear view mirror. One of the plurality Tag 2260 is configured to control an audio system and another of the plurality of switchable RFID tags is configured to control a climate system (e.g., air conditioner or heating). In some embodiments, the wireless response signals generated by both of these Tag 2260 is received by a RF receiver and communicated to a circuit that then controls the separate

electronic devices. In alternative embodiments, each of the separate electronic devices (e.g., audio system and climate system) includes a separate RF receiver configured to receive the response signals.

[00234] FIG. 36 illustrates an embodiment of Switchable RFID Device 2200 including a Multiswitch Credit Card 3600, according to various embodiments of the invention. Multiswitch Credit Card 3600 includes two or more switches, such as Switch 3610, Switch 3611, and optional Switch 3612. Switches 3610, 3611 and 3612 are optionally embodiments of Switch 3110 and Switch 3120. Multiswitch Credit Card 3600 further includes one or more instances of Tag 2260, an optional instance of Circuit 2250 configured to generate power for used by Tag 2260, and RFID Antenna 2240. In embodiments without Circuit 2250, Multiswitch Credit Card 3600 includes its own power source (not shown).

[00235] Switches 3610-3612 are each configured to make or break an electrical connection, the state of which can be determined by the resistance of electric current flow or the presence of a current or voltage. In some embodiments, Switches 3610-3612 are membrane switches, such as Membrane Switch 2600. In various embodiments, Multiswitch Credit Card 3600 including Switches 3610-3612 is less than 4, 3, 2, 1.5, 1, or 0.5 mm thick. In various embodiments, Switches 3610-3612 are essentially flush with a front surface of Multiswitch Credit Card 3600.

[00236] In some embodiments, Circuit 2250 is configured to generate electrical power from the RF signal received via RFID Antenna 2240 for use by one or more instances of Tag 2260. In some embodiments, Circuit 2250 and/or RFID Antenna 2240 are shared by several instances of Tag 2260 within Multiswitch Credit Card 3600. In some embodiments, Multiswitch Credit Card 3600 is configured not to transmit an RF signal unless at least one of Switches 3610-3612 is activated. In some embodiments, Switches 3610-3612 are configured for entering an access code, such as PIN or password. The access code is optionally encoded by an order in which the states of switches are changed, by a switch combination, and/or by a temporal relationship between changes in switch state, e.g., a temporal pattern.

[00237] In some embodiments, Switches 3610-3612 are configured for approving the amount of a financial transaction. In some embodiments, Switches 3610-3612 are

configured for selecting from among a plurality of financial accounts. For example, activating Switch 3610 may result in a transaction being debited from a checking account, activating Switch 3611 may result in a transaction being applied a first charge account, and activating Switch 3612 may result in a transaction being applied to a second charge account.

[00238] In some embodiments, Multiswitch Credit Card 3600 (or other embodiments of Switchable RFID Device 2200) includes encryption logic configured to operate in response to the activation of switches. For example, the encryption logic may be configured to use data received via switches as an encryption or decryption key. The encryption logic may be configured to encrypt data received via switches prior to transmission of this data. In some embodiments, Switchable RFID Tag 2200 is configured to make use of rolling codes for security purposes. In these embodiments, synchronization of the codes is optionally be coordinated by a central server configured to communicate with point of sale stations. In some embodiments, a switch is activated using a biometric sensor. The features described herein with respect to various embodiments of Switchable RFID Device 2200, such as Multiswitch Credit Card 3600, may be included in other types of identity devices.

[00239] In various embodiments of the invention, an identity device includes both one or more electrical contact configured to make physical electrical contact with a reader and a RFID tag configured to communicate wirelessly with a reader. The physical contact is optionally used to convey communication that is different from the wireless communication. For example, the physical connection based communication may include programming of a circuit within the RFID tag (e.g., programming account number), while the wireless communication may be more limited than the physical connection based programming, (e.g., the wireless communication may be limited to reading the programmed account number). In another example, the wireless communication may be configured for a limited set of transaction types (e.g., those less than $50, or deposits), while the physical communication is configured for additional transaction types (e.g., larger value withdrawals). Further, the physical communication may be used for downloading transaction logs or other data stored on the ID card. Transaction logs are optionally stored using power received through RFID Antenna 2240.

[00240] In various embodiments, an identity device includes a plurality of switches and is configured to engage in a transaction or allow access (to an account, data, or a physical location) responsive to whether proper members of the plurality of switches are pressed. For example, in one embodiment the ID card includes 10 switches configured for a user to enter a PIN (personal identification number) or password. Only when the proper data is entered using the plurality of switches will the ID card participate in certain functions, such as an electronic payment or opening of a lock. As described further herein, different numbers of switches are possible.

[00241] In various embodiments, an identity device includes logic configured to process data entered using a plurality of switches. This logic may, for example, prevent the identity device from transmitting an RF signal unless the entered data matches previously stored data, for example, if an entered PIN matches a stored access code. The logic may be responsive to the order of switches activated, combinations of switch activation (e.g., which switches are activated at the same time), or which of the plurality of switches are activated. Timing may be achieved through the use of appropriate RC (resister-capacitor) circuits or a clock signal.

[00242] Various embodiments of the invention include a modified version of Basic Access Control. In these embodiments, the logic is configured to prevent the identity device from transmitting certain data unless the data entered using switches on the identity device matches an ID number of a RFID reader making a request. The logic may be configured to implement Basic Access Control, such as that used in electronic U.S. passports, but unlike the system used in current passports, the data entered is an ID of the reader and the data is entered at the passport (or other identity device) rather than at the reader.

[00243] In various embodiments, the identity device includes a plurality of switches configured for a user to enter data associated with a reader. For example, in some embodiments, the switches are configured to receive an ID number of a point of sale (POS) device. Logic within the identity device may then use this ID number to assure that a transaction is communicated to the correct POS device. For example, if several vending devices are positioned adjacent to each other, the ID number of one of the vending devices may be entered in the identity device using the plurality of switches and

SAMSUNG EXHIBIT 1010, Page 342

the ID card may then be enabled to engage in a transaction with that particular vending device but not the other nearby vending devices.

[00244] Passwords, PINs, or the like received by the identity device through the plurality of switches are optionally stored in volatile memory within the identity device. When the identity device ceases to receive energy through an RF signal the data stored in this volatile memory is discarded (lost). In some embodiments, this data is stored in non-volatile memory and thus retained between RF transmissions.

[00245] In some embodiments, the identity device is configured to store an account balance in static memory. Logic within the identity device is optionally configured such that the account balance can only be increased using a physical connection, while the account balance can be debited using a wireless connection. Alternatively, logic within the identity device is optionally configured such that the account balance can only be debited using a physical connection.

[00246] Some embodiments of the invention include methods of purchasing using a switchable RFID. The identity device is placed within the reading range of a wireless POS device. One of a plurality of switches within identity device is activated such that an RFID tag will respond to an RF signal from the POS device. The RFID tag responses to the RF signal from the POS by energizing itself using the RF signal and generating a response RF signal. The responsive RF signal includes an account number such as a checking or savings account number, a credit card number, identity number, or the like, responsive to the switch.

[00247] FIGs. 37A-37C illustrate positions of RFID Antenna 2240 within Multiswitch Credit Card 3600, according to various embodiments of the invention. As illustrated in FIG. 37A, in some embodiments, RFID Antenna 2240 is disposed such that Embossed Lettering or Numbering 3620 is inside of RFID Antenna 2240. In these embodiments, at least part of Switch 2270 (or a plurality thereof) is optionally disposed inside of RFID Antenna 2240. As illustrated in FIGs. 37B and 37C, in some embodiments, RFID Antenna 2240 is disposed primarily in the part of a credit card (e.g., the upper half) that does not include Embossed Lettering or Numbering 3620. In these embodiments, Switch 2270 (or a plurality thereof) may be disposed either inside and/or outside of RFID Antenna 2240. As illustrated in FIG. 37C, when Switch 2270 is disposed outside of

SAMSUNG EXHIBIT 1010, Page 343

RFID Antenna, Connections 3615 between Switch 2270 and Tag 2260 are optionally routed to avoid Embossed Lettering or Numbering 3620. In some embodiments, Spacer 2640 is comprised of a material that can be embossed to form raised lettering and numbering (e.g., a name and credit card number). In these embodiments, the manufacture of Embossed Lettering or Numbering 3620 can be made through Spacer 2640.

[00248] In some embodiments, of the invention, one or more instances of Switch 2270 are configured to control whether Tag 2260 (and/or associated memory) are in a programmable state or a non-programmable state. For example, when an instance of Switch 2270 is in a first state writing to non-volatile memory within Tag 2260 is allowed and when Switch 2270 is in a second state writing to the non-volatile memory is not allowed but reading of the non-volatile memory may be allowed. In some embodiments, Switch 2270 is initially in a state wherein the non-volatile memory can be written to and the switch is then irreversible changed to a state wherein the non-volatile memory can no longer be written to.

[00249] The irreversible change optionally includes breaking of a conductor. For example, in some embodiments, an RFID enabled identity device is configured such that an instance of Switch 2270 comprises a Conductor 3810 coupled to Tag 2260. As illustrated in FIG. 38, when Conductor 3810 is unbroken Tag 2260 is in a programmable state, e.g., non-volatile memory within Switchable RFID Tag 2230 can be written to. After programming this conductor is broken and Tag 2260 is thus irreversibly changed to a nonprogrammable state. Data already programmed within Switchable RFID Tag 2230 may be locked by the breaking of Conductor 3850. In one embodiment, Conductor 3810 is broken through the manufacture of Embossed Lettering or Numbering 3620. For example, embossing a credit card number into a credit card can break a conductor and thus lock the contents of non-volatile memory within the credit card. In alternative embodiments, an identity device includes a plurality of Conductor 3810 and members of this plurality are broken in order to program function of Tag 2260. Each member of the plurality of Conductor 3810 that is or is not broken represents one bit of logic programmed.

[00250] Some embodiments of the invention include a switchable RFID tag is configured to be remotely switched using an RF signal. In some embodiments, in an OFF state, the RFID tag will not transmit a response signal and thus is not remotely detectable using an RF signal. In an ON state, the RFID tag will transmit a response signal. The RFID tag is switched between the ON state and the OFF state through receipt of a specific command or commands, through an RF signal. In alternative embodiments, the RFID tag includes multiple ON states, optionally in combination with an OFF state.

[00251] FIG. 39 illustrates a remotely switchable RFID Tag 3900 including an Antenna 3910, a Power Electronics 3920 , and an Integrated Circuit 3930. RFID Tag 3900 is optionally an embodiment of other RFID tags disclosed herein. Likewise, Antenna 3910, Power Electronics 3920 and Integrated Circuit 3930 are optionally embodiments of other antennae, power electronics and integrated circuits disclosed herein. Antenna 3910 is configured to send and receive data encoded in an RF signal and also optionally configured to receive sufficient energy to power RFID Tag 3900.

[00252] Power Electronics 3920 are configured to receive energy through Antenna 3910 and to power Integrated Circuit 3930 using this received energy. Power Electronics 3920 typically include elements such as a diode, capacitor, transistor, or the like.

[00253] Integrated Circuit 3930 includes an Input 3935 configured to receive data from Antenna 3910 and power from Power Electronics 3920. Integrated Circuit 3930 further includes an Output 3940 configured to convey data to Antenna 3910 for transmission as an RF signal.

[00254] Integrated Circuit 3930 further includes an optional State Memory 3945 configured to store the current state of the RFID Tag, e.g., ON or OFF. In various embodiments, State Memory 3945 includes a memory location in a static random access memory, a magnetic memory, or the like. In these embodiments, the state stored within State Memory 3945 is preserved without a constant source of power. In some embodiments, State Memory 3945 includes memory configured to store data only while power is available. In this embodiment, the ON state is typically temporary and automatically reverts to the OFF state after power is no longer available.

[00255] Integrated Circuit 3930 further includes an optional Data Memory 3950 configured to store data received through Antenna 3910, and/or to be transmitted using

Antenna 3910. The data stored in Data Memory 3950 may include a serial number of RFID Tag 3900, identification data, biometric data, medical information, license information, or the like.

[00256] Integrated Circuit 3930 further includes a Key Memory 3955 configured to store a key required to change the state of the RFID Tag 3900 from ON to OFF, from OFF to ON, and/or between two ON states. Key Memory 3955 is typically static memory, and optionally read only memory or write-once memory. In other embodiments, the Key Memory 3955 is memory configured for temporary storage of data.

[00257] Integrated Circuit 3930 further includes Switch Logic 3960 configured to read the state stored in State Memory 3945 and, responsive to the read state, either transmit or not transmit an RF signal using Antenna 3910. The transmitted data optionally includes data stored in Data Memory 3950. In some embodiments, Switch Logic 3960 is configured to not transmit an RF signal unless the state read from State Memory 3945 indicates that the RFID Tag is in an ON state. In some embodiments, Switch Logic 3960 is configured to read the state stored in State Memory 3945 and, responsive to the read state, transmit one of a plurality of alternative data stored in Data Memory 3950. In some embodiments, Switch Logic 3960 is configured to read the state stored in State Memory 3945 and, responsive to the read state, transmit different amounts of data stored in Data Memory 3950.

[00258] In some embodiments, Switch Logic 3960 is configured to receive data through Antenna 3910, to read a key from Key Memory 3955, to compare the received data with the read key, and to change the state stored in State Memory 3945 responsive to this comparison. For example, in some embodiments, if the read key matches the received data, the state of the RFID Tag 3900 is set to ON, or changed from one ON state to another ON state. In some embodiments, Switch Logic 3960 includes logic configured to decrypt or apply a hash function to the received data prior to the comparison. The Switch Logic 3960 can include software, hardware, and/or firmware. In some embodiments, State Memory 3945 is configured to store a rolling code.

[00259] In some embodiments, Integrated Circuit 3930 is embodied in several devices. For example, the functionality of Integrated Circuit 3930 may be distributed among

several chips. In some embodiments, Key Memory 3955, Antenna 3910, Switch Logic 3960 and/or State Memory 3945 are configured to be shared by more than one instance of Integrated Circuit 3930. For Example, two or more instances of RFID Tag 3900 may be included in a single device and these two or more instances of RFID Tag 3900 may share a single instance of Key Memory 3955, Antenna 3910, Switch Logic 3960 and/or State Memory 3945.

[00260] In some embodiments, RFID Tag 3900 further includes a mechanical switch configured to control operation of RFID Tag 3900. This switch may include, for example, Switch 2270 (FIG. 22). For example, in one embodiment, Switch Logic 3960 is configured for turning ON and OFF operation of RFID Tag 3900, while Switch 2270 is configured to select between alternative ON states. In an alternative embodiment, Switch 2270 is configured for turning ON and OFF operation of RFID Tag 3900 and Switch Logic 3960 is configured for selecting between alternative ON states. In some embodiments, proper activation of both Switch 2270 and Switch Logic 3960 is required to turn RFID Tag 3900 to an ON state. Thus, in order for RFID Tag 3900 to transmit certain information, or to transmit at all, Switch 2270 must be activated by a person and Switch Logic 3960 must receive a proper key from an RF reader. This provides a dual layer of mechanical and key based security. In some embodiments, the switch must be activated and a proper key must be received in order for RFID Tag 3900 to transmit certain information. In some embodiments, use of Switch 2270 will activate RFID Tag 3900 in a first ON state and use of Switch Logic 3960 (through an RF signal) will activate RFID Tag 3900 in a second ON state. The second ON state optionally requires use of both Switch 2270 and Switch Logic 3960.

[00261] In some embodiments, Integrated Circuit 3930 also includes an independent Power Supply 3965 such as a battery or capattery.

[00262] In some embodiments, the switchable RFID Tag 3900 of FIG. 1 is included in an identification document such as a driver's license, green card, passport, or the like. In some embodiments, the Switchable RFID Tag 3900 is included in a wireless key configured to open a lock, to access data, to gain entry, or the like. In some embodiments, Switchable RFID Tag 3900 is included in a cellular telephone or another device configured to communicate using WiFi, WiMAX, or similar non-RFID standards.

[00263] FIG. 40 is a flowchart illustrating a method of changing a state of RFID Tag 3900. In an optional Receive Energy Step 4010, energy sufficient to power RFID Tag 3900 is received by Antenna 3910. Receive Energy Step 4010 is typically similar to Receive Power Step 3410. In a Receive Data Step 4020, data is received by Antenna 3910 in the form of an RF signal. In some embodiments, Receive Data Step 4020 requires that a mechanical switch be activated. In a Read Key Step 4030, a key is read from Key Memory 3955. Optionally, the data received in the Receive Data Step 4020 is decrypted or otherwise processed. In a Compare Step 4040, the read key is compared with the, optionally processed, data received in the Receive Data Step 4020.

[00264] In a Change State Step 4050, the state of RFID Tag 3900 is changed responsive to results of the comparison made in the Compare Step 4040. In some embodiments, if there is a match between the key and the data then the state of RFID Tag 3900 is set to ON. Setting the state ON optionally includes writing a value to State Memory 3945. In some embodiments, if there is no match between the key and the data then the state is set to OFF. In some embodiments, if there is a match between the key and the data, then the state is set to one of two or more possible ON states. In one of the two or more possible ON states, RFID Tag 3900 can transmit a response RF signal but the data that can be included in the response RF signal is restricted relative to another of the two or more possible ON states. For example, in one embodiment, in one ON state RFID tag 3900 is configured to include a name in the response RF signal, but another ON state RFID tag 3900 is configured to include the name and medical information in the response RF signal.

[00265] In some embodiments, RFID Tag 3900 is automatically returned to the OFF state from the ON state, in a Revert Step 4060. For example, in one embodiment the ON state remains only so long as there is charge on a capacitor. When this charge dissipates or is used, the RFID automatically returns to a default OFF state. The automatic switch back to the OFF state can be dependent on when power is no longer received from an RF signal, on the timing characteristics of an RC (resistor-capacitor) circuit, on Switch 2270, on an RF signal received, and/or the like.

[00266] FIG. 41 is a flowchart illustrating a method of operating the RFID Tag 3900 illustrated in FIG. 39. In an optional Receive Energy Step 4010 energy sufficient to

power the RFID is received by Antenna 3910. In a Read State Step 4120 the state of the RFID Tag is read from State Memory 2245. In a State? Step 4130 the read state is examined. If the read state is ON, then in a Send Response Step 4140 an RF response is sent from the RFID Tag 3900 using Antenna 3910. If the read state is OFF, then the RFID Tag 3900 is prevented from sending an RF response, in an Abort Response Step 4150. In some embodiments, that include more than two states, the read state can be something other than ON or OFF. If the read state is a state other than ON or OFF then a restricted RF response is sent in a Send Restricted Response Step 4160. The restricted response typically includes less or different data than would be included if the read state had been ON.

[00267] The steps shown in FIGs. 40 and 41 are optionally performed using Integrated Circuit 3930 of FIG. 39.

[00268] In some embodiments, first data in a transmission is configured to change the state of an RFID tag to ON. Further data in the transmission is then configured to elicit a responding transmission from the RFID tag. After the transmission is concluded the RFID tag automatically reverts to the OFF state. These embodiments optionally include non-volatile memory for storage of the state.

[00269] In some embodiments, data in a transmission is configured to change the state of an RFID tag to ON. The ON state persists until the RFID tag receives data configured to change the state of the RFID tag to OFF.

[00270] Several embodiments are specifically illustrated and/or described herein. However, it will be appreciated that modifications and variations are covered by the above teachings and within the scope of the appended claims without departing from the spirit and intended scope thereof. For example, an RFID key device may include more than one RFID tag and moving of shielding may be used to determine which RFID tag can communicate with readers. The RFID tags discussed herein may include active or passive contactless circuits configured to transmit identification information. For example, in some embodiments, Tag 2260 is an active rather than a passive RFID tag. Examples discussed herein in relation to credit cards can equally be applied to other types of financial card such as a debit card, or prepaid card. For example, in some embodiments, RFID Tag 3900 is configured to change the ON/OFF state in response to a

signal from a point of sale system indicating that an item has been sold. In these embodiments, RFID Tag 3900 is optionally configured to send different signals before and after a sale. A first of the different signals may be used to determine that the item has not yet been sold, and a second of the different signals may be used to determine that the item has been sold and/or may be returned. The features illustrated in FIGs. 39-41 are optionally included in embodiments illustrated by other figures of this application.

[00271] The embodiments discussed herein are illustrative of the present invention. As these embodiments of the present invention are described with reference to illustrations, various modifications or adaptations of the methods and or specific structures described may become apparent to those skilled in the art. All such modifications, adaptations, or variations that rely upon the teachings of the present invention, and through which these teachings have advanced the art, are considered to be within the spirit and scope of the present invention. Hence, these descriptions and drawings should not be considered in a limiting sense, as it is understood that the present invention is in no way limited to only the embodiments illustrated.

CLAIMS

What is claimed is:

1. A method of performing a financial transaction using a cellular telephone, the method comprising:

placing the cellular telephone within reading range of a wireless communication device, the cellular telephone being configured to communicate wirelessly using an inductive coupling and an RF antenna, wherein the communication (verb) is responsive to a circuit including an electronic switch configured to change a state of the circuit, the circuit being configured to communicate responsive to the state of the circuit;

activating the electronic switch within the cellular telephone to change the state of the circuit, activation of the electronic switch being responsive to a biometric sensor; and

communicating financial account information from the cellular telephone to the wireless communication device responsive to the state of the circuit to facilitate the financial transaction, the communication of the account information using the inductive coupling or the RF antenna.

2. The method of claim 1, wherein the cellular telephone includes the biometric sensor.

3. The method of claim 1, wherein the circuit is configured to facilitate the financial transaction responsive to the biometric sensor.

4. The method of claim 1, wherein the circuit is configured to approve the financial transaction responsive to the biometric sensor.

5. The method of claim 1, wherein the circuit is configured to communicate financial account information responsive to the biometric sensor.

6. The method of claim 1, wherein the circuit is changed from a first ON state to a second ON state, responsive to the electronic switch, and wherein the circuit includes a memory configured to store the first and second ON states.

7. The method of claim 1, wherein the circuit is changed from a first ON state to a second ON state, responsive to the electronic switch, and wherein different amounts of personal information are communicated via the inductive coupling or RF antenna in the first ON state relative to the second ON state.

SAMSUNG EXHIBIT 1010, Page 351

8. The method of claim 1, wherein the circuit is configured to store transaction logs.

9. The method of claim 1, wherein the circuit is configured for a user to select between a plurality of financial accounts for the financial transaction.

10. The method of claim 1, further comprising entering a personal identification number or a password to facilitate the financial transaction.

11. The method of claim 1, wherein the circuit is configured to communicate an account number via the inductive coupling or RF antenna to facilitate the financial transaction.

12. The method of claim 1, wherein the cellular telephone includes a user interface configured to enter a financial account number and includes memory configured to store the financial account number for use in the financial transaction.

13. The method of claim 1, wherein the cellular telephone is configured for a user to enter a personal identification number (PIN), communication of the financial account information via the inductive coupling or RF antenna being responsive to the personal identification number.

14. The method of claim 1, wherein the cellular telephone includes a memory configured to store an encryption key used to facilitate the financial transaction.

15. The method of claim 1, wherein the cellular telephone includes a memory configured to store a key required to change the state of the circuit to facilitate the financial transaction.

16. The method of claim 1, wherein the cellular telephone is configured for insertion of an electronic key, the electronic key including a personal identification number, a signal communicated via the inductive coupling or RF antenna to facilitate the financial transaction being responsive to entry of the personal identification number by a user.

17. The method of claim 1, wherein the cellular telephone is configured for insertion of an electronic key, the electronic key including an account identifier and the communication via the inductive coupling or RF antenna being responsive to the account identifier, the electronic key being configured to store a password or personal identification number.

18. The method of claim 1, wherein activating the electronic switch is responsive to data stored in memory of the cellular telephone and the data stored in memory includes biometric data.

19. A method of performing a financial transaction using a cellular telephone, the method comprising:

placing the cellular telephone within reading range of a wireless communication device, the cellular telephone being configured to communicate wirelessly using an RF antenna, wherein the RF antenna is responsive to a circuit including an electronic switch configured to change a state of the circuit, the circuit being configured to communicate via the RF antenna responsive to the state of the circuit;

activating the electronic switch within the cellular telephone to change the state of the circuit, activation of the electronic switch being responsive to entry of a personal identification number; and

communicating financial account information from the cellular telephone to the wireless communication device responsive to the state of the circuit to facilitate the financial transaction, the communication of the financial account information using the RF antenna.

20. The method of claim 19, wherein the communication of the financial account information is responsive to a biometric sensor included in the cellular telephone.

21. The method of claim 19, further comprising approving the financial transaction using a biometric sensor.

22. The method of claim 19, further comprising approving the financial transaction using a mechanical switch.

23. The method of claim 19, wherein the cellular telephone includes a user interface configured to enter a financial account number and includes memory configured to store the financial account number for use in the financial transaction.

24. The method of claim 19, wherein the circuit is configured for a user to select between a plurality of financial accounts for the financial transaction

25. The method of claim 19, wherein the circuit is changed from a first ON state to a second ON state, responsive to the electronic switch, and wherein different

amounts of personal information are communicated via the RF antenna in the first ON state relative to the second ON state.

26. The method of claim 19, wherein the circuit is configured to store transaction logs.

27. The method of claim 19, wherein the circuit is configured to communicate an account number via the RF antenna to facilitate the financial transaction.

28. The method of claim 19, wherein the cellular telephone is configured for insertion of a memory, the memory including account information and a personal identification number, and a signal communicated via the RF antenna to facilitate the financial transaction being responsive to the account information and the personal identification number.

29. The method of claim 19, wherein the cellular telephone is configured for insertion of an electronic key, the electronic key being configured to store a password, the communication via the RF antenna being responsive to the password.

30. The method of claim 19, wherein the cellular telephone is configured for insertion of an electronic key, the electronic key being configured to store a personal identification number, the communication via the RF antenna being responsive to the personal identification number.

ABSTRACT

Various switchable devices, e.g., cellular telephones, including inductive and/or RF antennas are disclosed. These switchable devices may include one or more switches and a biometric sensor. Some of these one or more switches are optionally wireless and/or manual. In various embodiments, the switchable devices include are included within cellular phones, security devices, identity devices, financial devices, remote controls, and the like. The switchable devices are optionally configured to perform financial transactions.

SAMSUNG EXHIBIT 1010, Page 355

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	SMC-83-C12C3
	Application Number	
Title of Invention	Methods of Using a Cellular Telephone	

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
	Steven	Michael	Colby	

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

City	Verdi	State/Province	NV	Country of Residence i	US

Mailing Address of Inventor:

Address 1	c/o Rimon Law PC
Address 2	420 West Main Street, Suite 101B
City	Boise
State/Province	ID
Postal Code	83702
Country i	US

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	43198		
Email Address	pv-patentdoc@rimonlaw.com	Add Email	Remove Email
Email Address	steven.colby@rimonlaw.com	Add Email	Remove Email

Application Information:

Title of the Invention	Methods of Using a Cellular Telephone		
Attorney Docket Number	SMC-83-C12C3	**Small Entity Status Claimed**	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	35	**Suggested Figure for Publication (if any)**	34

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	SMC-83-C12C3
	Application Number	
Title of Invention	Methods of Using a Cellular Telephone	

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

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	43198		

Domestic Benefit/National Stage Information:

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

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	17728412	2022-04-25
Prior Application Status	Patented		Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
17728412	Continuation of	17522697	2021-11-09	11347949	2022-05-31

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	SMC-83-C12C3
	Application Number	

Title of Invention	Methods of Using a Cellular Telephone

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
17522697	Continuation of	16186543	2018-11-11	11170185	2021-11-09
Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
16186543	Continuation in part of	15418726	2017-01-28	10503940	2019-12-10
Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
15418726	Continuation of	14660825	2015-03-17	9569777	2017-02-14
Prior Application Status	Abandoned				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)		
14660825	Continuation in part of	13481104	2012-05-25		
Prior Application Status	Abandoned				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)		
13481104	Continuation of	12777474	2010-05-11		
Prior Application Status	Abandoned				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)		
14660825	Continuation in part of	13084433	2011-04-11		
Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13084433	Continuation of	11458620	2006-07-19	7924156	2011-04-12
Prior Application Status	Abandoned				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)		
11458620	Continuation in part of	11382052	2006-05-07		
Prior Application Status	Abandoned				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)		
11458620	Continuation in part of	11382053	2006-05-07		
Prior Application Status	Abandoned				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)		
11458620	Continuation in part of	11382054	2006-05-08		
Prior Application Status	Abandoned				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)		
11458620	Continuation in part of	11382264	2006-05-08		
Prior Application Status	Abandoned				Remove

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	SMC-83-C12C3
	Application Number	
Title of Invention	Methods of Using a Cellular Telephone	

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
11458620	Continuation in part of	11382265	2006-05-08
Prior Application Status	Abandoned		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
11458620	Continuation in part of	11420721	2006-05-26
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
11458620	Claims benefit of provisional	60700884	2005-07-19
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
11458620	Claims benefit of provisional	60712308	2005-08-30
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
11458620	Claims benefit of provisional	60715641	2005-09-10
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
11458620	Claims benefit of provisional	60752933	2005-12-21
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
11458620	Claims benefit of provisional	60758751	2006-01-13
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
11458620	Claims benefit of provisional	60782068	2006-03-13
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
11458620	Claims benefit of provisional	60744154	2006-04-03
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
11458620	Claims benefit of provisional	60746636	2006-05-06
Prior Application Status	Abandoned		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
11458620	Continuation in part of	11382050	2006-05-07
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
11382050	Claims benefit of provisional	60678428	2005-05-06
Prior Application Status	Expired		Remove

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	SMC-83-C12C3
	Application Number	
Title of Invention	Methods of Using a Cellular Telephone	

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
11382050	Claims benefit of provisional	60685331	2005-05-27
Prior Application Status	Patented		Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14660825	Continuation in part of	14468110	2014-08-25	9495852	2016-11-15
Prior Application Status	Patented				Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14468110	Continuation of	12577209	2009-10-12	8816826	2014-08-26
Prior Application Status	Abandoned				Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
12577209	Continuation of	11468026	2006-08-29
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
11468026	Claims benefit of provisional	60746636	2006-05-06
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
11468026	Claims benefit of provisional	60744154	2006-04-03
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
11468026	Claims benefit of provisional	60782068	2006-03-13
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
11468026	Claims benefit of provisional	60758751	2006-01-13
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
11468026	Claims benefit of provisional	60752933	2005-12-21
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
11468026	Claims benefit of provisional	60715641	2005-09-10
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
11468026	Claims benefit of provisional	60712308	2005-08-30

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

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	SMC-83-C12C3
	Application Number	
Title of Invention	Methods of Using a Cellular Telephone	

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(d). 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(h)(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).

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.

Authorization to Permit Access:

☐ Authorization to Permit Access to the Instant Application by the Participating Offices

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	SMC-83-C12C3
	Application Number	
Title of Invention	Methods of Using a Cellular Telephone	

If 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 World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date o f filing this Authorization.

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. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

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	SMC-83-C12C3
	Application Number	
Title of Invention	Methods of Using a Cellular Telephone	

Mailing Address Information For Applicant:			
Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		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 subsitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

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. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:			
Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

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

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	SMC-83-C12C3
	Application Number	
Title of Invention	Methods of Using a Cellular Telephone	

Signature:

Remove

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Signature	/Steven M. Colby 50,250/			Date (YYYY-MM-DD)	2022-09-22
First Name	Steven	Last Name	Colby	Registration Number	50250

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

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 C o o p eration Treaty.

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

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

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

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

PTO/AIA/01 (06-12)
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 displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	Methods of Using a Cellular Telephone

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [x] The attached application, or
- [ ] United States application or PCT international application number _____

filed on _____.

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 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.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Steven Michael Colby Date (Optional) : Sept. 22, 2022

Signature: /Steven M. Colby 50,250/

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute 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.

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.

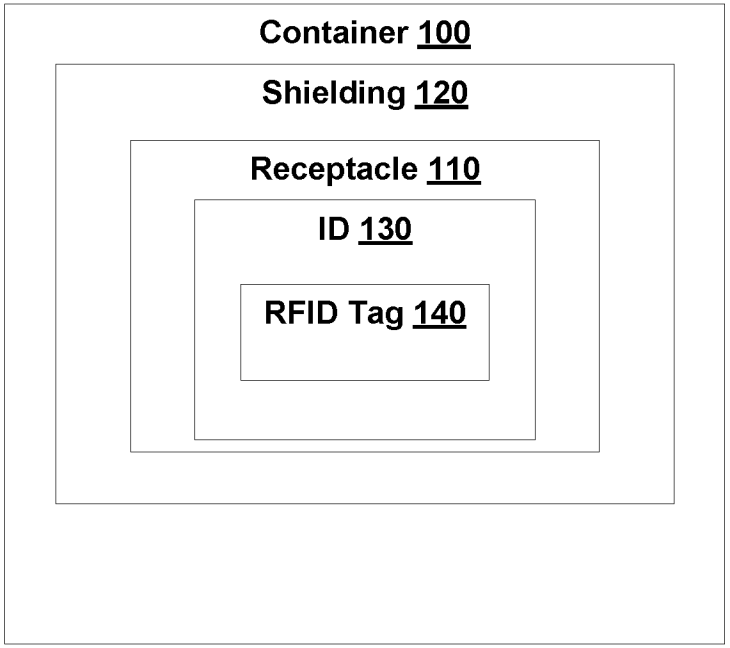

Container 100
Shielding 120
Receptacle 110
ID 130
RFID Tag 140

FIG. 1

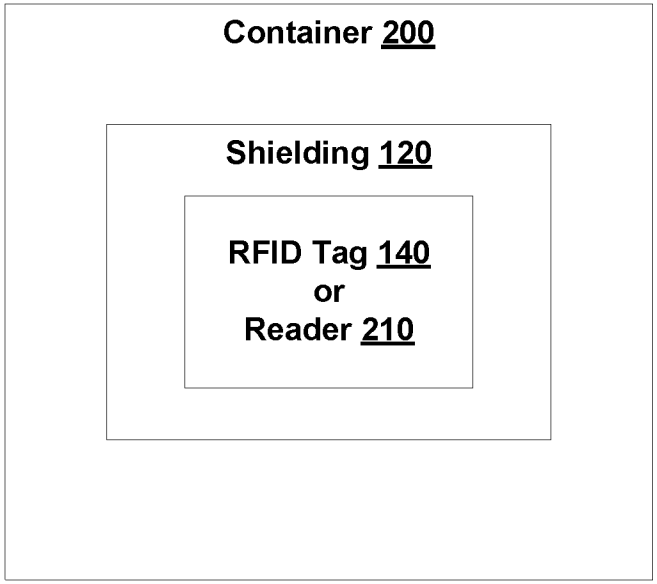

Container 200
Shielding 120
RFID Tag 140
or
Reader 210

FIG. 2

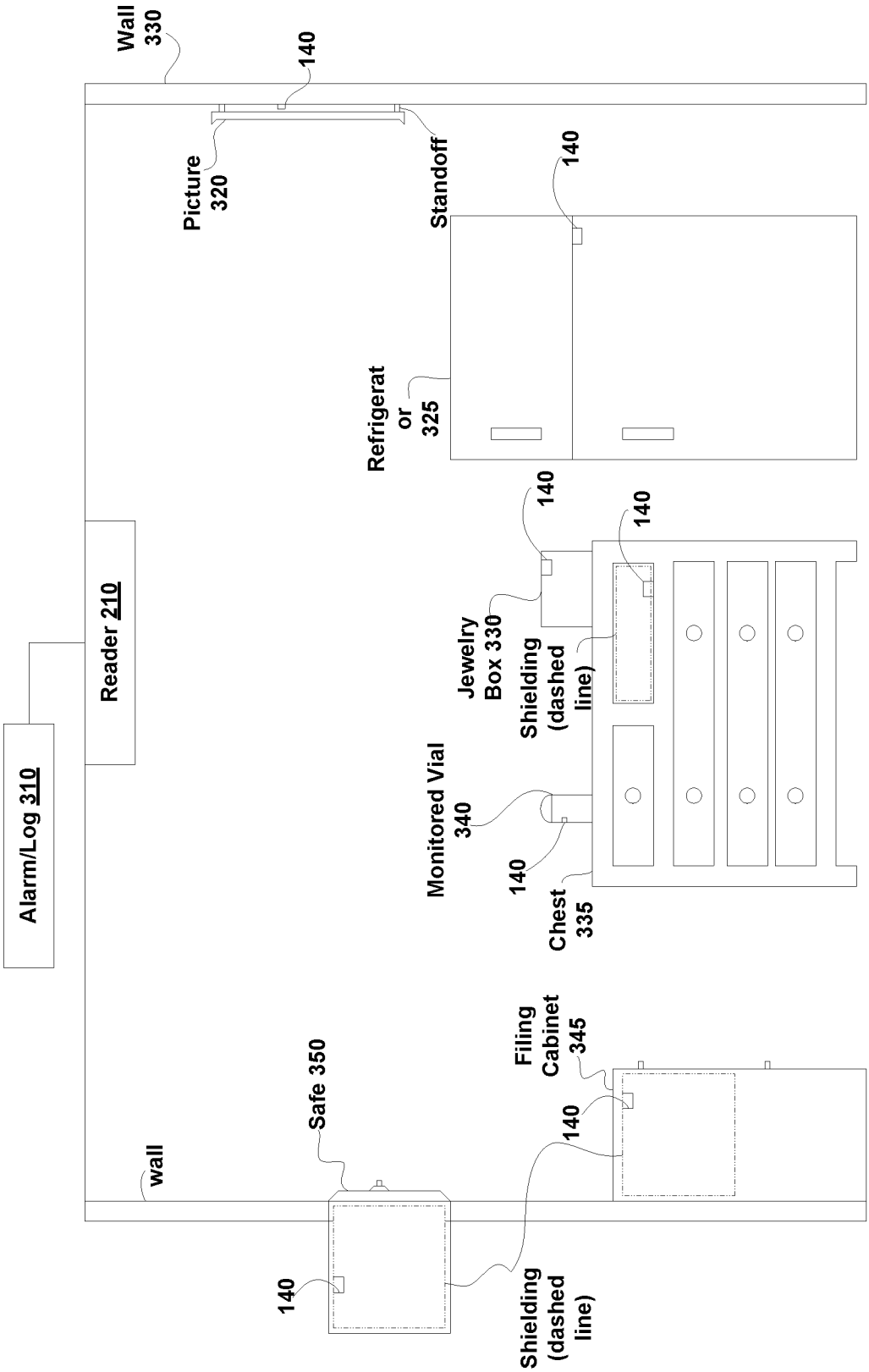

Alarm/Log 310
Reader 210
Wall 330
140
Picture 320
Standoff
140
Refrigerat or 325
140
140
Jewelry Box 330
Shielding (dashed line)
Monitored Vial 340
140
Chest 335
Filing Cabinet 345
Safe 350
140
wall
140
Shielding (dashed line)

FIG. 3

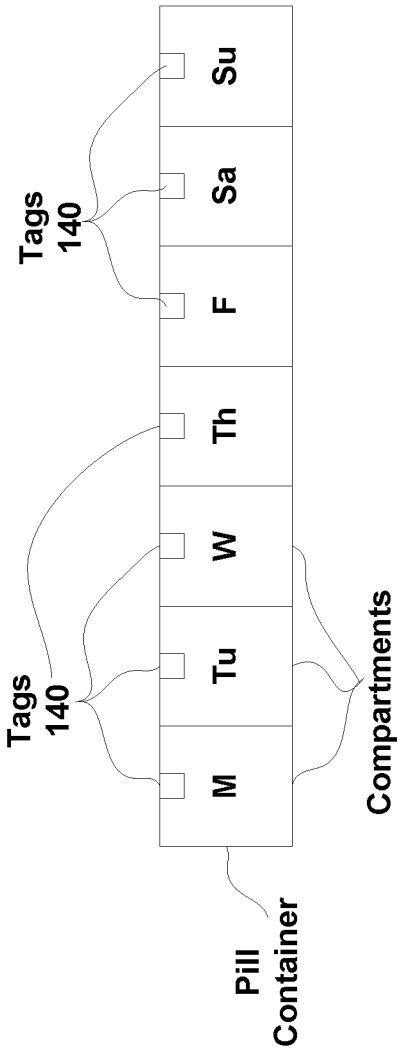

Tags
140
Tags
140
M
Tu
W
Th
F
Sa
Su
Compartments
510
Pill
Container

FIG. 5

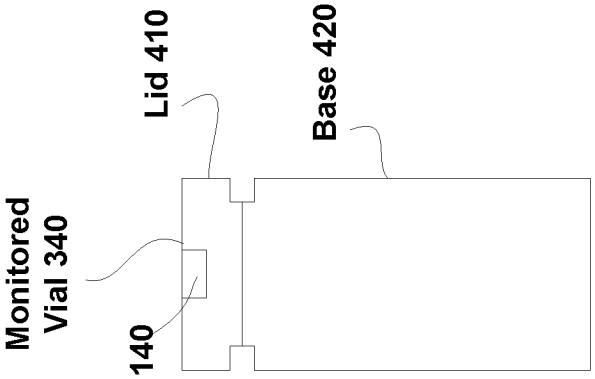

Monitored
Vial 340
140
Lid 410
Base 420

FIG. 4

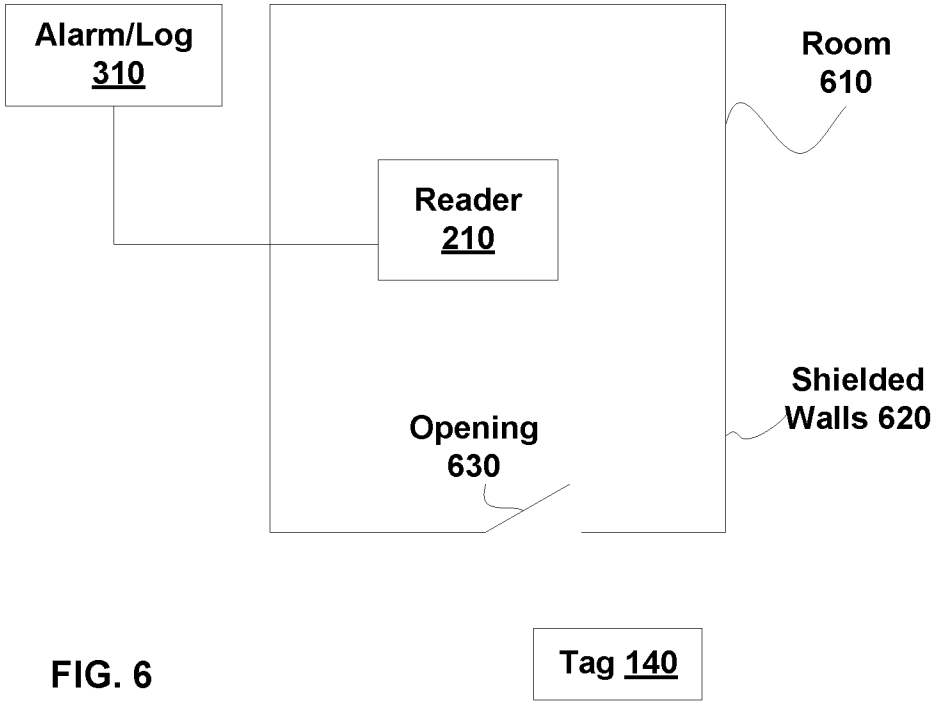

Alarm/Log
310
Room
610
Reader
210
Shielded
Walls 620
Opening
630
Tag 140

FIG. 6

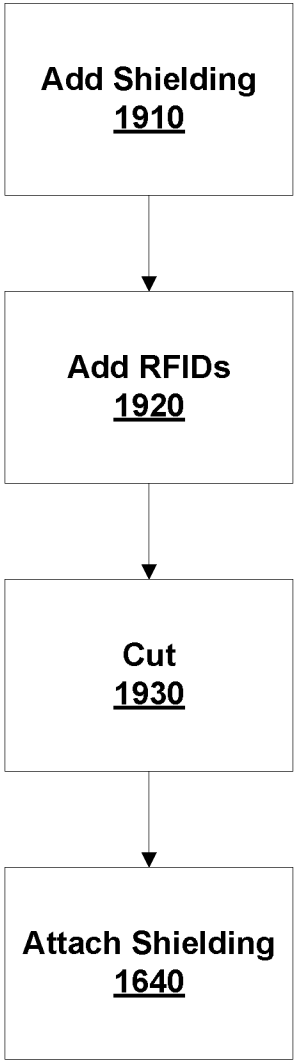

Add Shielding
1910
Add RFIDs
1920
Cut
1930
Attach Shielding
1640

FIG. 19

Reader/Lock
Control 710
Lock 740
Barrier
730
Animal/
Person 720
Tag 140

FIG. 7

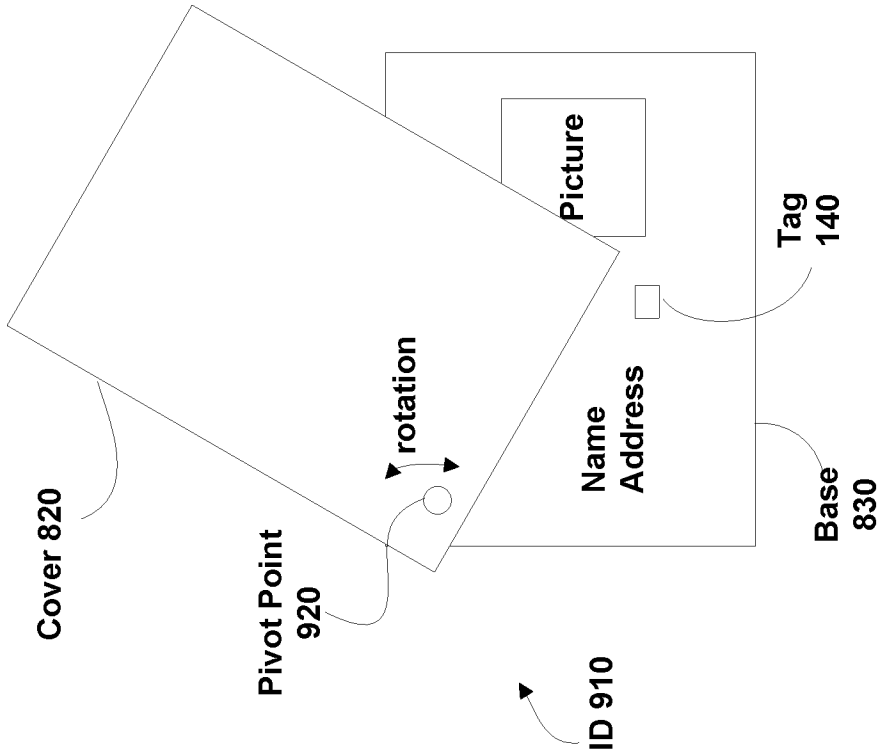

Cover 820
Pivot Point
920
rotation
Picture
Name
Address
Tag
140
Base
830
ID 910

FIG. 9

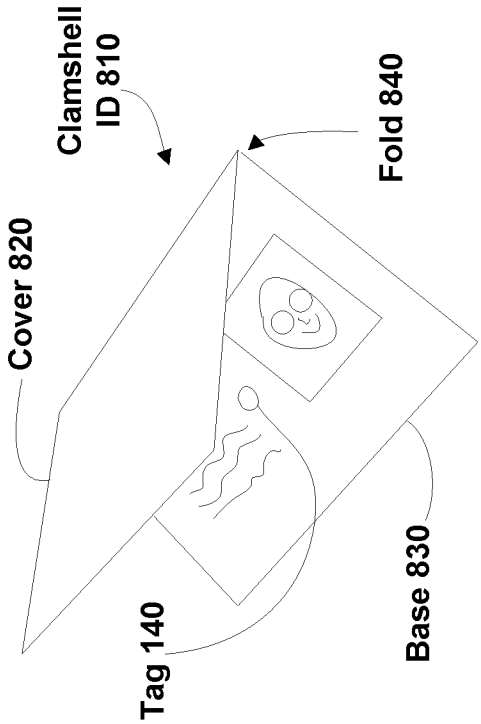

Clamshell
ID 810
Cover 820
Fold 840
Tag 140
Base 830

FIG. 8

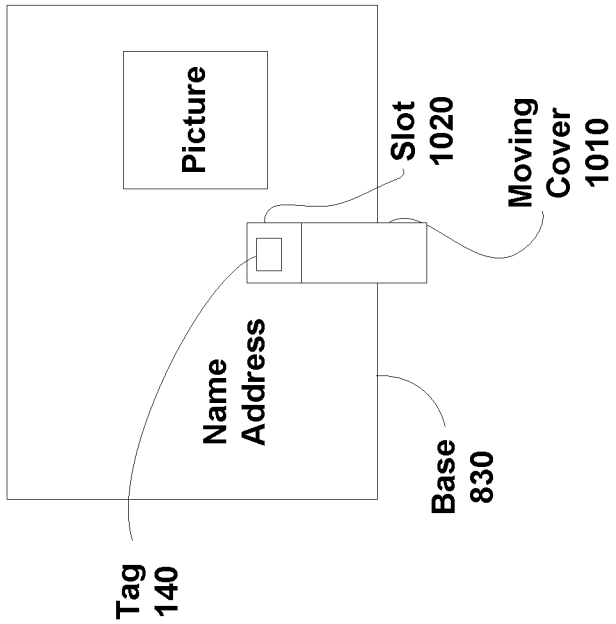


FIG.
10B

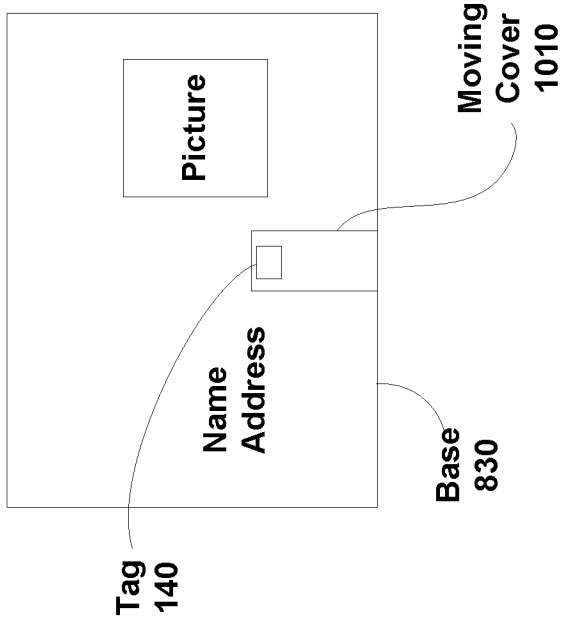


FIG.
10A

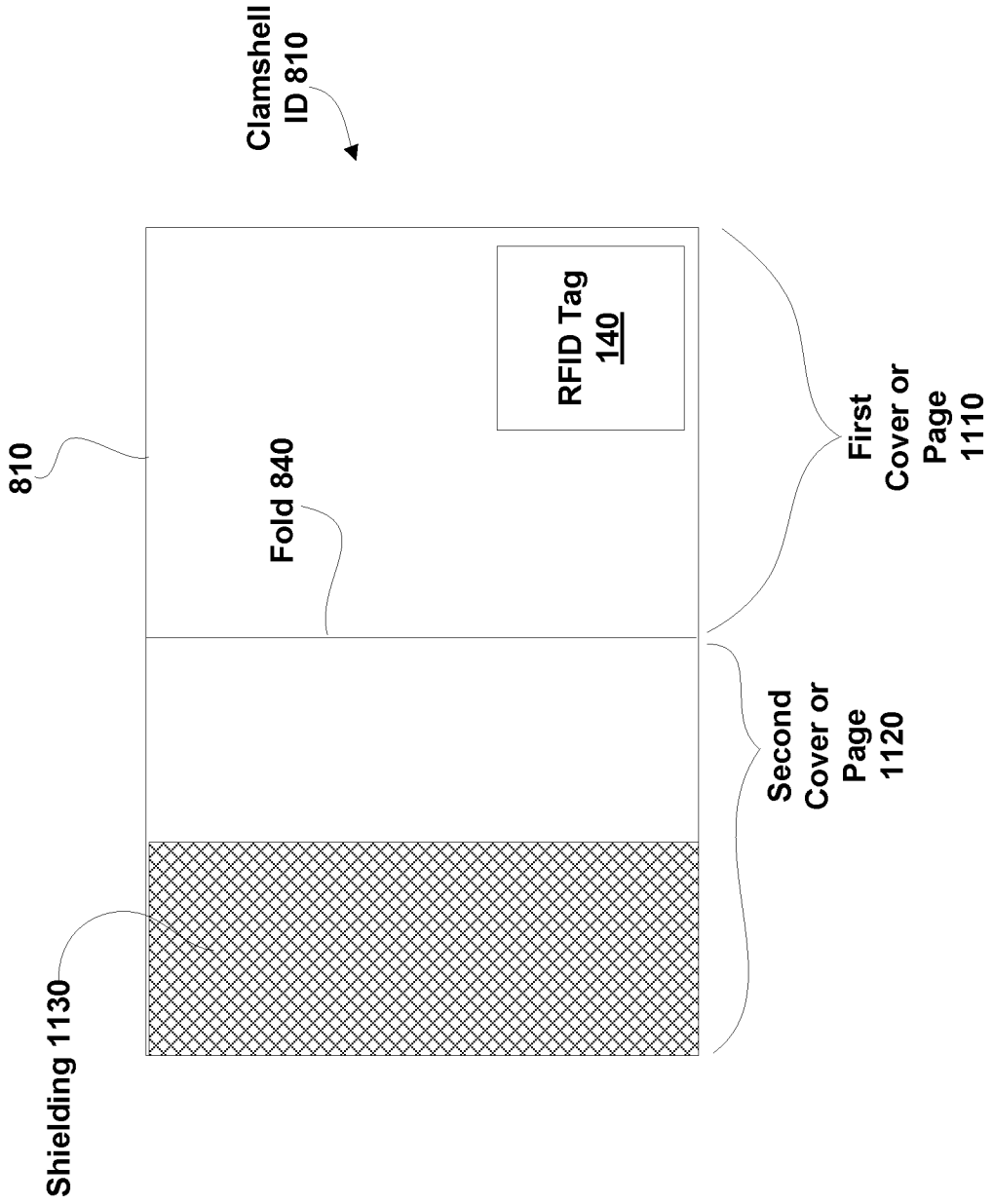

Clamshell
ID 810
810
Fold 840
RFID Tag
140
First
Cover or
Page
1110
Second
Cover or
Page
1120
Shielding 1130

FIG. 11

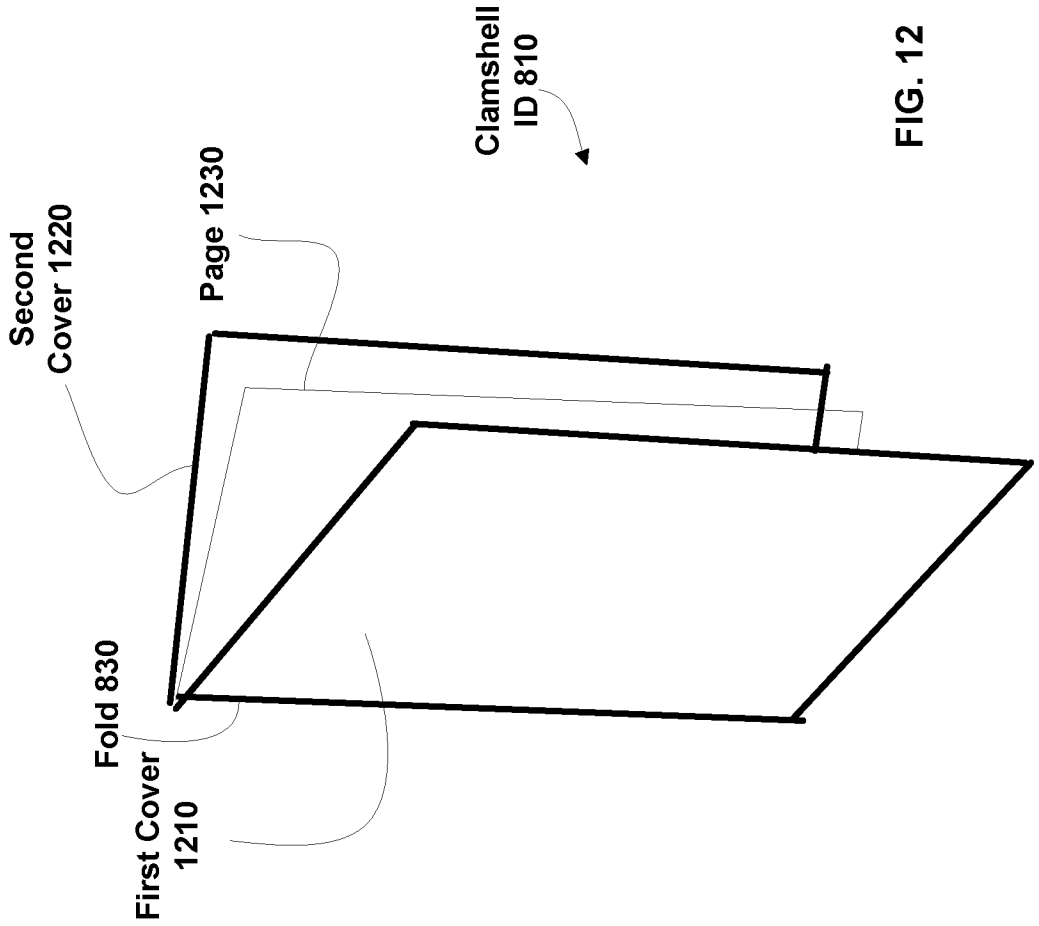

Second
Cover 1220
Page 1230
Clamshell
ID 810
Fold 830
First Cover
1210

FIG. 12

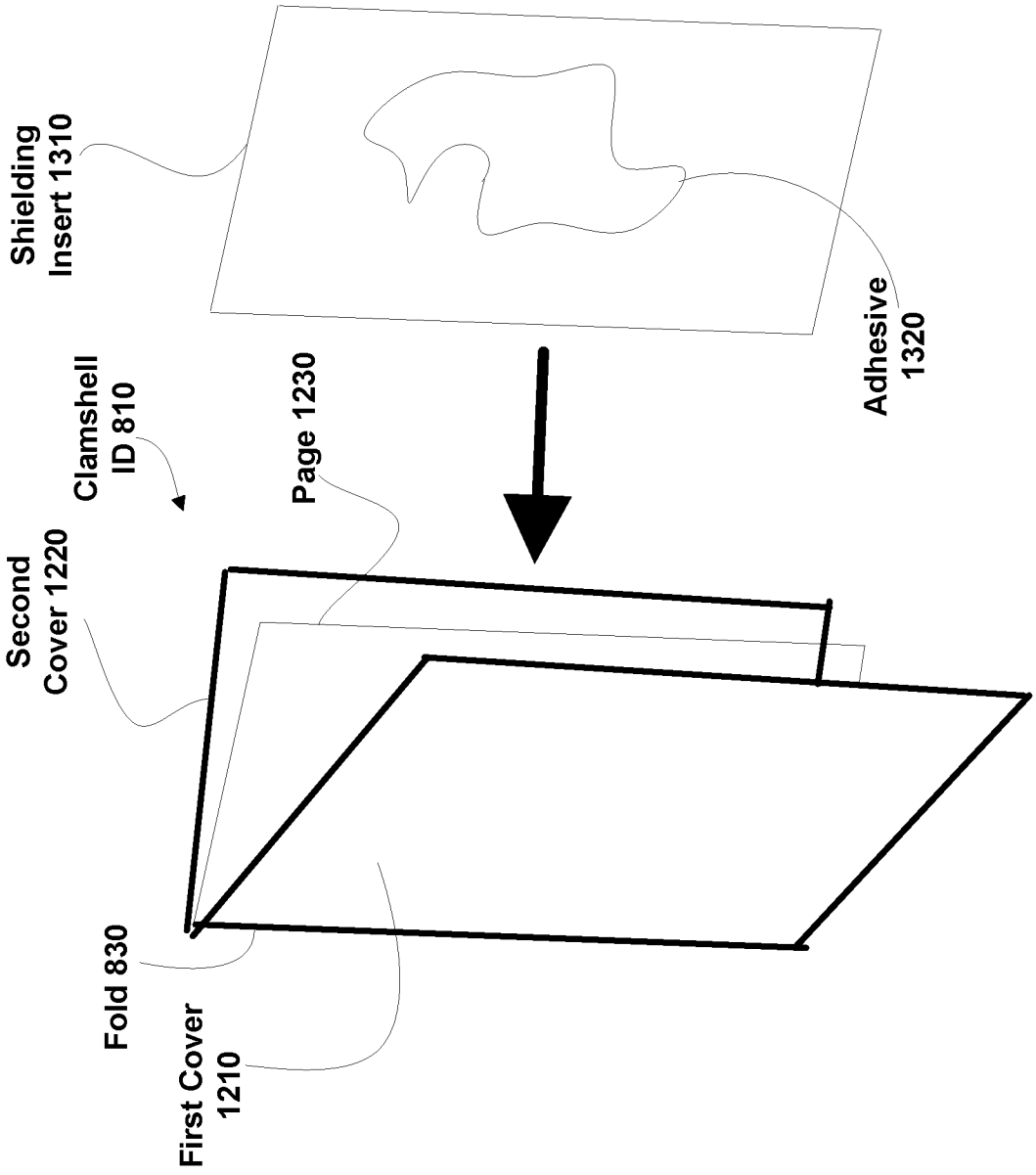

Shielding Insert 1310
Clamshell ID 810
Second Cover 1220
Fold 830
First Cover 1210
Page 1230
Adhesive 1320

FIG. 13

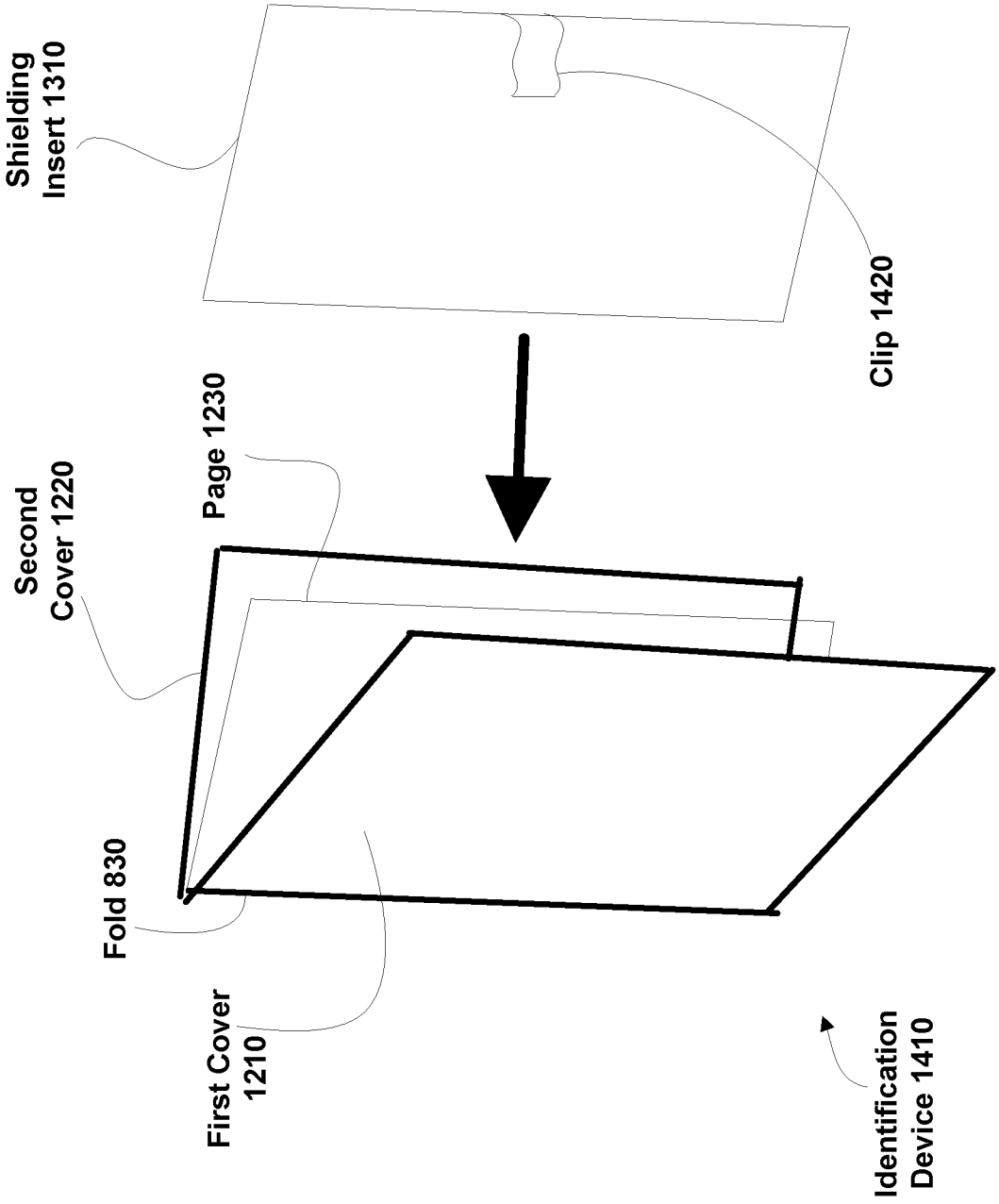

Shielding Insert 1310
Clip 1420
Second Cover 1220
Page 1230
Fold 830
First Cover 1210
Identification Device 1410

FIG. 14

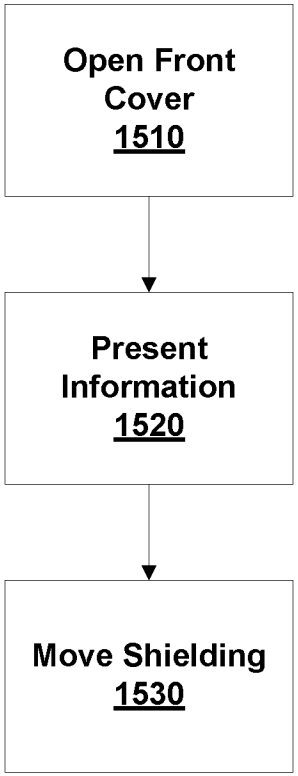


FIG. 15

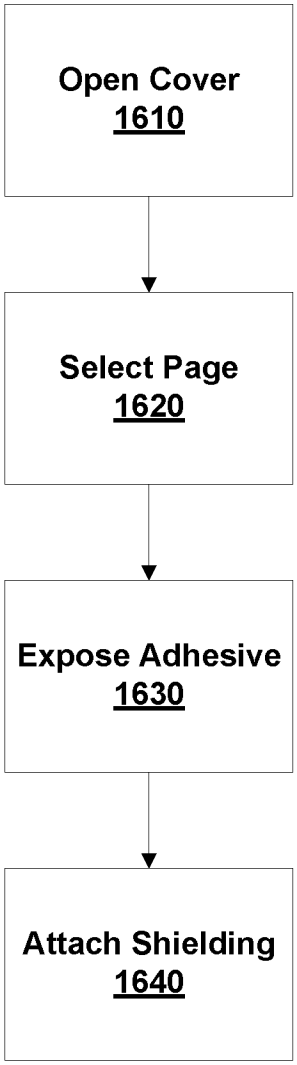


FIG. 16

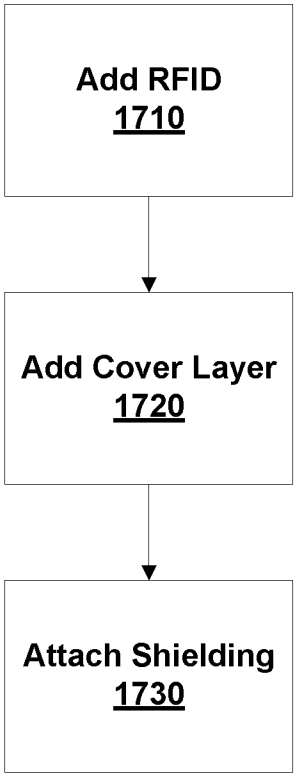


FIG. 17

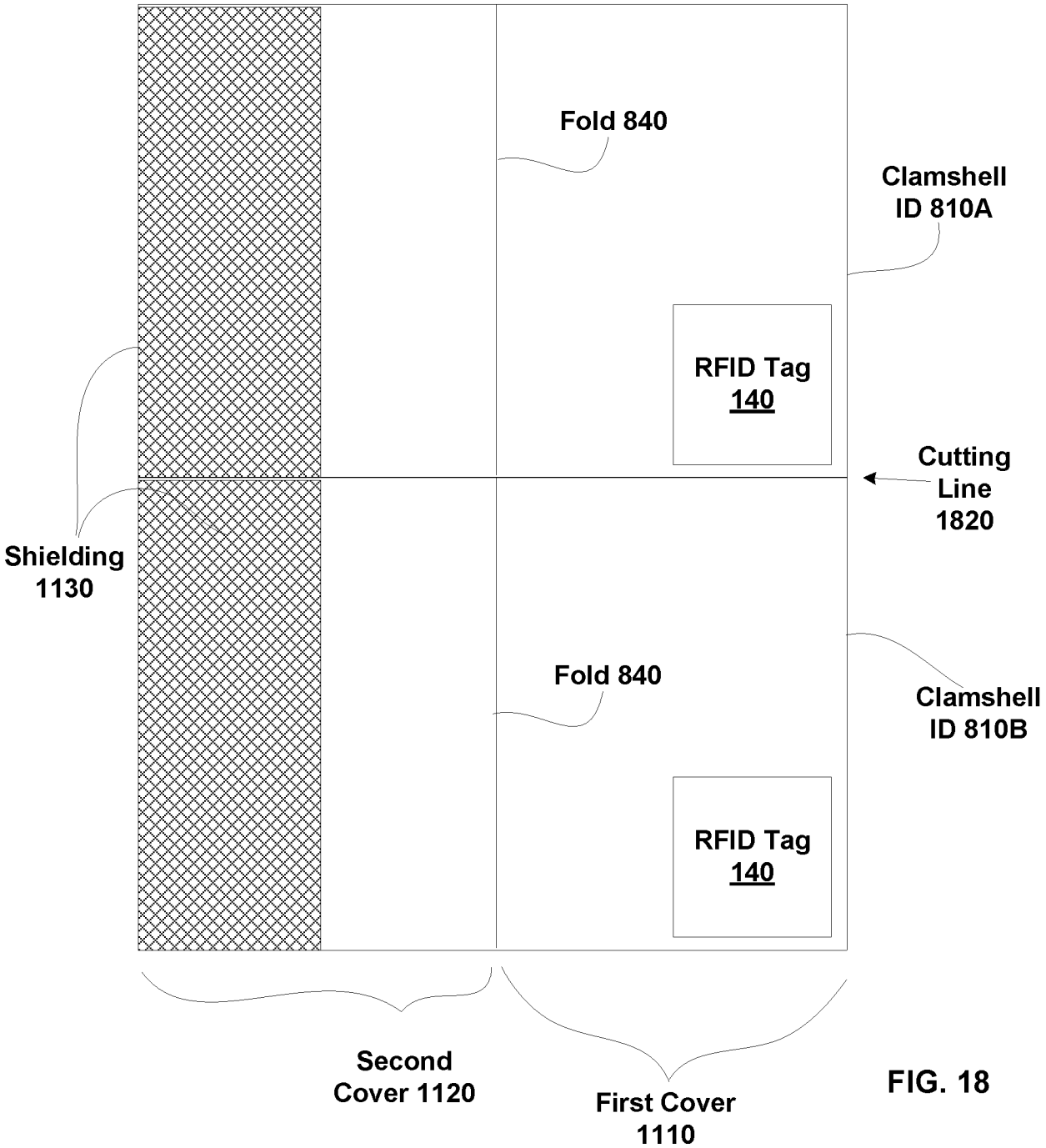

Fold 840
Clamshell
ID 810A
RFID Tag
140
Cutting
Line
1820
Shielding
1130
Fold 840
Clamshell
ID 810B
RFID Tag
140
Second
Cover 1120
First Cover
1110

FIG. 18

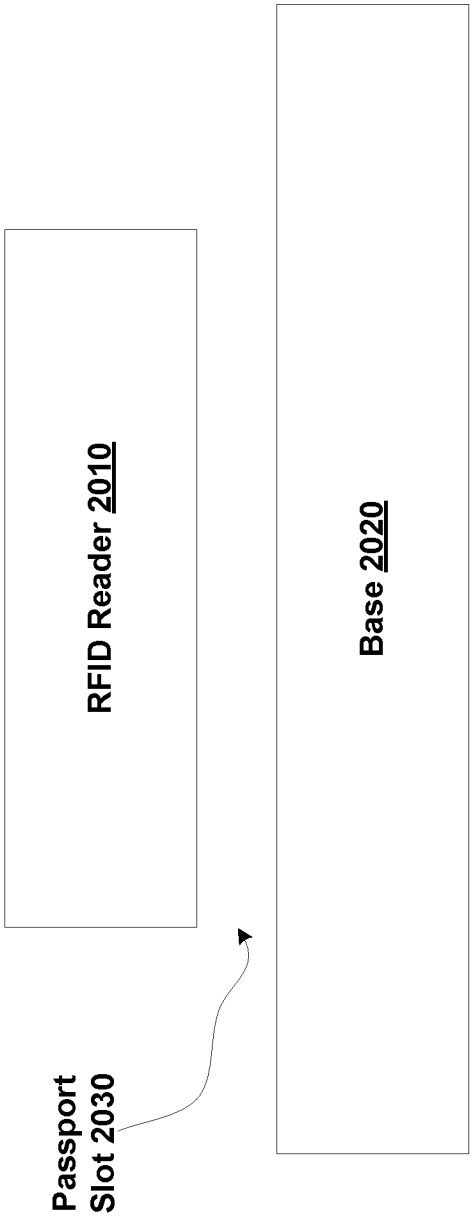


FIG. 20

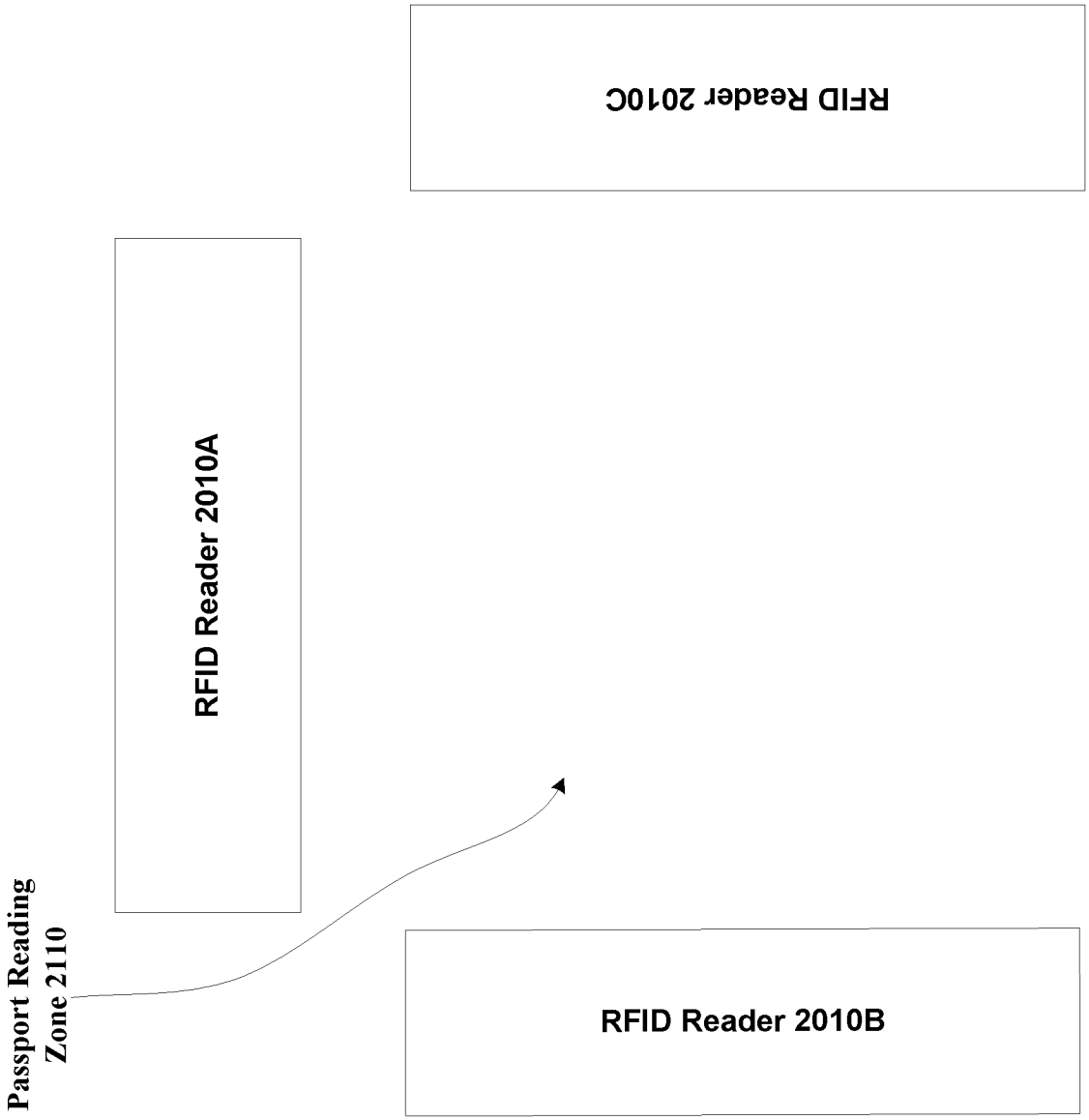

Passport Reading Zone 2110
RFID Reader 2010A
RFID Reader 2010B
RFID Reader 2010C

FIG. 21

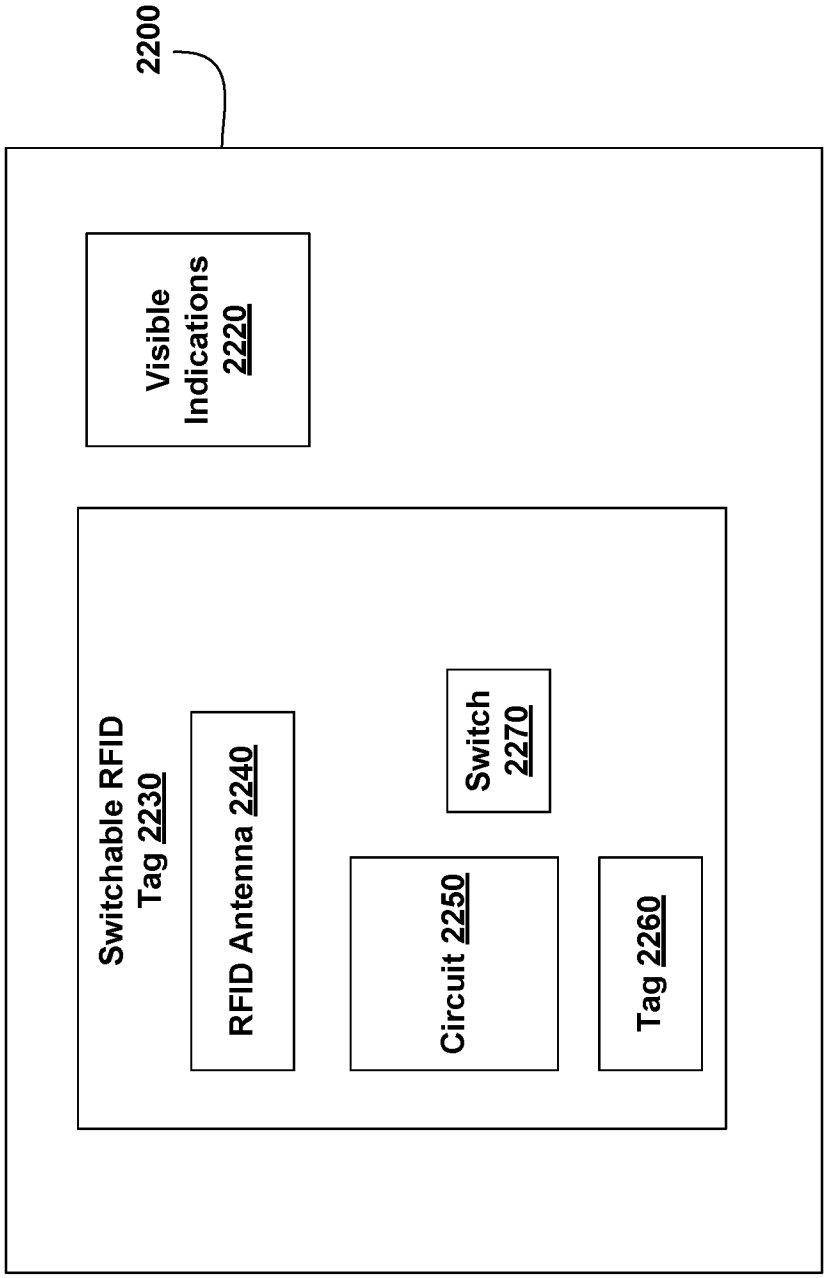

2200
Visible Indications 2220
Switchable RFID Tag 2230
RFID Antenna 2240
Circuit 2250
Switch 2270
Tag 2260

FIG. 22

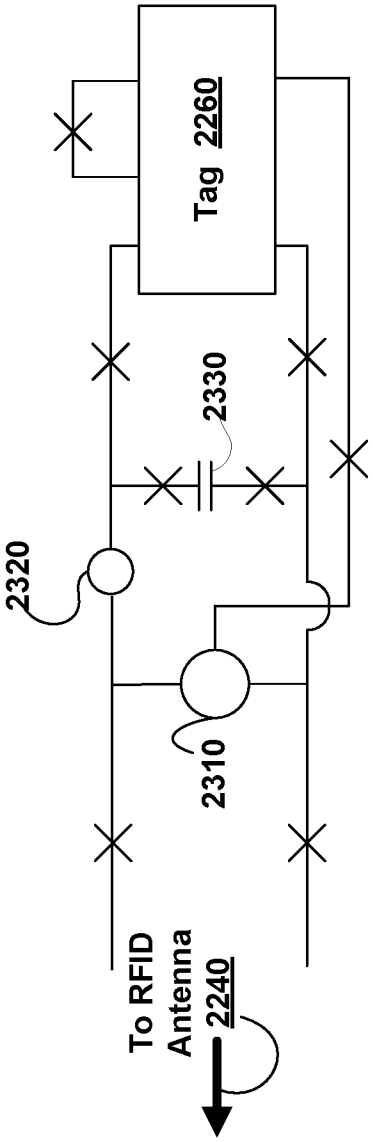
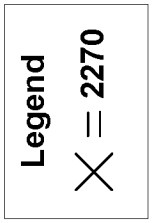

Tag 2260
2330
2320
2310
To RFID Antenna 2240

FIG. 23


Legend
= 2270

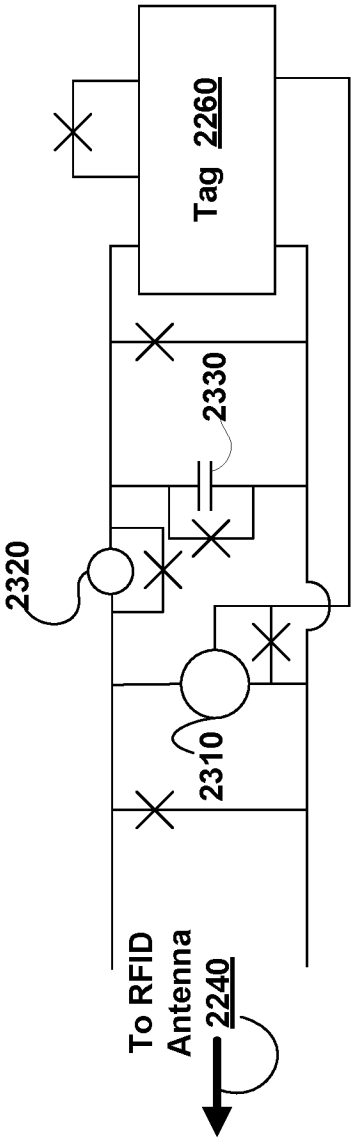
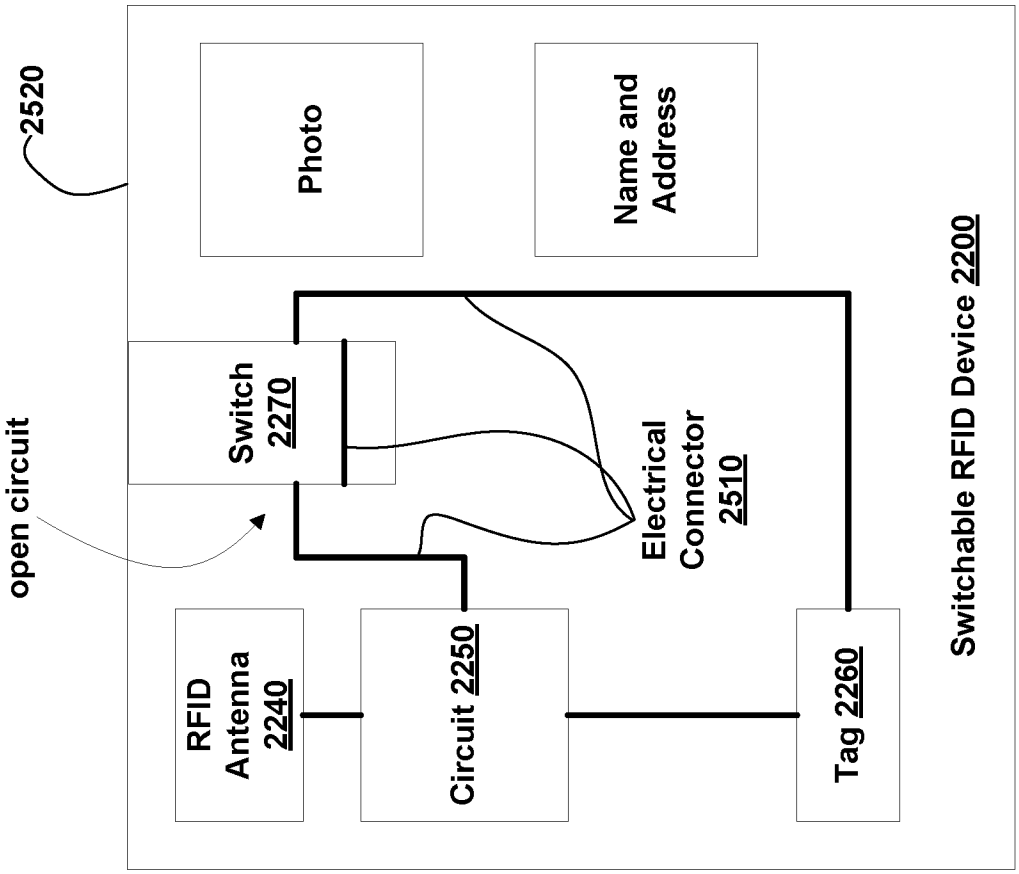

Tag 2260
2330
2320
2310
To RFID Antenna 2240

FIG. 24



OFF Position FIG. 25A

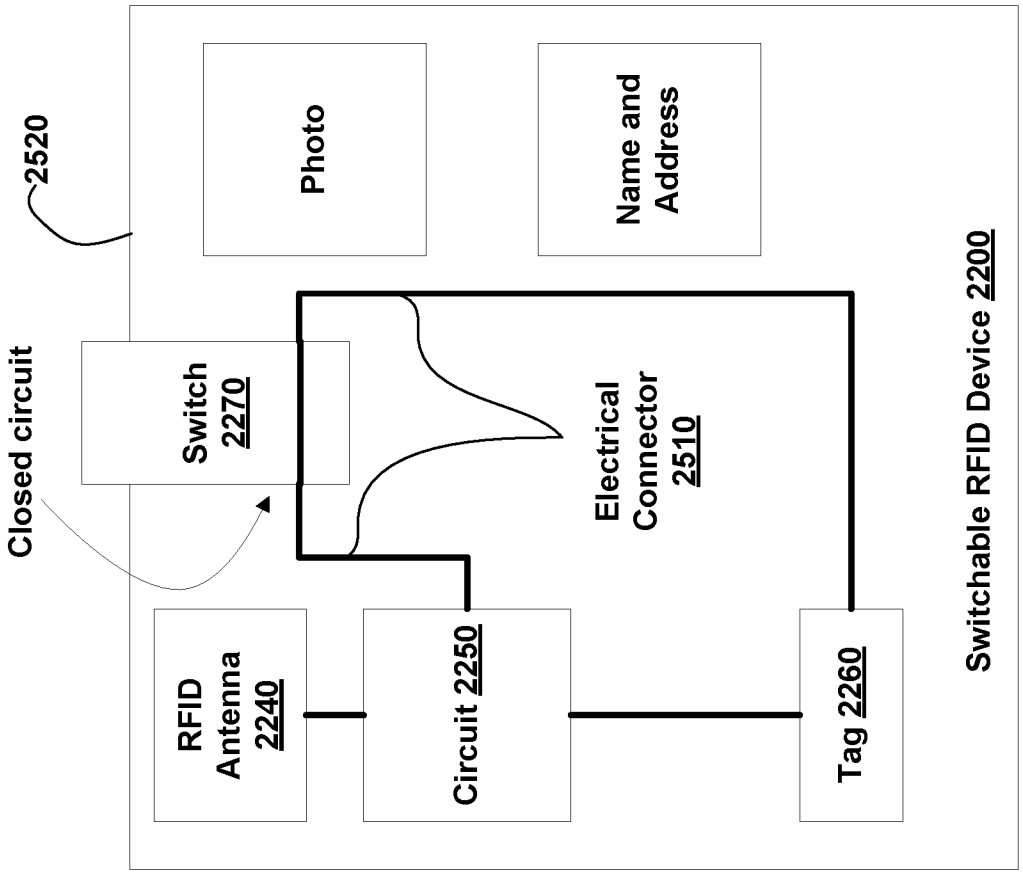


FIG. 25B ON Position

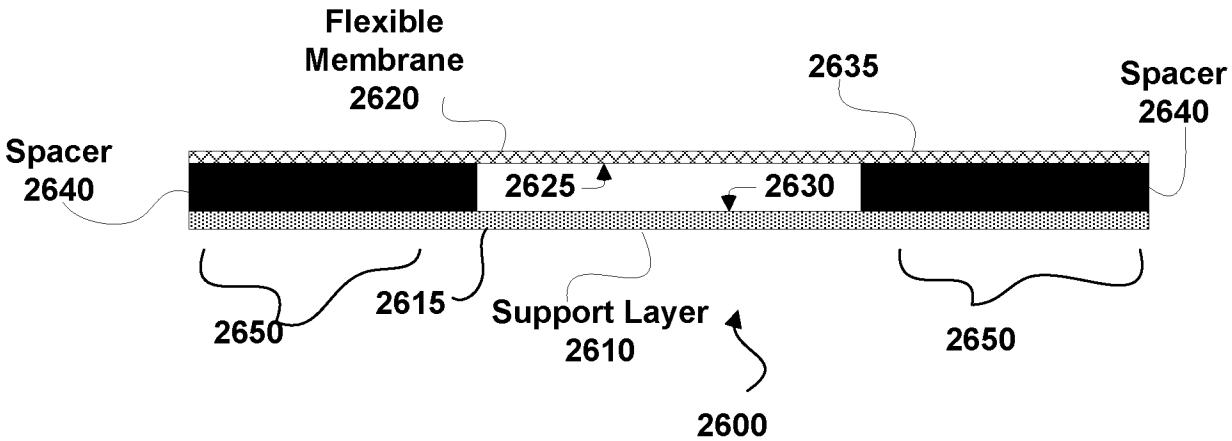


FIG. 26A
Membrane Switch (OFF)

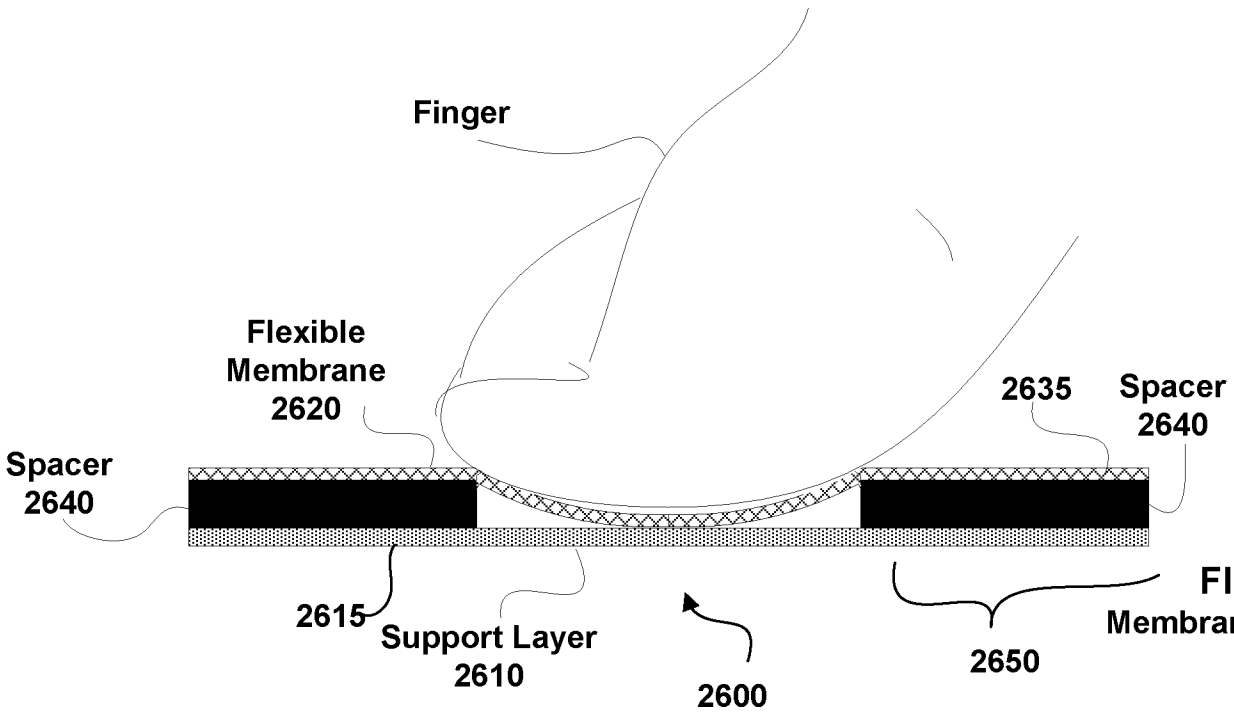


FIG. 26B
Membrane Switch (ON)

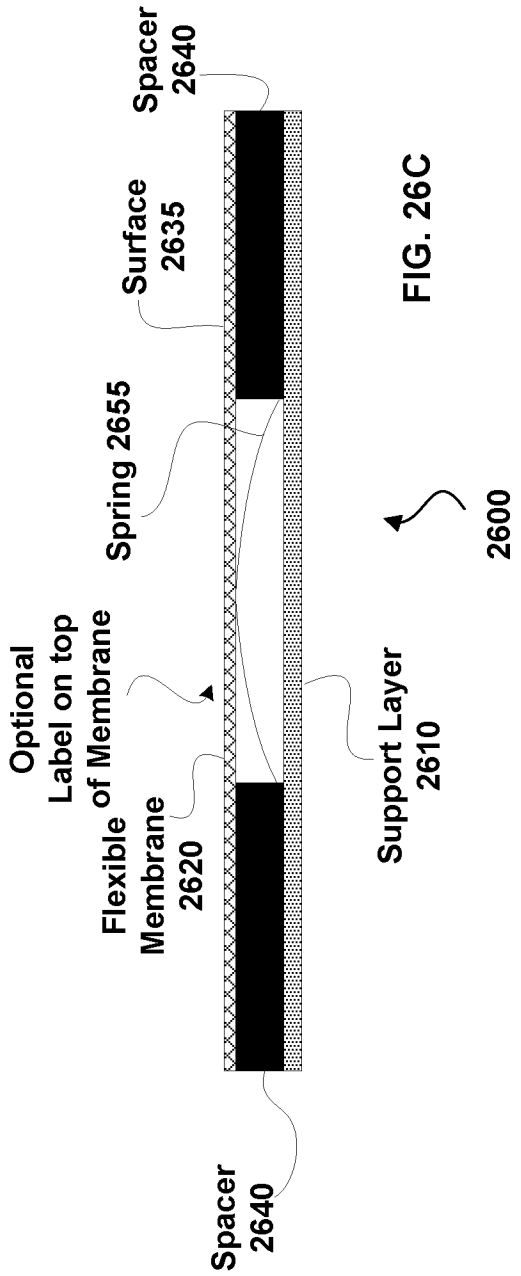


FIG. 26C

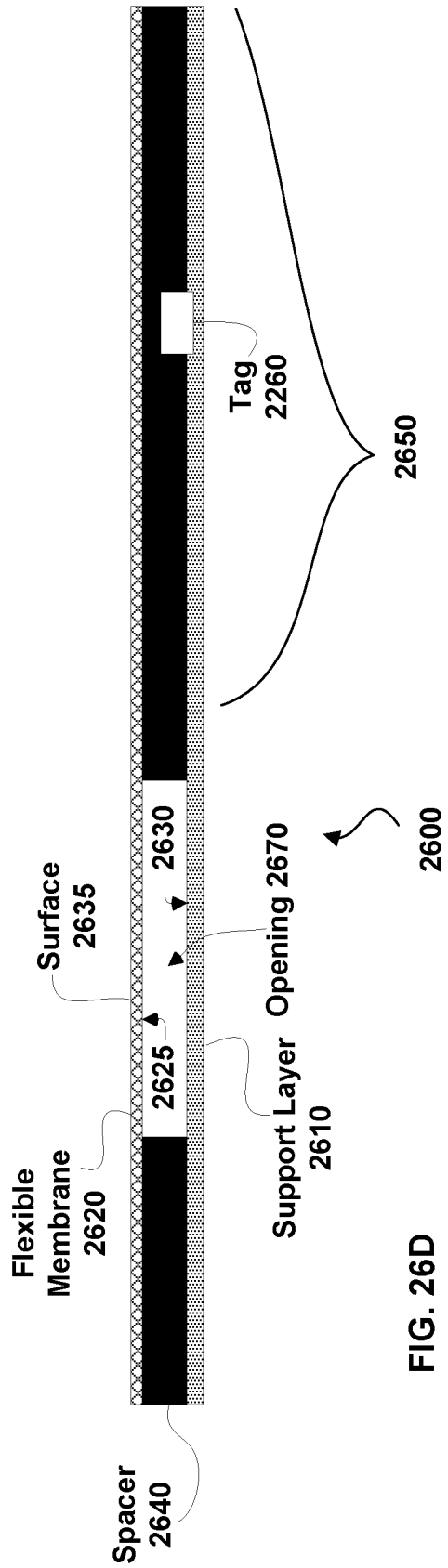


FIG. 26D

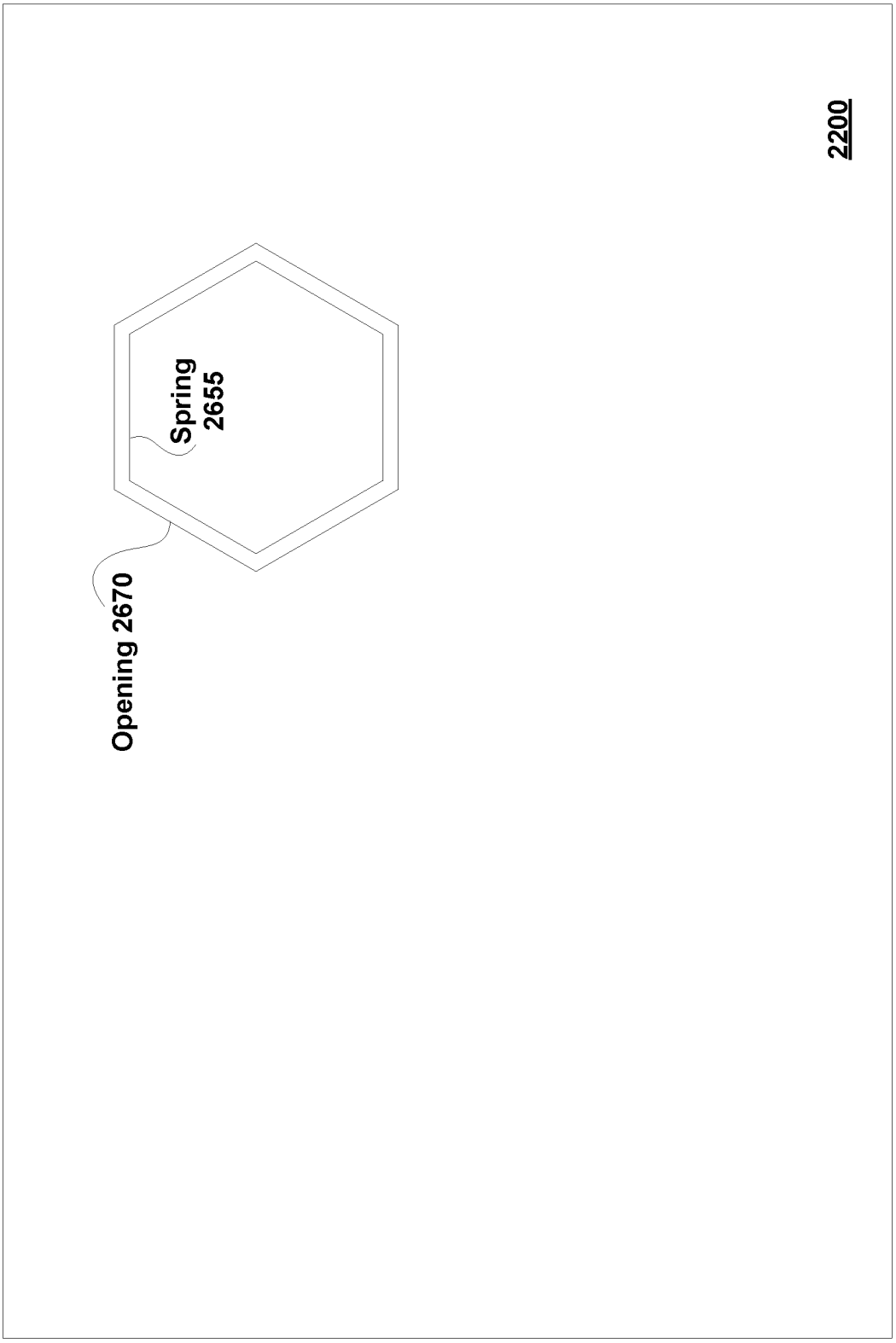


FIG. 27
(Top View)

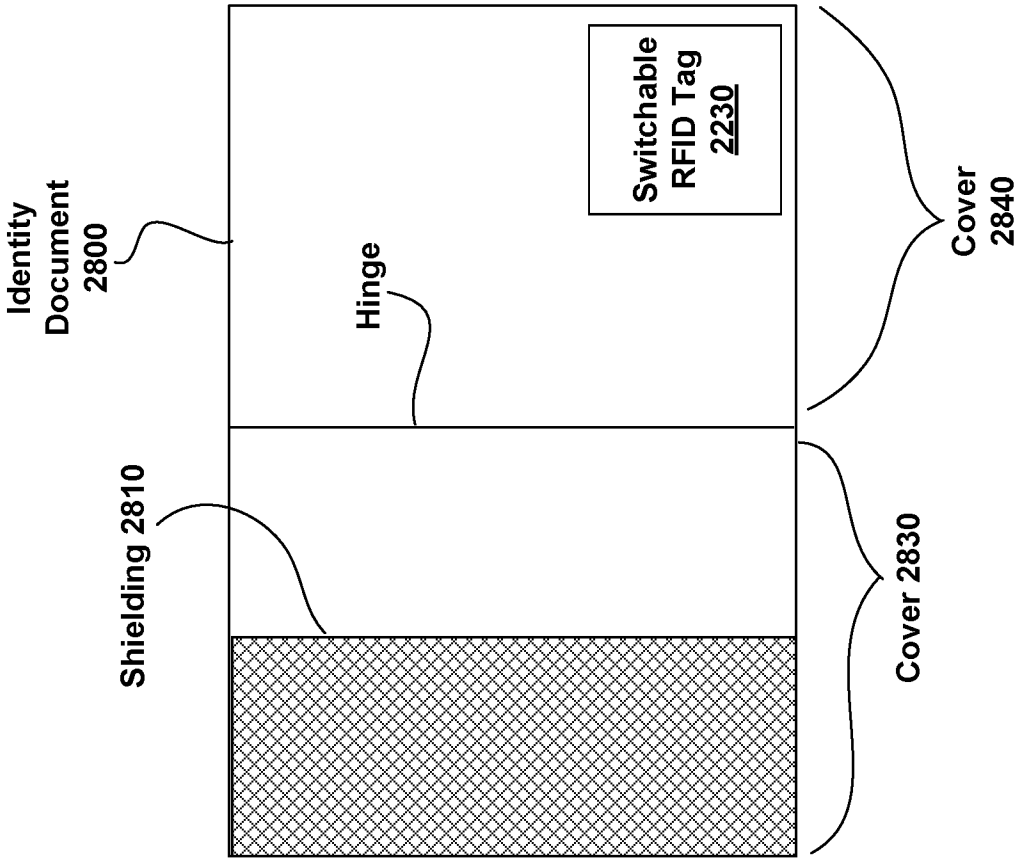

Identity Document 2800
Shielding 2810
Hinge
Switchable RFID Tag 2230
Cover 2830
Cover 2840

FIG. 28

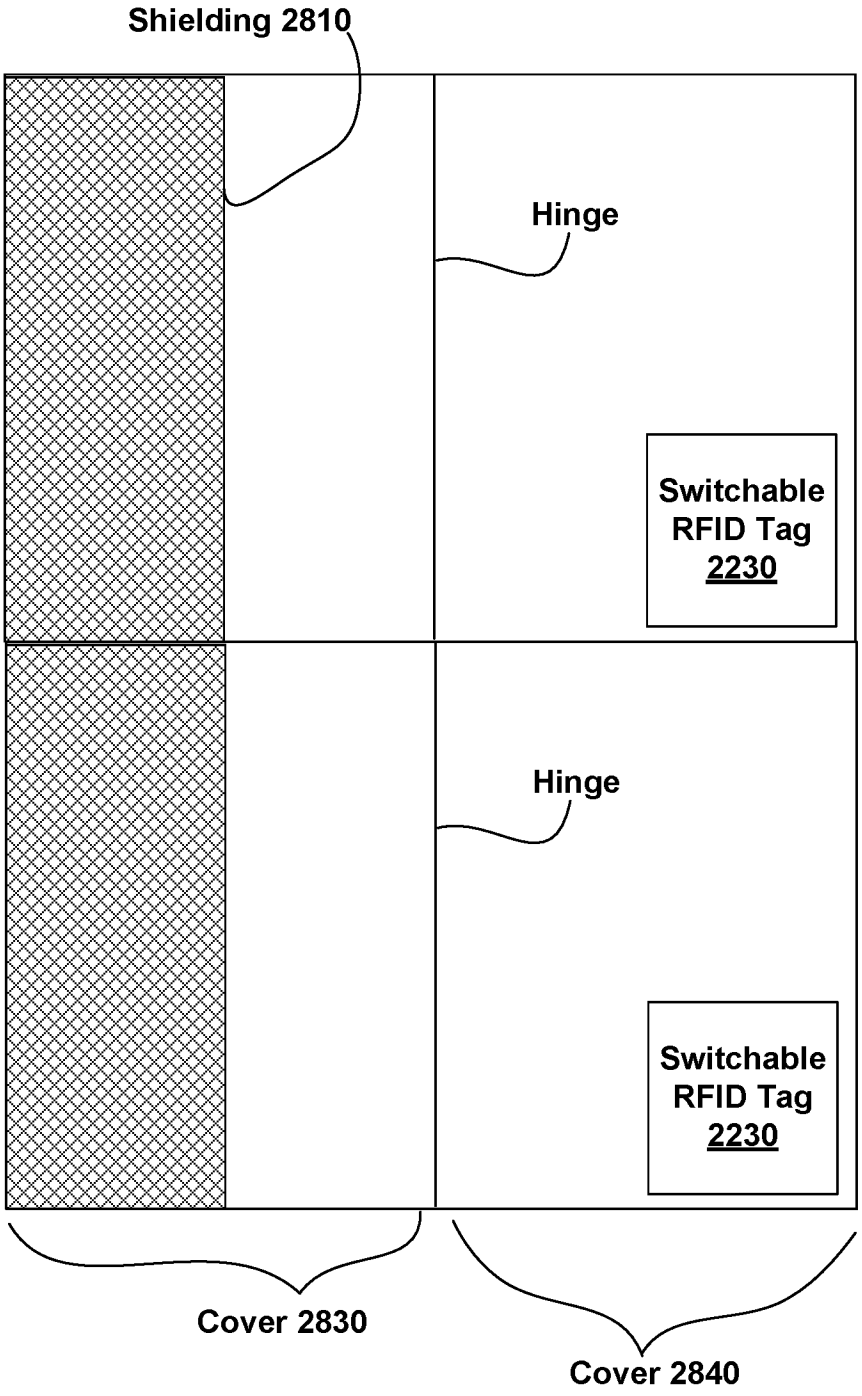

Shielding 2810
Hinge
Switchable RFID Tag 2230
Hinge
Switchable RFID Tag 2230
Cover 2830
Cover 2840

FIG. 29

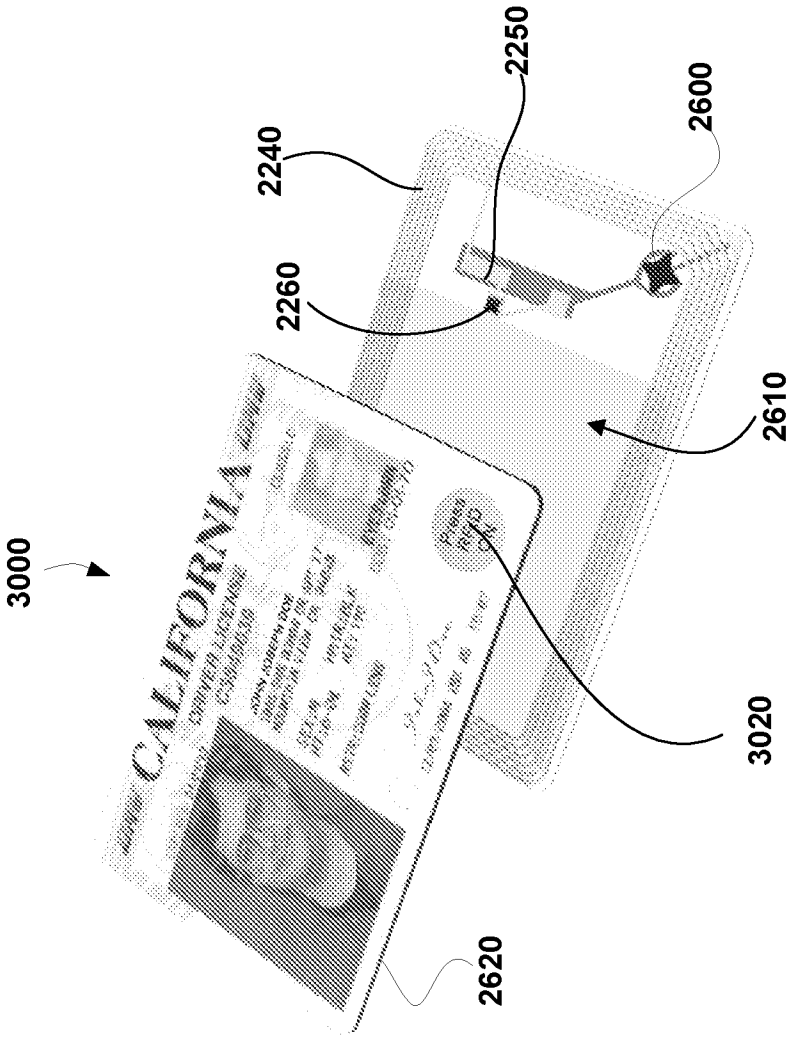


FIG. 30

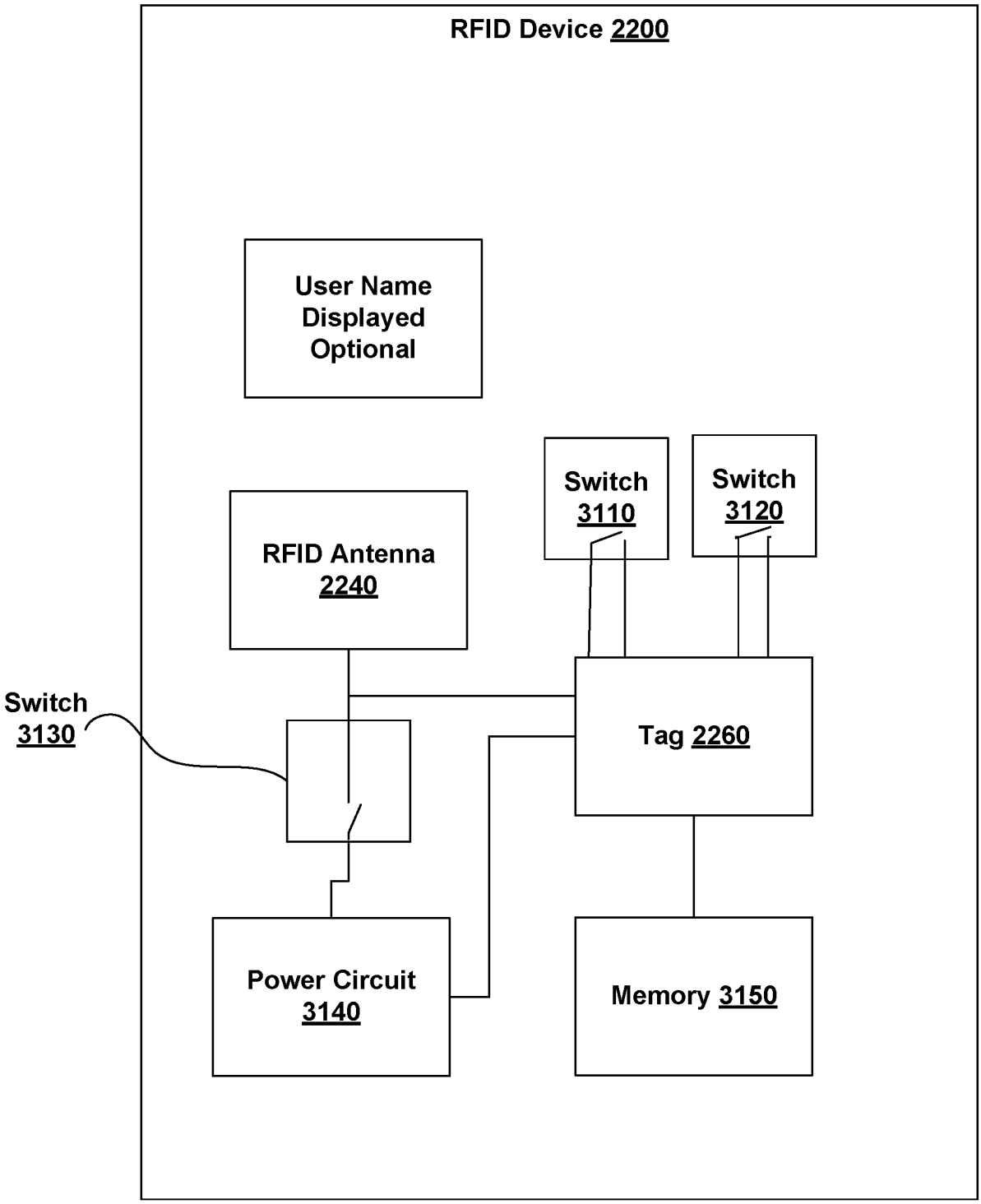

RFID Device 2200
User Name Displayed Optional
Switch 3110
Switch 3120
RFID Antenna 2240
Switch 3130
Tag 2260
Power Circuit 3140
Memory 3150

FIG. 31

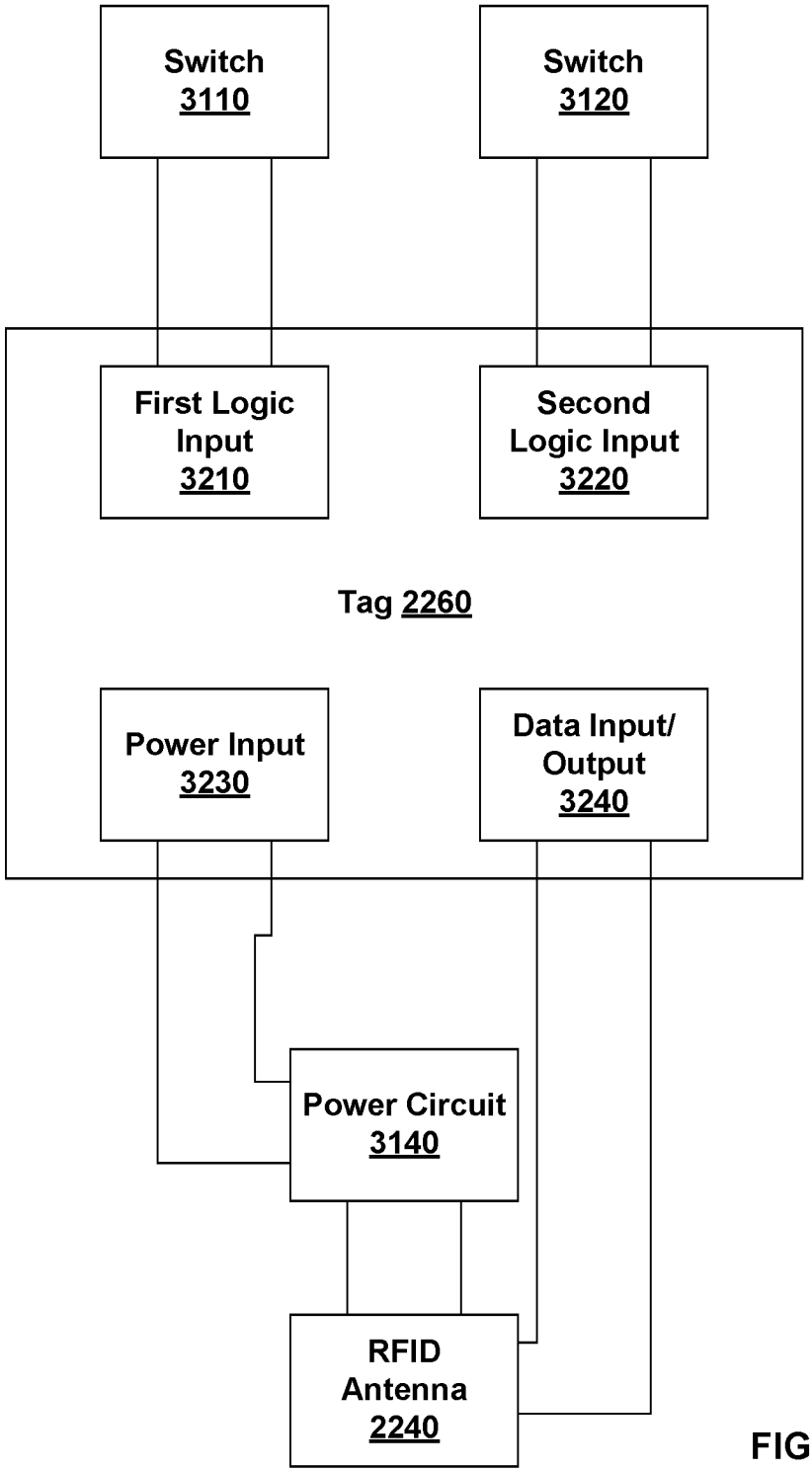

Switch
3110
Switch
3120
First Logic
Input
3210
Second
Logic Input
3220
Tag 2260
Power Input
3230
Data Input/
Output
3240
Power Circuit
3140
RFID
Antenna
2240

FIG. 32

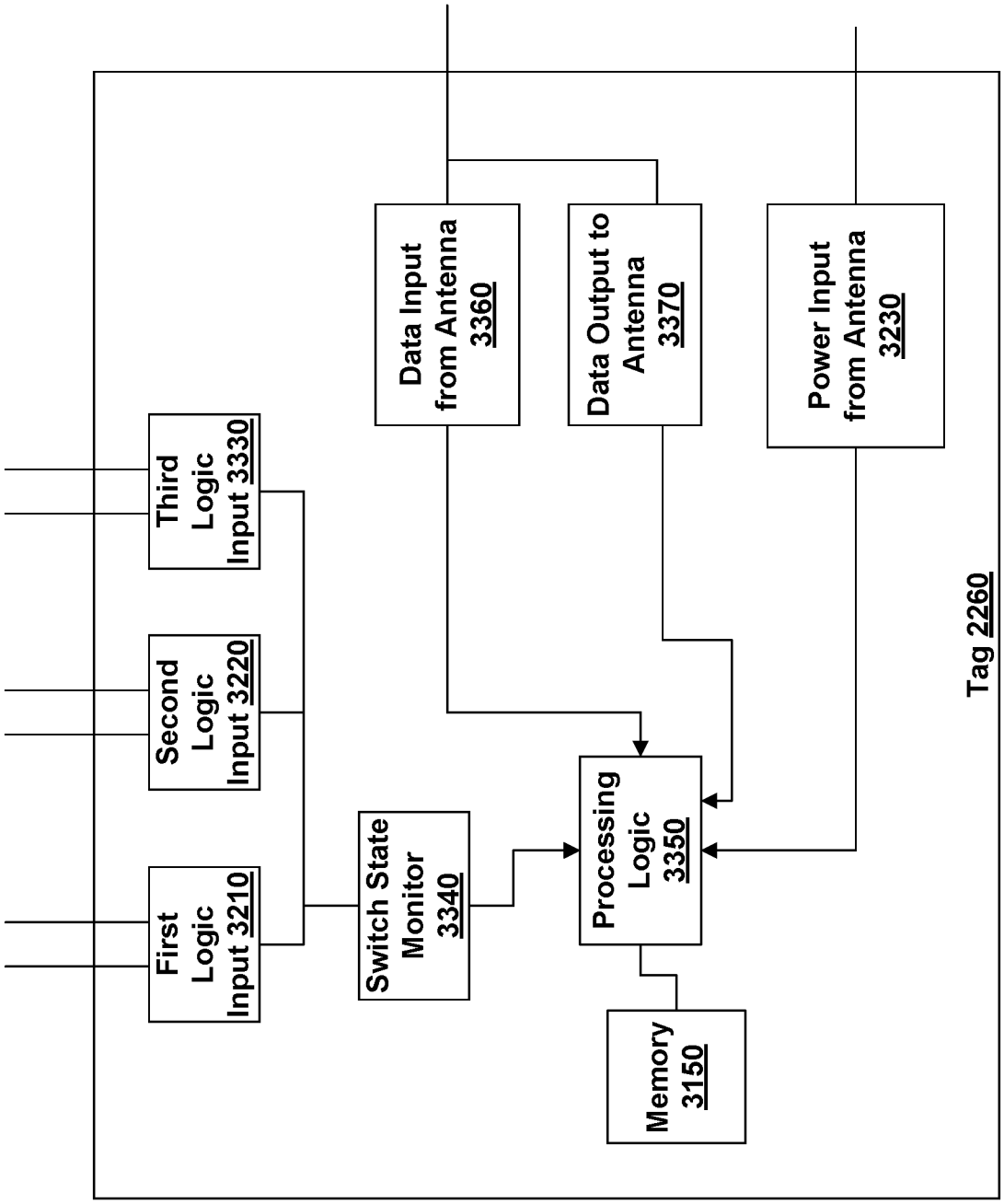

Third Logic Input 3330
Second Logic Input 3220
First Logic Input 3210
Switch State Monitor 3340
Data Input from Antenna 3360
Data Output to Antenna 3370
Power Input from Antenna 3230
Processing Logic 3350
Memory 3150
Tag 2260

FIG. 33

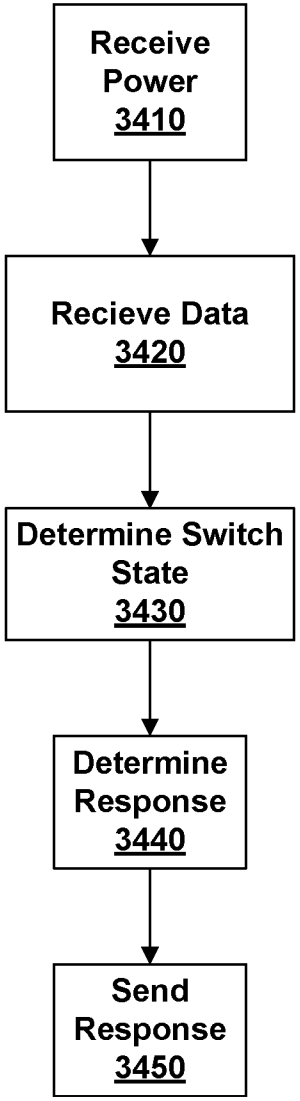

Receive Power 3410
Recieve Data 3420
Determine Switch State 3430
Determine Response 3440
Send Response 3450

FIG. 34

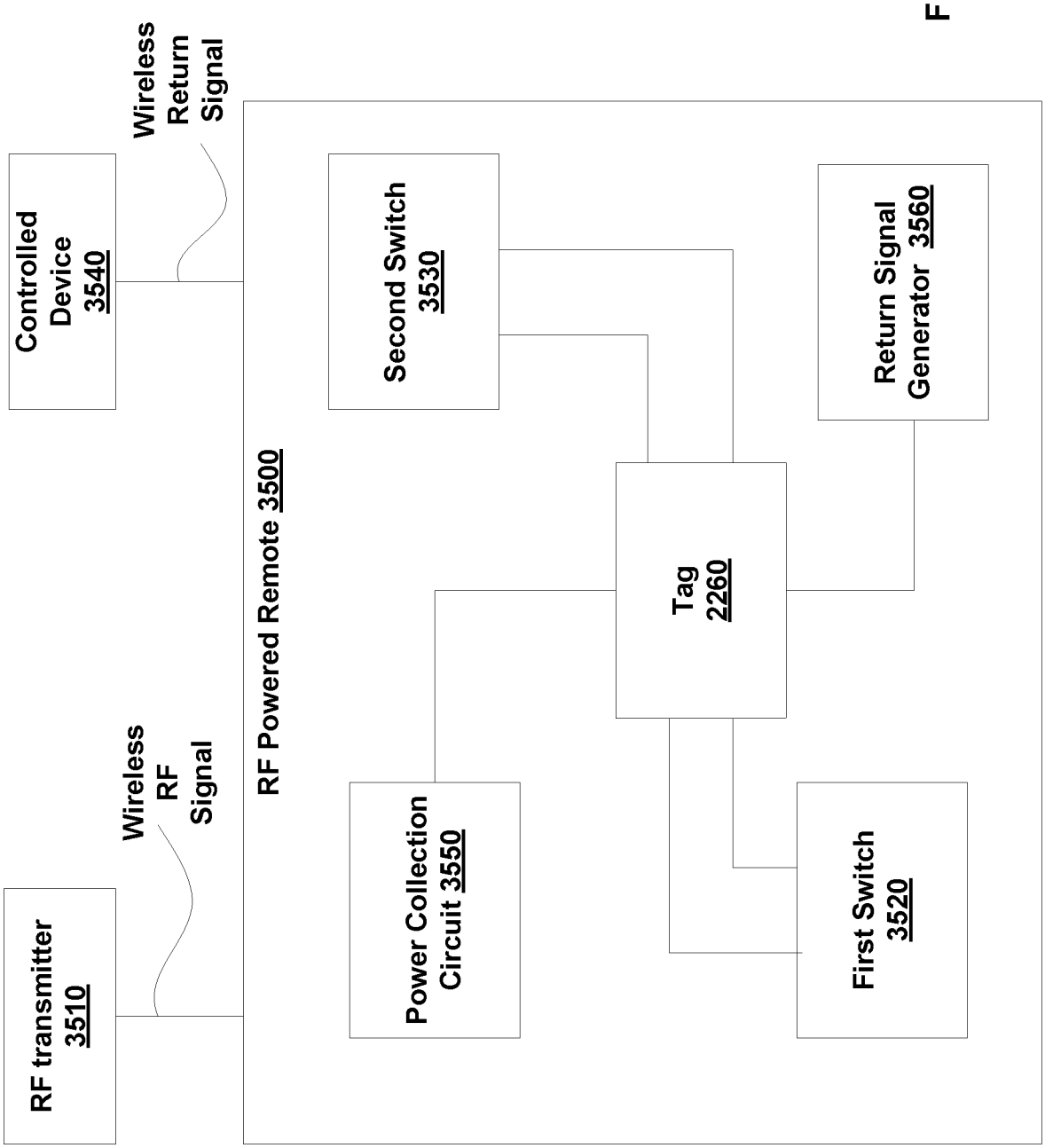

Controlled Device 3540
Wireless Return Signal
RF transmitter 3510
Wireless RF Signal
RF Powered Remote 3500
Second Switch 3530
Return Signal Generator 3560
Tag 2260
Power Collection Circuit 3550
First Switch 3520

FIG. 35

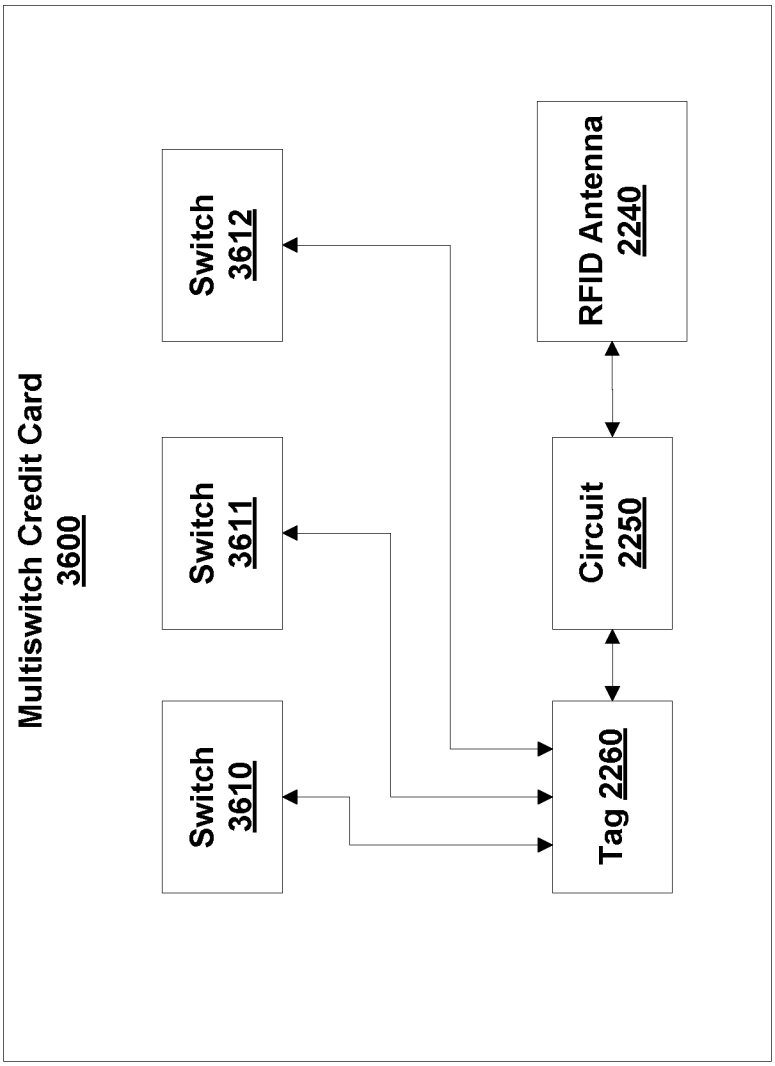

Multiswitch Credit Card
3600
Switch
3610
Switch
3611
Switch
3612
Tag 2260
Circuit
2250
RFID Antenna
2240

FIG. 36

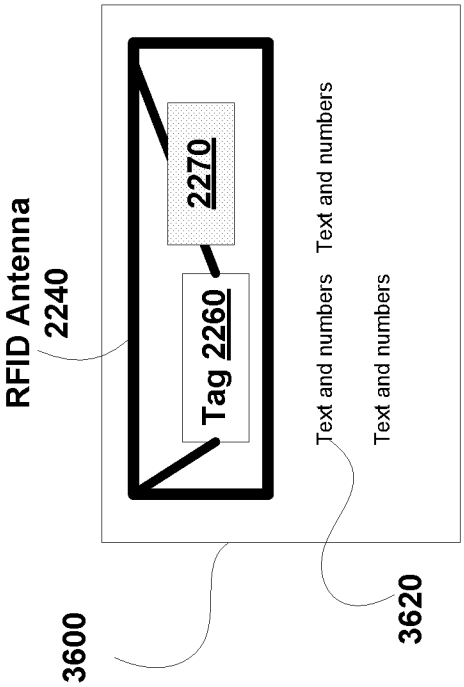


FIG. 37B

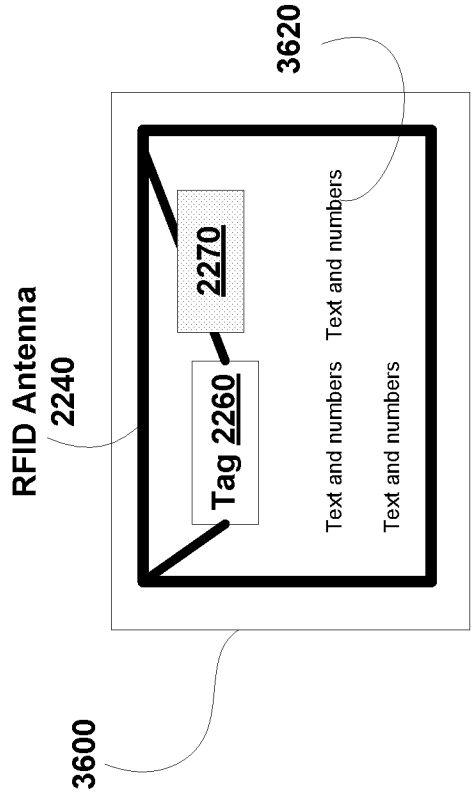


FIG. 37A

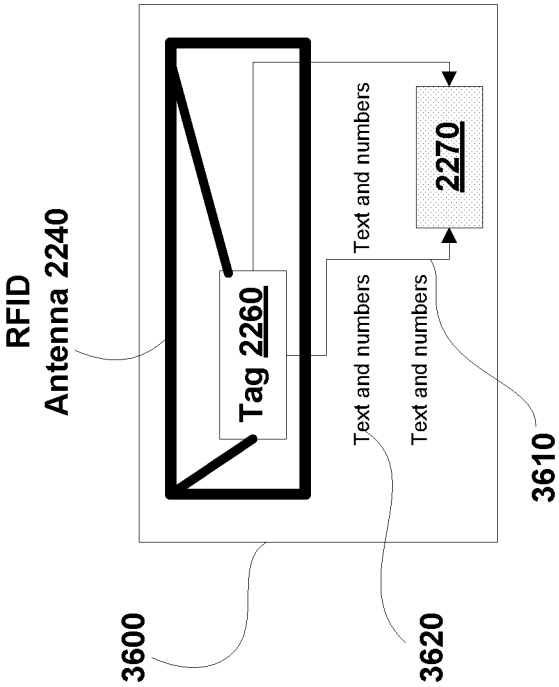


FIG. 37C

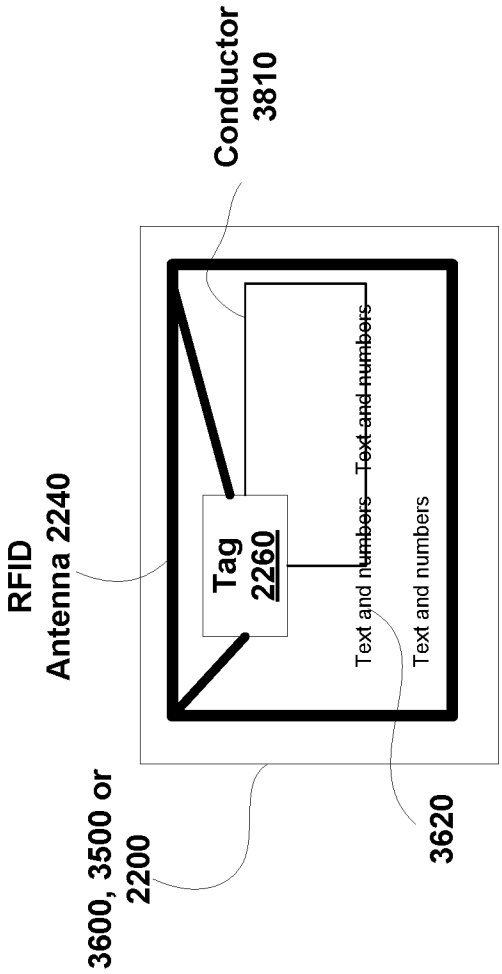

Conductor
3810
RFID
Antenna 2240
Tag
2260
Text and numbers
Text and numbers
Text and numbers
3600, 3500 or
2200
3620

FIG. 38

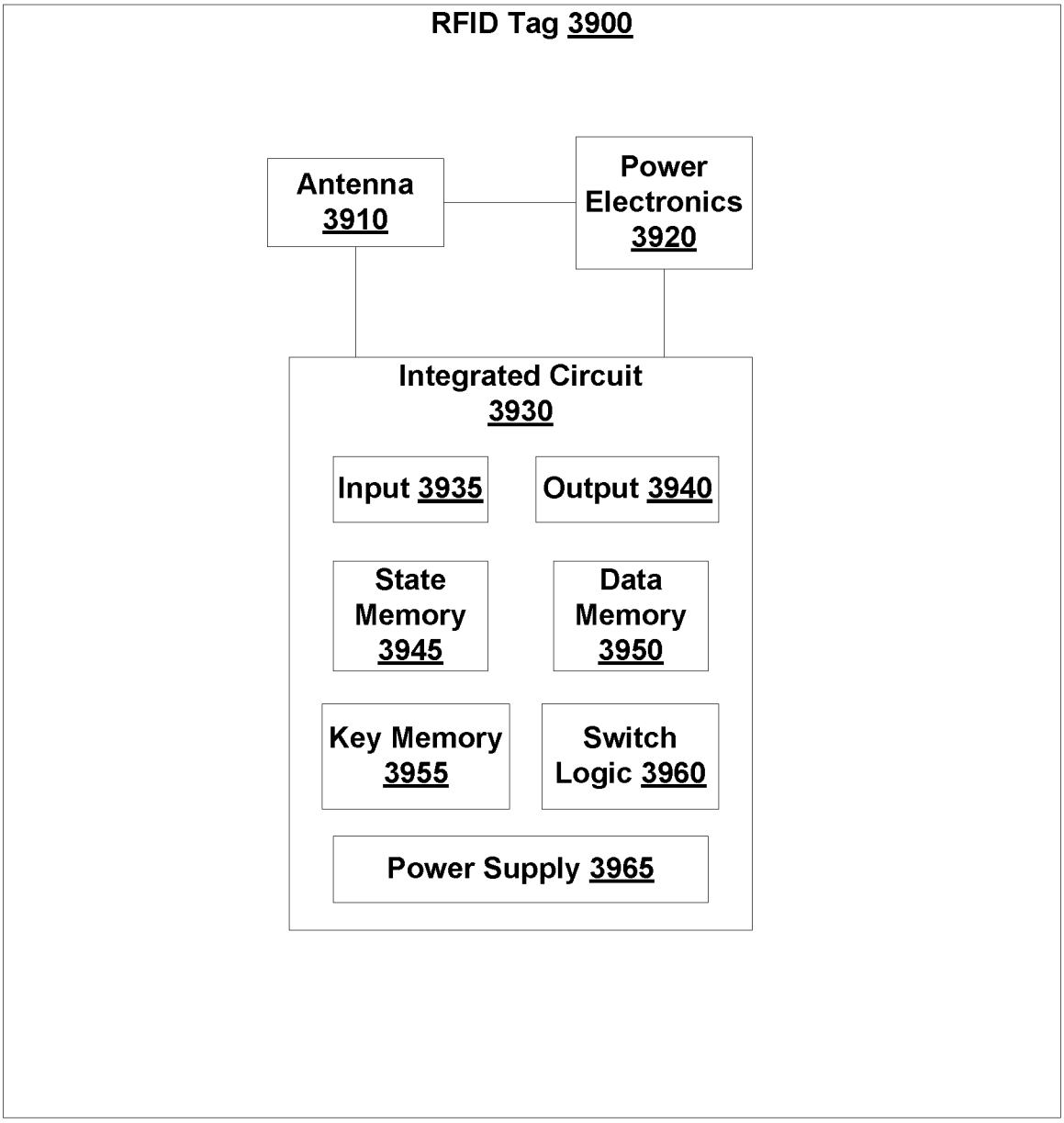

RFID Tag 3900
Antenna 3910
Power Electronics 3920
Integrated Circuit 3930
Input 3935
Output 3940
State Memory 3945
Data Memory 3950
Key Memory 3955
Switch Logic 3960
Power Supply 3965

FIG. 39

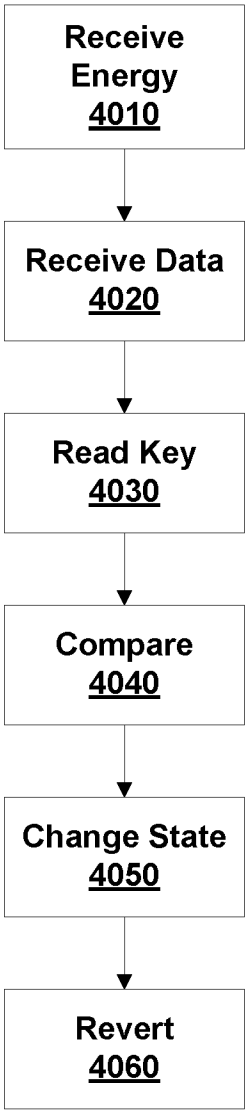

Receive Energy 4010
Receive Data 4020
Read Key 4030
Compare 4040
Change State 4050
Revert 4060

FIG. 40

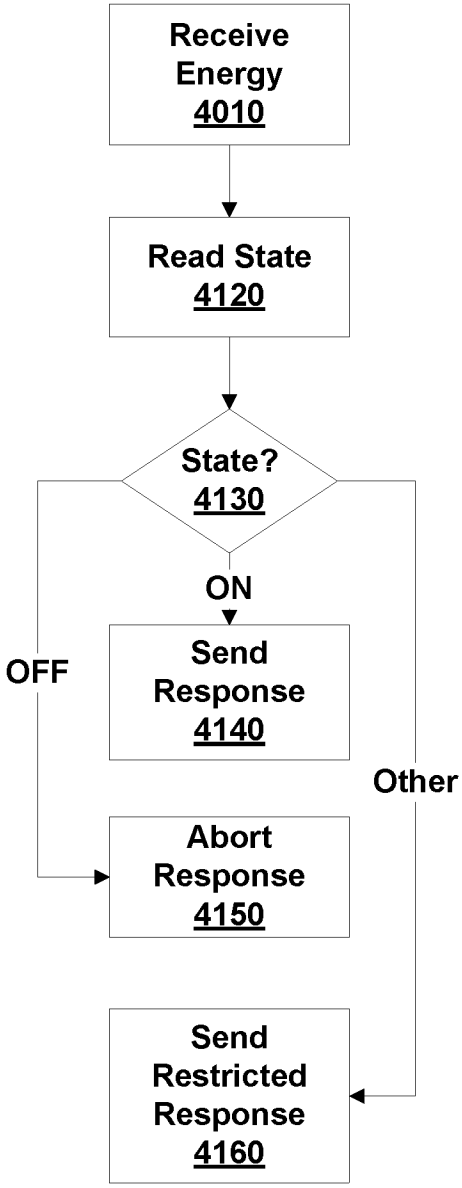

Receive Energy 4010
Read State 4120
State? 4130
ON
OFF
Other
Send Response 4140
Abort Response 4150
Send Restricted Response 4160

FIG. 41