AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:23-CV-00187	4/24/2023	Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
CardWare Inc.	Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	11,620,634	4/4/2023	CARDWARE INC.
2			
3			
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

Print Save As... Reset

UNITED STATES PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

ACKNOWLEDGEMENT OF LOSS OF ENTITLEMENT TO ENTITY STATUS DISCOUNT

APPLICATION #	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET #	REQUEST ID
17/528,073	11/16/2021	David WYATT	WYAT-0002-13C12US	267402

The entity status change request below filed through Patent Center on 08/29/2024 has been accepted.

Certifications

APPLICANT CHANGING TO REGULAR UNDISCOUNTED FEE STATUS

Signature

I certify, in accordance with 37 CFR 1.4(d)(4), that I am one of the signatories making the entity status change.

Signature	Name	Registration #
/Anthony C. Murabito/	Anthony Murabito	35295

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.
17/528,073	04/04/2023	11620634	WYAT-0002-13C12US	4809

136197 7590 03/15/2023

David Wyatt c/o Murabito, Hao & Barnes
111 North Market Street
Suite 700
San Jose, CA 95113

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

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

The Patent Term Adjustment is 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):

David WYATT, Austin, TX;

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

CARDWARE, INC, Austin, TX;

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.

IR103 (Rev. 10/09)

PART B – FEE(S) TRANSMITTAL

Complete and send this form, together with the 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, VA 22313-1450

By fax, send to: (571) 273-2885

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

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

David Wyatt c/o Murabito, Hao & Barnes LLP
111 North Market Steet
Suite 700
San Jose, CA 95113

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.

Mina Oliveri	(Typed or printed name)
/Mina Oliveri/	(Signature)
2-14-2023	(Date)

APPLICATION NO	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO	CONFIRMATION NO
17/528,073	11/16/2021	David Wyatt	WYAT-0002.USD1C1C1C1C1C	4809

TITLE OF INVENTION: MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

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	05/15/2023

EXAMINER	ART UNIT	CLASS-SUBCLASS

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

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

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

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

(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. 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: CARDWARE, INC.

(B) RESIDENCE: (CITY and STATE or COUNTRY): AUSTIN, TEXAS

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

4a. Fees Submitted: ☑ Issue Fee ☐ Publication Fee (if required) ☐ Advance Order - # of Copies _____

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

☑ Electronic Payment via EFS-Web ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. 504160

5. Change of 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 as a notification of loss of entitlement to micro entity status.

☐ Applicant changing to regular undiscounted fee status. NOTE: Checking this box will be taken as 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 /Anthony C. Murabito/ Date 2-14-2023

Typed or printed name Anthony C. Murabito Registration No. 35,295

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.

Electronic Patent Application Fee Transmittal

Application Number:	17528073
Filing Date:	16-Nov-2021
Title of Invention:	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE
First Named Inventor/Applicant Name:	David WYATT
Filer:	Anthony C. Murabito/Mina Oliveri
Attorney Docket Number:	WYAT-0002-13C12US

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:	47531835
Application Number:	17528073
International Application Number:	
Confirmation Number:	4809
Title of Invention:	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE
First Named Inventor/Applicant Name:	David WYATT
Customer Number:	136197
Filer:	Anthony C. Murabito/Mina Oliveri
Filer Authorized By:	Anthony C. Murabito
Attorney Docket Number:	WYAT-0002-13C12US
Receipt Date:	14-FEB-2023
Filing Date:	16-NOV-2021
Time Stamp:	15:28:05
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	EFT
Payment was successfully received in RAM	$480
RAM confirmation Number	E20232DF29188730
Deposit Account	504160
Authorized User	Mina Oliveri
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.17 (Patent application and reexamination processing fees) 37 CFR 1.19 (Document supply fees)	

37 CFR 1.20 (Post Issuance 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	Issue Fee Payment (PTO-85B)	WYAT-0002-USD1C1C1C1C1C_IssueFee_Tran_2-14-2023.pdf	296037 42f56887661a1a626d828d80618bf2d84b591e2e	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	38083 9be0bc43f8aeafb866a9db489893a13bcfeb6807	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	334120		

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.

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
17/528,073	11/16/2021	2876	3750	WYAT-0002-USD1C1C1C1C1C	14	2

CONFIRMATION NO. 4809

CORRECTED FILING RECEIPT

136197
David Wyatt c/o Murabito, Hao & Barnes
111 North Market Street
Suite 700
San Jose, CA 95113

OC000000137392572

Date Mailed: 02/14/2023

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)

David WYATT, Austin, TX;

Applicant(s)

CARDWARE, INC, Austin, TX;

Power of Attorney: The patent practitioners associated with Customer Number 136197

Domestic Priority data as claimed by applicant

This application is a CON of 17/075,637 10/20/2020 PAT 11176538
which is a CON of 16/459,150 07/01/2019 PAT 10810579
which is a CON of 15/701,261 09/11/2017 PAT 10339520
which is a CON of 14/981,757 12/28/2015 PAT 9760884
which is a CON of 14/680,979 04/07/2015 PAT 9224083
which is a DIV of 14/217,261 03/17/2014 PAT 9022286
which claims benefit of 61/794,891 03/15/2013

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: 11/30/2021
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 17/528,073**
Projected Publication Date: Not Applicable
Non-Publication Request: No
Early Publication Request: No
Title

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Preliminary Class

235

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

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

136197 7590 02/13/2023

David Wyatt c/o Murabito, Hao & Barnes
111 North Market Street
Suite 700
San Jose, CA 95113

EXAMINER	
LEE, SEUNG H	
ART UNIT	PAPER NUMBER
2876	

DATE MAILED: 02/13/2023

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/528,073	11/16/2021	David WYATT	WYAT-0002.USD1C1C1C1C1C	4809

TITLE OF INVENTION: MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

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	05/15/2023

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.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

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

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

136197 7590 02/13/2023
David Wyatt c/o Murabito, Hao & Barnes
111 North Market Street
Suite 700
San Jose, CA 95113

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.
17/528,073	11/16/2021	David WYATT	WYAT-0002.USD1C1C1C1C1C	4809

TITLE OF INVENTION: MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

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	05/15/2023

EXAMINER	ART UNIT	CLASS-SUBCLASS
LEE, SEUNG H	2876	235-380000

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) ❑ Advance Order - # of Copies _____

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

❑ Electronic Payment via EFS-Web ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

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

❑ Applicant certifying micro entity status. See 37 CFR 1.29

❑ Applicant asserting small entity status. See 37 CFR 1.27

❑ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/528,073	11/16/2021	David WYATT	WYAT-0002.USD1C1C1C1C1C	4809

136197 7590 02/13/2023

David Wyatt c/o Murabito, Hao & Barnes
111 North Market Street
Suite 700
San Jose, CA 95113

EXAMINER	
LEE, SEUNG H	

ART UNIT	PAPER NUMBER
2876	

DATE MAILED: 02/13/2023

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.

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. 17/528,073	Applicant(s) WYATT, David	
	Examiner SEUNG H LEE	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 1/12/2023.
   ☐ 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 15-86 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some* c) ☐ None of the:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____ .

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

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

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

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

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☑ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 6 IDSs filed on 1/12/2023.
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 _____.

/SEUNG H LEE/
Primary Examiner, Art Unit 2876

DETAILED ACTION

Notice of Pre-AIA or AIA Status

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

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on January 12, 2023 has been entered.

Allowable Subject Matter

3. Claims 15-86 are allowed.

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

None of prior art teaches a method of generating and using limited-use payment information for performing a payment transaction, the method comprising: receiving an input at an electronic device, wherein the input comprises a priming operation, and, wherein the electronic device comprises: a processor; a touch-screen display coupled to the processor; and a near field communications (NFC) interface coupled to the processor; responsive to said priming operation, readying said device to perform a payment transaction by an identified user; receiving a payment request for the payment transaction at said electronic device; displaying, on the touch-screen display, information reflecting the payment request, and an image representing a selected

issued payment account; dynamically generating, by the processor, limited-use payment information; wherein said limited-use payment information is dynamically generated based on a per-transaction sequential parameter originating from the electronic device; using said limited-use payment information in connection with the payment transaction in place of issued payment information associated with said selected issued payment account; transmitting said limited-use payment information from said electronic device via said NFC interface for receipt by an NFC recipient.; responsive to the transmitting the limited-use payment information, receiving via the NFC interface information reflecting a status of said payment transaction; and displaying the status of said payment transaction via said touch-screen display, and a system of the same as set forth in the claims.

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

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to SEUNG H LEE whose telephone number is (571)272-2401. The examiner can normally be reached 7-4:00PM.

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, Steven Paik can be reached on 571-272-2404. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of 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.

/SEUNG H LEE/
Primary Examiner, Art Unit 2876

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/528,073	WYATT, David
	Examiner	Art Unit
	SEUNG H LEE	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	11/05/2022	01/28/2023							
1	15	=	=							
2	16	=	=							
7	17	=	=							
8	18	=	=							
9	19	=	=							
10	20	=	=							
11	21	=	=							
12	22	=	=							
13	23	=	=							
14	24	=	=							
15	25	=	=							
16	26	=	=							
17	27	=	=							
23	28	=	=							
24	29	=	=							
25	30	=	=							
26	31	=	=							
3	32	=	=							
18	33	=	=							
4	34	=	=							
27	35	=	=							
28	36	=	=							
21	37	=	=							
22	38	=	=							
5	39	=	=							
6	40	=	=							
19	41	=	=							
20	42	=	=							
29	43	=	=							
30	44	=	=							
31	45	=	=							
32	46	=	=							
33	47	=	=							
34	48	=	=							
35	49	=	=							
36	50	=	=							
38	51	=	=							
37	52	=	=							
39	53	=	=							
40	54	=	=							
41	55	=	=							
44	56	=	=							

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/528,073	WYATT, David
	Examiner	**Art Unit**
	SEUNG H LEE	2876

CLAIM		DATE								
Final	Original	11/05/2022	01/28/2023							
42	57	=	=							
43	58	=	=							
45	59	=	=							
46	60	=	=							
47	61	=	=							
48	62	=	=							
49	63	=	=							
50	64	=	=							
51	65	=	=							
52	66	=	=							
53	67	=	=							
54	68	=	=							
55	69	=	=							
56	70	=	=							
57	71	=	=							
60	72	=	=							
61	73	=	=							
58	74	=	=							
59	75	=	=							
62	76	=	=							
63	77	=	=							
64	78	=	=							
65	79	=	=							
66	80	=	=							
67	81	=	=							
68	82	=	=							
69	83	=	=							
70	84	=	=							
71	85	=	=							
72	86	=	=							

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/528,073	WYATT, David
	Examiner	Art Unit
	SEUNG H LEE	2876

CPC - Searched*		
Symbol	Date	Examiner
G06Q20/341 or G06K19/06206 or G06K19/0716 or G06K19/07749 or G06Q20/06 or G06Q20/065 or G06Q20/223 or G06Q20/24 or G06Q20/346 or G06Q20/347 or G06Q20/352 or G06Q20/3827 or G06Q20/385 or G06Q20/4012 or G06Q20/409 or G07F7/0873 or G07F19/00	01/28/2023	sl

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
PE2E	01/28/2023	sl
14/680979,14/981757,15/701261,16/459150, 17/075637 (parent cases)	01/28/2023	sl
NPL	11/05/2022	sl

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
	same as above	01/28/2023	sl

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/528,073	WYATT, David
	Examiner	Art Unit
	SEUNG H LEE	2876

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/528,073	WYATT, David
	Examiner	**Art Unit**
	SEUNG H LEE	2876

CPC						
Symbol					**Type**	**Version**
G06Q	/	20	/	341	F	2013-01-01
G07F	/	19	/	00	I	2013-01-01
G06Q	/	20	/	06	I	2013-01-01
G06Q	/	20	/	223	I	2013-01-01
G06Q	/	20	/	347	I	2013-01-01
G06Q	/	20	/	385	I	2013-01-01
G07F	/	7	/	0873	I	2013-01-01
G06K	/	19	/	06206	I	2013-01-01
G06K	/	19	/	0716	I	2013-01-01
G06K	/	19	/	07749	I	2013-01-01
G06Q	/	20	/	24	I	2013-01-01
G06Q	/	20	/	352	I	2013-01-01
G06Q	/	20	/	409	I	2013-01-01
G06Q	/	20	/	065	I	2013-01-01
G06Q	/	20	/	346	I	2013-01-01
G06Q	/	20	/	3827	I	2013-01-01
G06Q	/	20	/	4012	I	2013-01-01

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

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	72	
/SEUNG H LEE/ Primary Examiner, Art Unit 2876	28 January 2023	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

U.S. Patent and Trademark Office — Part of Paper No.: 20230126

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/528,073	WYATT, David
	Examiner	**Art Unit**
	SEUNG H LEE	2876

INTERNATIONAL CLASSIFICATION					
CLAIMED					
G06Q20/34	/	20	/	34	

NON-CLAIMED					
	/		/		

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**

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

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	72	
/SEUNG H LEE/ Primary Examiner, Art Unit 2876	28 January 2023	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

U.S. Patent and Trademark Office — Part of Paper No.: 20230126

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/528,073	WYATT, David
	Examiner	**Art Unit**
	SEUNG H LEE	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	15	14	24	18	33	20	42	38	51	46	60	55	69	64	78
2	16	15	25	4	34	29	43	37	52	47	61	56	70	65	79
7	17	16	26	27	35	30	44	39	53	48	62	57	71	66	80
8	18	17	27	28	36	31	45	40	54	49	63	60	72	67	81
9	19	23	28	21	37	32	46	41	55	50	64	61	73	68	82
10	20	24	29	22	38	33	47	44	56	51	65	58	74	69	83
11	21	25	30	5	39	34	48	42	57	52	66	59	75	70	84
12	22	26	31	6	40	35	49	43	58	53	67	62	76	71	85
13	23	3	32	19	41	36	50	45	59	54	68	63	77	72	86

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	72	
/SEUNG H LEE/ Primary Examiner, Art Unit 2876	28 January 2023	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

U.S. Patent and Trademark Office — Part of Paper No.: 20230126

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

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. 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	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

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]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	1	"Isis NFC-payment from SXSW 2012," YouTube, https://www.youtube.com/watch?v=Z2MOAtUhR7k, March 10, 2012, pp. 1- 2.	
	2	"Isis NFC-payment from SXSW 2012," Transcript of YouTube, https://www.youtube.com/watch?v=Z2MOAtUhR7k, March 10, 2012, pp. 1- 3.	
	3	"NFC - Google Wallet and More - EE Times - Mobile World Congress," YouTube, https://www.youtube.com/watch?v=AgSk7L6HhVw, March 6, 2012, pp. 1-3.	
	4	"NFC - Google Wallet and More - EE Times - Mobile World Congress," Transcript of YouTube, https://www.youtube.com/watch?v=AgSk7L6HhVw, March 6, 2012, pp. 1-8.	
	5	"Paying With Google Wallet," YouTube, https://www.youtube.com/watch?v=jTeilSlzBPQ, February 6, 2012, pp. 1-2.	
	6	"Seinfeld - Google Wallet," YouTube, https://www.youtube.com/watch?v=baaCvgTRYsU, June 14, 2013, pp. 1-2.	
	7	"Technology: Google Wallet - The New York Times," YouTube, https://www.youtube.com/watch?v=I8JOT6ban7o, September 23, 2011, pp. 1-2.	
	8	"Using Google Wallet in McDonald's!," YouTube, https://www.youtube.com/watch?v= 1p6co4YIvbA, September 14, 2012, pp. 1-2.	
	9	"Virtual terminal- #1 storing credit card data with tokenization," YouTube, https://www.youtube.com/watch?v=eSXIlGbACew, February 28, 2011, pp. 1-3.	
	10	"What is Google Wallet?," YouTube, https://www.youtube.com/watch?v=iuvyN4iZiP8, August 9, 2011, pp. 1-3.	
	11	"What is Tokenization?," YouTube, https://www.youtube.com/watch?v=ypm5FFfEN34, January 17, 2011, pp. 1-3.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	12	"How Credit Card Number Tokenization can Reduce PCI Compliance Stress - File 1 of 3," YouTube, https://www.youtube.com/watch?v=FHD5XzAIKDI, Jul 28, 2009, pp. 1-3.	
	13	"How Credit Card Number Tokenization can Reduce PCI Compliance Stress - File 1 of 3," Transcript of YouTube, https://www.youtube.com/watch?v=FHD5XzAIKDI, Jul 28, 2009, pp. 1-12.	
	14	"HOW CREDIT CARD NUMBER "TOKENIZATION" CAN REDUCE PCI COMPLIANCE STRESS - File 2 of 3," YouTube, https://www.youtube.com/watch?v=t-fWpcLdb3o, Jul 28, 2009, pp. 1-3.	
	15	"HOW CREDIT CARD NUMBER "TOKENIZATION" CAN REDUCE PCI COMPLIANCE STRESS - File 2 of 3," Transcript of YouTube, https://www.youtube.com/watch?v=t-fWpcLdb3o, Jul 28, 2009, pp. 1-12.	
	16	"HOW CREDIT CARD NUMBER "TOKENIZATION" CAN REDUCE PCI COMPLIANCE STRESS- File 3 of 3," YouTube, https://www.youtube.com/watch?v=_CdoKEuEB9s, Jul 28, 2009, pp. 1-3.	
	17	"HOW CREDIT CARD NUMBER "TOKENIZATION" CAN REDUCE PCI COMPLIANCE STRESS- File 3 of 3," Transcript of YouTube, https://www.youtube.com/watch?v=_CdoKEuEB9s, Jul 28, 2009, pp. 1-8.	
	18	"Caixer contactless lacaixa," YouTube, https://www.youtube.com/watch?v=lt2CpMcxQC4, April 4, 2011, pp. 1-2.	
	19	"Understanding Proximity Sensors - T-Mobile," YouTube, https://www.youtube.com/watch?v=npD48agt0xY, January 2010, pp. 1-2.	
	20	"Understanding Proximity Sensors - T-Mobile," YouTube, https://www.youtube.com/watch?v=npD48agt0xY, January 2010, page 1.	
	21	"Understanding Proximity Sensors - T-Mobile," Transcript of YouTube, https://www.youtube.com/watch?v=npD48agt0xY, January 2010, pp. 1-2.	
	22	"Google I/O 2012 - The Sensitive Side of Android," YouTube, https://www.youtube.com/watch?v=Q0V_Id7iNw4, June 29, 2012, pp. 1-2.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	23	"Google Wallet Overview," YouTube, https://www.youtube.com/watch?v=VuFVsaFCzsw, August 1, 2012, page 1.	
	24	"Google Wallet Overview," Transcript of YouTube, https://www.youtube.com/watch?v=VuFVsaFCzsw, August 1, 2012, pp. 1-2.	
	25	"Android 4.0 APIs | Android Developers," mit.edu, https://stuff.mit.edu/afs/sipb/project/android/docs/about/versions/android-4.0.html, 2011, pp. 1-23.	
	26	"EMV Integrated Circuit Card Specifications for Payment Systems, Book 2, Security and Key Management, Version 4.3," EMVCo, November 2011, pp. 1-174.	
	27	"Exploring Google Wallet using the secure element interface," nelenkov.blogspot.com, August 27, 2012, pp. 1-20.	
	28	GARSIDE, "Google Wallet mobile payments system launched to public," The Guardian, https://www.theguardian.com/technology/2011/sep/19/google-wallet-available-public, September 19, 2011, pp. 1-5.	
	29	PURDY, "How to grab a screenshot from iPhone, Android, and nearly any other smartphone," Computer World, April 20, 2012, pp. 1-6.	
	30	"Maximum failed passcode attempts in restrictions - what happens?," Apple Community, https://discussions.apple.com/thread/3690633, January 2012, pp. 1-3.	
	31	"Simplify, Organize & Pay with Loop by Will Graylin & George Wallner," Kickstarter, March 2019, pp. 1-13.	
	32	"Hands-on with ISIS Mobile Wallet," YouTube, https://www.youtube.com/watch?v=eOMqvGVKjmM, March 10, 2012, page 1.	
	33	"EMV Solutions," Paragon Application Systems, https://web.archive.org/web/20120818221214/http://www.paragonedge.com/solutions/emv-solutions.html, August 18, 2012, page 1.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	34	SULLIVAN, "The Changing Nature of U.S. Card Payment Fraud: Industry and Public Policy Options," Economic Review, Federal Reserve Bank of Kansas City, Second Quarter 2010, ProQuest Information and Learning, Vol. 95, No. 2, pp 101-133.
	35	"EMV Integrated Circuit Card Specifications for Payment Systems, Book 1, Application Independent ICC to Terminal Interface Requirements, Version 4.3," EMVCo, November 2011, pp. 1-189.
	36	"EMV Contactless Specifications for Payment Systems, Book B, Entry Point Specification, Version 2.1," EMVCo, March 2011, pp. 1-50.
	37	ETHERINGTON, "Android Pay Is Real, And Will Give Developers The Reins As An API," TechCrunch, https://techcrunch.com/2015/03/02/android-pay-is-real-and-will-give-developers-the-reins-as-an-api, March 2, 2015, pp. 1-7.
	38	"PCI DSS Version 2.0 Information Supplement: PCI DSS Tokenization Guidelines," PCI Security Standards Council, pcisecuritystandards.org, https://listings.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf., v 2.0, August 2011, pp. 1-23.
	39	"EMVCo Updates Payment Tokenisation Specification to Introduce 'Payment Account Reference,'" www.emvco.com, March 29, 2016, pp. 1-2.

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

EXAMINER SIGNATURE

Examiner Signature	/SEUNG H LEE/	Date Considered	01/28/2023

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

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	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

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

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. 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	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

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]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	1	"EMVCO Publishes Technical Framework for its Payment Tokenisation Specification," EMVCO, March 11, 2014, pp. 1-2.	
	2	"Encryption and Tokenization: Which is best for your business?," Townsend Security, 2010, pp. 1-4.	
	3	MOLEN, "Engadget Primed: What is NFC, and why do we care?," Engadget, June 10, 2011, pp. 1-11.	
	4	"Exploring Google Wallet using the secure element interface," nelenkov.blogspot.com, August 27, 2012, pp. 1-11.	
	5	"Financial Cryptography," 5th International Conference, FC 2001 Proceedings, Grand Cayman, British West Indies, February 19-22, 2001, Paul F. Syverson (Editor), pp. 1-57.	
	6	"Gemalto to Provide Isis Mobile Commerce Platform with Trusted Service Manager (TSM) Solution," Business Wire, December 12, 2011, pp. 1-3.	
	7	"Google Checkout checks out, replaced by Google Wallet," Android Community, November 17, 2011, page 1.	
	8	"Google Checkout HTML API Short Attribute Reference," Google Checkout, Google Code (archive.org), March 27, 2012, pp. 1-4.	
	9	"Google Commerce: Building one wallet: Google Checkout is transitioning to Google Wallet," commerce.googleblog.com, November 16, 2011, pp. 1-2.	
	10	"Google Prepaid Cards," Wallet Help, Google (archive.org), October 3, 2012, page 1.	
	11	CLARK, "Google Unveils first Android NFC phone - but Nexus S is limited to tag reading only for now," NFC World, December 7, 2010, pp. 1-4.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	12	"Google Wallet launches officially on Nexus S 4G," Android Community, September 19, 2011, pp. 1-2.	
	13	GARSIDE, "Google Wallet mobile payments system launched to public," The Guardian, September 19, 2011, page 1.	
	14	BOULTON, "Google Wallet Mobile Payments Coming to New York, Francisco; Google Wallet will launch this summer to enable consumers to pay for goods by tapping their Samsung Nexus 2 4G Android phones at NFC-fitted sales terminals at Subway, Macy's and other retailers," eWeek.com, May 26, 2011, pp. 1-2.	
	15	FINGAS, "Google Wallet reaches the web, reminds most of us that it exists," Engadget, October 4, 2012, pp. 1-6.	
	16	RAPHAEL, "Google's Eric Schmidt spills clues about Android Gingerbread," ComputerWorld, November 15, 2010, pp. 1-3.	
	17	"Handset makers line up behind Isis NFC payment platform," Old GigaOm, September 27, 2011, pp. 1-2.	
	18	"How it Works," Wallet Help, Google (archive.org), March 12, 2013, page 1.	
	19	"How to find out IMEI number on Google Nexus S phone," Tech Notes Desk, January 10, 2013, page 1.	
	20	"La Caixa," Annual Report, 2010, Barcelona, Spain, pp. 1-190.	
	21	"INSIDE Contactless to Equip KTFMobile Payment Project Mobile Phones; Korean Manufacturer Confirms INSIDE's NFC Maturity by Embedding MicroRead into LG Electronics and Samsung Electronics Mobile Phones for its Mobile Payment Project," Business Wire, July 16, 2007, pp. 1-2.	
	22	CLUCKEY, "Is a contactless ATM inevitable? Bank of America seems to think so; the FI has filed a patent application for a 'Contactless Automated Teller Machine,'" ATM Marketplace, September 20, 2012, pp. 1-3.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	23	"Isis™ Launches in Austin and Salt Lake City; As Many as 20 Isis Ready™ Handsets to Be Available by Year End," Business Wire, October 22, 2012, page 1.	
	24	PEREZ, "Isis Revealed: Carrier-Led Mobile Payments Venture Shows Off Its New App, Announces Banking Partners," TechCrunch, February 27, 2012, pp. 1-6.	
	25	SADEWO, "Isis to officially launch on Oct 22, more supported devices announced," androidauthority.com, October 18, 2012, pp. 1-2.	
	26	"MasterCard Approves NFC Phones from HTC, Intel, LG Electronics, Nokia, RIM, Samsung Electronics and Sony," Professional Services Close-Up, May 10, 2012, Close-Up Media, Inc., pp. 1-2.	
	27	"MASTERCARD INC, FORM 10-K (Annual Report)," Filed February 28, 2007, for the Period Ending December 31, 2006, pp. 1-204.	
	28	"MasterCard, Visa and American Express Propose New Global Standard to Make Online and Mobile Shopping Simpler and Safer," Global Hub, Engagement Bureau, Press Release, October 1, 2013, pp. 1-2.	
	29	"Fact Sheet: Mobile Commerce: A New Way to Pay: MasterCard Mobile Commerce," May 26, 2011, pp. 1-4.	
	30	"McDonald's testing e-payment system," USA Today, May 29, 2001, pp. 1-3.	
	31	"Mobile Contactless Payments Trialled Live at Mobile World Congress 2010; GSMA, Samsung, Telefónica and Visa, with Giesecke & Devrient, Ingenico, ITN International and La Caixa, collaborate across industries to give Congress attendees an opportunity to experience NFC," Business Wire, February 15, 2010, pp. 1-3.	
	32	"Mobile Payment Bringing value to payments on mobile," Gemalto, November 2011, pp. 1-4.	
	33	WOO, "Mobile PayPass Meets Cloud in Google Wallet," Global Hub, August 1, 2012, pp. 1-2.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	34	HEUN, "Mobile Wallet Consortium Strives Cautiously In 2012; The telco joint effort proceeded more slowly than expected, but its leaders maintain that the mobile wallet business is big enough for lots of players," Section: MOBILE: ISIS, January 1, 2013, Page 47, Vol. 2, No. 1, SouceMedia LLC d/b/a Arizent, pp. 1-3.
	35	BELL, "Mobile's Gains Prompt More Banks To Move Beyond Cards For ATM Access," Payments Source, Section: DEBIT: Vol. 1, No. 1, May 12, 2011, pp. 1-4.

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

EXAMINER SIGNATURE

Examiner Signature	/SEUNG H LEE/	Date Considered	01/28/2023

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

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	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

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

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. 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	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

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]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	1	"Standing Document (SD1): WG8 Projects: ISO/IEC 14443, Proximity Cards (PICCS)," ISO/IEC JTC1/SC17/WG8 (archive.org), October 25, 2010, pp. 1-6.	
	2	"Telefonica O2 Czech Republic prepares NFC payments," DmEurope, March 25, 2011, page 1.	
	3	MARKKANEN, "Telefonica, Samsung to Pilot SIM-Based NFC Payment Solution in Spain," IHS Global Insight, February 15, 2010, pp. 1-2.	
	4	"The Mobile Payments and NFC Landscape: A U.S. Perspective," Smart Card Alliance, September 2011, pp. 1-53.	
	5	"Tokenization Guidance: How to reduce PCI compliance costs, Version 1.0," Securosis, December 10, 2011, pp. 1-31.	
	6	"Tokenization: What's Next After PCI," RSA, 2012, pp. 1-8.	
	7	SEIFERT, "Verizon won't offer Google Wallet for the Galaxy Nexus because it uses a 'secure element'," The Verge, December 10, 2012, pp. 1-2.	
	8	"Visa and Google Sign Licensing Deal to Boost Mobile Payment Adoption," Visa, September 19, 2011, pp. 1-2.	
	9	"Visa Best Practices for Tokenization Version 1.0," Visa, July 14, 2010, pp. 1-4.	
	10	CROSMAN, "Visa Certifies BlackBerry, Samsung And LG Phones For PayWave NFC Payments," Payments Source, January 10, 2012, pp. 1-2.	
	11	"Visa Completes Acquisition of Rambus Payments Portfolio," Business Wire, October 22, 2019, page 1.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	12	"Convenience for customers. Profits for you," Visa PayWave (archive.org), January 2013, pp. 1-2.	
	13	"Verizon User Manual: Samsung Galaxy SIII," Verizon, January 2012, pp. 1-204.	
	14	"World leader in proven and efficient cards for EMV deployment," Gemalto, February 2010, pp. 1-2.	
	15	BECKER, "29C3: A Rambling Walk Through an EMV Transaction (EN)," YouTube, https://www.youtube.com/watch?v=VdNm9JJmCzg, December 30, 2012, pp. 1-2.	
	16	"ARQC and ARPC Generation and Validation," YouTube, https://www.youtube.com/watch?v=I1XTn175FFk, Paragon Application Systems, July 25, 2012, pp. 1-3.	
	17	"CardVault by 3Delta Systems - Securing Credit Card Payments for B2B and B2G through Tokenization," YouTube, https://www.youtube.com/watch?v=h3zuiLiF51k, February 1, 2010, pp. 1-3.	
	18	"CardVault by 3Delta Systems - Securing Credit Card Payments for B2B and B2G through Tokenization," Transcript of YouTube, https://www.youtube.com/watch?v=h3zuiLiF51k, February 1, 2010, pp. 1-3.	
	19	"Credit Card Processing with EPX BuyerWall Tokenization," YouTube, https://www.youtube.com/watch?v=_7E5hj9li4g, December 21, 2010, pp. 1-3.	
	20	"Credit Card Processing with EPX BuyerWall Tokenization," Transcript of YouTube, https://www.youtube.com/watch?v=_7E5hj9li4g, December 21, 2010, pp. 1-7.	
	21	"Find out how PayPal works," YouTube, https://www.youtube.com/watch?v=dn42Y-2uFQM, March 14, 2012, pp. 1-2.	
	22	"Google checkout," YouTube, https://www.youtube.com/watch?v=-UeYkxePW2c, June 29, 2006, pp. 1-2.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	23	"See Google I/O 2011: Google Checkout: A Foundation For Payments," YouTube, https://www.youtube.com/watch?v=7ts7Lkykn0E, May 13, 2011, pp. 1-2.	
	24	"See Google I/O 2011: Google Checkout: A Foundation For Payments," Transcript of YouTube, https://www.youtube.com/watch?v=7ts7Lkykn0E, May 13, 2011, pp. 1-64.	
	25	"Google I/O 2011: How to NFC," YouTube, https://www.youtube.com/watch?v=49L7z3rxz4Q, May 10, 2011, pp. 1-2.	
	26	"Google I/O 2011: How to NFC," Transcript of YouTube, https://www.youtube.com/watch?v=49L7z3rxz4Q, May 10, 2011, pp. 1-62.	
	27	"Google I/O 2012: Introducing Google Wallet Cloud APIs," YouTube, https://www.youtube.com/watch?v=tpEGuSwv1fY, June 29, 2012, pp. 1-3.	
	28	"Google I/O 2012: Introducing Google Wallet Cloud APIs," Transcript of YouTube, https://www.youtube.com/watch?v=tpEGuSwv1fY, June 29, 2012, pp. 1-40.	
	29	"Google Nexus S by Samsung at CES 2011," YouTube, https://www.youtube.com/watch?v=5ZjtXH9S9KM, January 11, 2011, pp. 1-2.	
	30	"Google Nexus S by Samsung at CES 2011," Transcript of YouTube, https://www.youtube.com/watch?v=5ZjtXH9S9KM, January 11, 2011, pp. 1-2.	
	31	"Google Payments Live - Google Wallet updates," YouTube, https://www.youtube.com/watch?v=1pxkQ1mFjNA, August 23, 2012, pp. 1-2.	
	32	"Google Payments Live - Google Wallet updates," Transcript of YouTube, https://www.youtube.com/watch?v=1pxkQ1mFjNA, August 23, 2012, pp. 1-40.	
	33	"Google Wallet Demonstration," YouTube, https://www.youtube.com/watch?v=6tBAB5ls5vM, May 26, 2011, pp. 1-2.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	34	"Google Wallet Demonstration," Transcript of YouTube, https://www.youtube.com/watch?v=6tBAB5ls5vM, May 26, 2011, pp. 1-2.	
	35	"Google Wallet Hands-On - Engadget," YouTube, https://www.youtube.com/watch?v=5s9wYEkRAgs, May 26, 2011, pp. 1-3.	
	36	"Google Wallet - How to Setup and Use this Exciting NFC Technology," YouTube, https://www.youtube.com/watch?v=_ay1FfLCsHs, July 26, 2012, pp. 1-3.	
	37	"Google Wallet - How to Setup and Use this Exciting NFC Technology," Transcript of YouTube, https://www.youtube.com/watch?v=_ay1FfLCsHs, July 26, 2012, pp. 1-7.	
	38	"Google Wallet Make Your Phone Your Wallet by Google," YouTube, https://www.youtube.com/watch?v=qRVQTQIJV0g, February 18, 2013, pp. 1-2.	
	39	"Google Wallet Make Your Phone Your Wallet by Google," Transcript of YouTube, https://www.youtube.com/watch?v=qRVQTQIJV0g, February 18, 2013, page 1.	
	40	"Google Wallet Product Launch," YouTube, https://www.youtube.com/watch?v=am8t6iZ7up0, May 27, 2011, pp. 1-3.	
	41	"Google Wallet Product Launch," Transcript of YouTube, https://www.youtube.com/watch?v=am8t6iZ7up0, May 27, 2011, pp. 1-56.	
	42	"Google Wallet Walkthrough," YouTube, https://www.youtube.com/watch?v=xmbRSXYdFFs, February 13, 2012, pp. 1-2.	
	43	"How does Google Wallet work? Really well!," YouTube, https://www.youtube.com/watch?v=jY2p-pNkjHA, December 7, 2011, pp. 1-2.	
	44	"How does Google Wallet work? Really well!," Transcript of YouTube, https://www.youtube.com/watch?v=jY2p-pNkjHA, December 7, 2011, pp. 1-2.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	45	"How Does PayPal Work?," YouTube, https://www.youtube.com/watch?v=MdrPOCCFQ2k, July 24, 2012, pp. 1-2.	
	46	"How To Use Google Wallet On Android," YouTube, https://www.youtube.com/watch?v=6DeiEVBIBcs, October 28, 2011, pp. 1-2.	
	47	"How To Use Google Wallet On Verizon Galaxy Nexus - Pocketnow," YouTube, https://www.youtube.com/watch?v=AZ8t757ZfUs, April 20, 2012, pp. 1-2.	

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

EXAMINER SIGNATURE

Examiner Signature	/SEUNG H LEE/	Date Considered	01/28/2023

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

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	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L1	30843	(G06Q20/341 or G06Q20/4012 or G06Q20/3827 or G06Q20/346 or G06Q20/065 or G06Q20/409 or G06Q20/352 or G06Q20/24 or G06K19/07749 or G06K19/0716 or G06K19/06206 or G07F7/0873 or G06Q20/385 or G06Q20/347 or G06Q20/223 or G06Q20/06 or G07F19/00).cpc.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/04/27 12:21 PM
L2	1	nfc same transaction same payment same logo same limited same issuer	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/04/27 12:22 PM
L4	311	monitor$4 same master same node same wireless same sensor	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/01 12:55 PM
L5	18	L4.clm.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/01 12:55 PM
L6	107	L4 same (slave peripheral)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/01 12:56 PM
L7	7	L6.clm.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/01 12:56 PM
L8	17	("20030018927"|"9860688"|"20180165568"|"20150154531"|"9189226"|"20100082870"|"20170039666"|"20180046964"|"9824329"|"20080239282"|"9182231"|"20130107770"|"20070049291"|"6614392"|"20100299401"|"20160233927").PN.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/01 12:58 PM
L9	9	L6 same (environment$4 temperature)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/01 01:00 PM
L10	9	("20130250357"|"20150324745"|"7177054"|"8292173"|"7048194"|"7299990"|"7540603"|"8072620"|"20100096181").PN.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/01 01:04 PM

L11	39	("2015/0324745").URPN.	(USPAT)	OR	OFF	OFF	2020/05/02 08:57 AM
L12	35	label same wireless same master same (slave peripheral)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/02 09:00 AM
L13	39	"517508"	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/02 09:19 AM
L14	6	(("10339520") or ("9760884") or ("9224083") or ("9022286")).PN.	(US-PGPUB; USPAT; USOCR; EPO; JPO)	OR	OFF	OFF	2020/05/04 05:07 AM
L15	55	nfc same transaction same payment same limited same issuer	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/04 05:07 AM
L16	5	L15 same proximity	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/04 05:08 AM
L17	30909	(G06Q20/341 or G06Q20/4012 or G06Q20/3827 or G06Q20/346 or G06Q20/065 or G06Q20/409 or G06Q20/352 or G06Q20/24 or G06K19/07749 or G06K19/0716 or G06K19/06206 or G07F7/0873 or G06Q20/385 or G06Q20/347 or G06Q20/223 or G06Q20/06 or G07F19/00).cpc.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/05 08:24 AM
L18	129	L17 and (nfc same select$4 same payment same limit$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/05 08:25 AM
L19	43	L17 and (nfc same select$4 same payment same limit$4 same display$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/05 08:26 AM
L20	6	(("10339520") or ("9760884") or ("9224083") or ("9022286")).PN.	(US-PGPUB; USPAT; USOCR; EPO; JPO)	OR	OFF	OFF	2020/05/05 08:33 AM
L21	0	L20 and (nfc same select$4 same payment same limit$4 same display$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/05 08:33 AM
L22	109	(nfc same select$4 same payment same limit$4 same display$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/05 08:33 AM
L23	94	L22 same (mobile portable)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/05 08:34 AM
L24	4186	dynamic same credit	(US-PGPUB; USPAT;	OR	OFF	OFF	2020/05/05

		same card	EPO; JPO)				08:35 AM
L25	7	L22 and L24	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/05 08:35 AM
L26	23	("20020073025" | "20030101137" | "20070278290" | "20100057553" | "20100082487" | "20110137748" | "20110302089" | "20120006891" | "20140052607" | "20140129422" | "20140143037" | "20140195324" | "20140249941" | "20140279474" | "20150058145" | "20160027005" | "20160086161" | "20160162857" | "20160162887" | "20160335619" | "6633223" | "9292849" | "9489671").PN.	(US-PGPUB; USPAT; USOCR)	OR	OFF	OFF	2020/05/05 08:38 AM
L27	6	("20040168067" | "20090276347" | "20110016047" | "20120173311" | "20130159186" | "6163771").PN.	(US-PGPUB; USPAT; USOCR)	OR	OFF	OFF	2020/05/05 08:39 AM
L28	4	(("10339520") or ("9760884") or ("9224083") or ("9022286")).PN.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2020/05/05 09:39 AM
L29	1	L28 and (respons$4 same nfc same generat$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/05 09:40 AM
L30	31288	(G06Q20/341 or G06Q20/4012 or G06Q20/3827 or G06Q20/346 or G06Q20/065 or G06Q20/409 or G06Q20/352 or G06Q20/24 or G06K19/07749 or G06K19/0716 or G06K19/06206 or G07F7/0873 or G06Q20/385 or G06Q20/347 or G06Q20/223 or G06Q20/06 or G07F19/00).cpc.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/06/21 02:19 PM
L31	135	L30 and (nfc same	(US-PGPUB; USPAT;	OR	OFF	OFF	2020/06/21

		select$4 same payment same limit$4)	EPO; JPO)				02:19 PM
L32	112	L30 and (nfc same payment same limit$4 same approv$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/06/21 02:20 PM
L33	7	L30 and (nfc same payment same limit$4 same approv$4 same interface)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/06/21 02:20 PM
L34	10	L30 and (nfc same select$4 same payment same limit$4 same approv$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/06/21 02:28 PM
L35	36	(nfc same select$4 same payment same limit$4 same approv$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/06/21 02:29 PM
L36	6	(("10339520") or ("9760884") or ("9224083") or ("9022286")).PN.	(US-PGPUB; USPAT; USOCR; EPO; JPO)	OR	OFF	OFF	2020/06/21 02:30 PM
L37	51	"075637"	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/28 10:02 PM
L38	1	"10810579".pn.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/28 10:03 PM
L39	35569	(G06Q20/341 or G06K19/07749 or G06Q20/347 or G06Q20/06 or G06Q20/409 or G06Q20/4012 or G06Q20/346 or G06Q20/3827 or G06K19/0716 or G07F19/00 or G06Q20/223 or G06Q20/24 or G06Q20/385 or G07F7/0873 or G06K19/06206 or G06Q20/065 or G06Q20/352).cpc.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 06:36 AM
L40	6275	payment same transaction same (limit$4 tempora$6) same generat$4	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 06:39 AM
L41	1592	L39 and L40	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 06:39 AM
L42	862	L40 same issuer same account	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 06:40 AM
L43	265	L39 and L42	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 06:40 AM
L44	30	L42 same wireless$4	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 06:42 AM

L45	2	("8851370"|"9646301").PN.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:07 AM
L46	31	("10013693" | "20060032908" | "20080223937" | "20100260388" | "20110140841" | "20130048712" | "20130124292" | "20130297509" | "20140052632" | "20140279555" | "20180240106" | "6631849" | "6641050" | "7128274" | "7202825" | "7360688" | "7784692" | "7793851" | "7841539" | "8577813" | "8639629" | "8702007" | "8768838" | "8856539" | "9022286" | "9100826" | "9224083" | "9430765" | "9530137" | "9536238" | "9760884").PN.	(US-PGPUB; USPAT; USOCR)	OR	OFF	OFF	2021/09/29 07:08 AM
L47	229	("7128274").URPN.	(USPAT)	OR	OFF	OFF	2021/09/29 07:16 AM
L48	369	("7793851").URPN.	(USPAT)	OR	OFF	OFF	2021/09/29 07:22 AM
L49	77	L40 and L48	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:22 AM
L50	47	L39 and L49	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:22 AM
L51	130	("2013/0159186").URPN.	(USPAT)	OR	OFF	OFF	2021/09/29 07:36 AM
L52	41	(nfc same select$4 same payment same limit$4 same approv$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:48 AM
L53	1218	(select$4 same payment same limit$4 same approv$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:48 AM
L54	267	L39 and L53	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:48 AM
L55	346	L53 same generat$4	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:49 AM
L56	2785621	L55 sane dynamic$6	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:49 AM
L57	48	L55 same dynamic$6	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:50 AM
L58	11	L55 same static$4	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:51 AM
L59	543	("10043164" | "10075437" | "10129648" |	(US-PGPUB; USPAT; USOCR)	OR	OFF	OFF	2021/09/29 08:20 AM

		"10133979" | "10217105" | "20010010723" | "20010029485" | "20010034702" | "20010054003" | "20020078345" | "20020093530" | "20020100808" | "20020120583" | "20020152116" | "20020153424" | "20020165827" | "20030023554" | "20030034873" | "20030055727" | "20030078882" | "20030167350" | "20030208449" | "20040015958" | "20040039919" | "20040127256" | "20040215674" | "20040230799" | "20050044367" | "20050075985" | "20050081038" | "20050138387" | "20050156026" | "20050160049" | "20050195975" | "20050247797" | "20060006230" | "20060040726" | "20060041402" | "20060044153" | "20060047954" | "20060085848" | "20060136334" | "20060173985" | "20060174331" | "20060242698" | "20060280338" | "20070033642" | "20070055630" | "20070061266" | "20070061487" | "20070116292" | "20070118745" | "20070197261" | "20070224969" | "20070241182" | "20070256134" | "20070258594" | "20070278291" | "20080008315" | "20080011831" | "20080014867" |				

		"20080035738" | "20080071681" | "20080072303" | "20080086767" | "20080103968" | "20080109309" | "20080110983" | "20080120711" | "20080156873" | "20080162312" | "20080164308" | "20080207307" | "20080209543" | "20080223918" | "20080285746" | "20080308641" | "20090048026" | "20090132417" | "20090143104" | "20090171682" | "20090210308" | "20090235339" | "20090249077" | "20090282264" | "20100023449" | "20100023455" | "20100029202" | "20100030549" | "20100033310" | "20100036769" | "20100078471" | "20100082491" | "20100094754").PN. OR ("20100095130" | "20100100480" | "20100114731" | "20100192230" | "20100207742" | "20100211797" | "20100240413" | "20100257357" | "20100312634" | "20100312635" | "20110035604" | "20110060631" | "20110084132" | "20110101093" | "20110113245" | "20110125638" | "20110131415" | "20110153437" | "20110153496" | "20110208658" | "20110208965" | "20110211219" | "20110218911" | "20110238564" | "20110246780" |				

		"20110258452" | "20110280406" | "20110282785" | "20110294418" | "20110312271" | "20120009946" | "20120024947" | "20120030047" | "20120030121" | "20120047071" | "20120079281" | "20120109735" | "20120143754" | "20120150737" | "20120178366" | "20120196583" | "20120207305" | "20120209773" | "20120238206" | "20120239560" | "20120252350" | "20120254394" | "20120284194" | "20120290472" | "20120296818" | "20120316992" | "20120317035" | "20120317628" | "20130005245" | "20130008956" | "20130026229" | "20130054474" | "20130065564" | "20130080228" | "20130080229" | "20130099587" | "20130104251" | "20130106576" | "20130119130" | "20130130614" | "20130144793" | "20130171929" | "20130179351" | "20130185772" | "20130191279" | "20130200999" | "20130216108" | "20130226791" | "20130226796" | "20130232082" | "20130238894" | "20130282360" | "20130303085" | "20130304651" | "20130312082" | "20130314593" | "20130344857" | "20140002238" |				

		"20140019352" | "20140027506" | "20140032409" | "20140032410" | "20140040120" | "20140040139" | "20140040147" | "20140047235" | "20140067690" | "20140074637").PN. OR ("20140074655" | "20140081720" | "20140095227" | "20140138435" | "20140171034" | "20140171039" | "20140172700" | "20140180851" | "20140208112" | "20140214674" | "20140229375" | "20140245391" | "20140256251" | "20140258099" | "20140258113" | "20140258125" | "20140274179" | "20140279479" | "20140337235" | "20140339315" | "20140346860" | "20140365780" | "20140379361" | "20150012444" | "20150032635" | "20150071486" | "20150088757" | "20150089586" | "20150134452" | "20150140960" | "20150154595" | "20150170138" | "20150178724" | "20150186871" | "20150205379" | "20150235211" | "20150302409" | "20150317626" | "20150332266" | "20150339474" | "20150371234" | "20160012465" | "20160026997" | "20160048913" | "20160055480" | "20160057619" | "20160065370" | "20160087957"				

		"20160092696" | "20160148193" | "20160232523" | "20160239672" | "20160253651" | "20160255072" | "20160267486" | "20160277383" | "20160277388" | "20160307187" | "20160307189" | "20160314472" | "20160330027" | "20160335531" | "20160379217" | "20170004502" | "20170011395" | "20170011406" | "20170017957" | "20170017964" | "20170024716" | "20170039566" | "20170041759" | "20170068950" | "20170103388" | "20170104739" | "20170109509" | "20170109730" | "20170116447" | "20170124568" | "20170140379" | "20170154328" | "20170154333" | "20170180134" | "20170221047" | "20170230189" | "20170237301" | "20170289127" | "20170295013" | "20170316696" | "20170317834" | "20170330173" | "20170374070" | "20180034507" | "20180039986").PN. OR ("20180068316" | "20180129945" | "20180160255" | "20180191501" | "20180205712" | "20180240106" | "20180254909" | "20180268132" | "20180270214" | "20180294959" | "20180300716" | "20180302396" | "20180315050" |				

		"20180316666" | "20180322486" | "20180359100" | "20190014107" | "20190019375" | "20190036678" | "20190238517" | "4683553"	"4827113" | "4910773"	"5036461" | "5363448"	"5377270" | "5533126"	"5592553" | "5616901"	"5666415" | "5764789"	"5768373" | "5778072"	"5796827" | "5832090"	"5883810" | "5901874"	"5929413" | "5960411"	"6021203" | "6049328"	"6058373" | "6061666"	"6105013" | "6199114"	"6199762" | "6216227"	"6227447" | "6282522"	"6324271" | "6342844"	"6367011" | "6402028"	"6438550" | "6501847"	"6631197" | "6641050"	"6655585" | "6662020"	"6721706" | "6731778"	"6779115" | "6792533"	"6829711" | "6834271"	"6834795" | "6852031"	"6865547" | "6873260"	"6877656" | "6889198"	"6905411" | "6910627"	"6971031" | "6990588"	"7006986" | "7085931"	"7127605" | "7128274"	"7140550" | "7152045"	"7165727" | "7175076"	"7202773" | "7206806"	"7232073" | "7246752"	"7254569" | "7263507"	"7270276" | "7278025"	"7287692" | "7290709"	"7306143" | "7319986"	"7325132" | "7373515"	"7374099" | "7375616"	"7380710" | "7424977"	"7453439" | "7472829"	"7487357" | "7568631"	"7584153" | "7597250"	"7628322" | "7652578"	"7689832" | "7703142"	"7748609" | "7748617"	"7748636" | "7762457"	"7789302" | "7793851" | "7796013").PN. OR ("7801799"	"7801829"					

		| "7805755" | "7809643" | "7827115" | "7828214" | "7848746" | "7882553" | "7900048" | "7908216" | "7922082" | "7933589" | "7949559" | "7954716" | "7954723" | "7962369" | "7993197" | "8005426" | "8010405" | "8041954" | "8060012" | "8074877" | "8082450" | "8095113" | "8099332" | "8103249" | "8108687" | "8127143" | "8135648" | "8140010" | "8141136" | "8150321" | "8150767" | "8186602" | "8196131" | "8215563" | "8224753" | "8232879" | "8233841" | "8245292" | "8249654" | "8266451" | "8285329" | "8302872" | "8312519" | "8316237" | "8332272" | "8365988" | "8369960" | "8371501" | "8381307" | "8391719" | "8417231" | "8439271" | "8475367" | "8489112" | "8511542" | "8559872" | "8566916" | "8567670" | "8572386" | "8577810" | "8583454" | "8589335" | "8594730" | "8615468" | "8620218" | "8667285" | "8723941" | "8726405" | "8740073" | "8750514" | "8752189" | "8794509" | "8799668" | "8806592" | "8807440" | "8811892" | "8814039" | "8814052" | "8818867" | "8850538" | "8861733" | "8880027" | "8888002" | "8898088" | "8934837" | "8977569" | "8994498" | "9004365" | "9038894" | "9042814" | "9047531" | "9069976" | "9081948" | "9104853" | "9118663" | "9122964" | "9129280" | "9152832" | "9203800" | "9209867" | "9251330" | "9251518" | "9258715" | "9270337" | "9306626" | "9306942" | "9324066" | "9324067" | "9332587" | "9338622" | "9373141" | "9379841" | "9413430" | "9413768" | "9420496" | "9426132"					

		| "9432339" | "9455968" | "9473509" | "9491626" | "9553637" | "9619952" | "9635000").PN. OR ("9665858" | "9674705" | "9679286" | "9680942" | "9710804" | "9740342" | "9740988" | "9763097" | "9767329" | "9769662" | "9773151" | "9780953" | "9891823" | "9940571" | "9953323" | "9961194" | "9965756" | "9965911" | "9978058" | "RE42762").PN.					
L60	84	L40 same dynamic$6 same static$4	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 08:34 AM
L61	3	L60.clm.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 08:34 AM
L62	417	("7580898").URPN.	(USPAT)	OR	OFF	OFF	2021/09/29 08:37 AM
L63	233	L39 and L62	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 08:38 AM
L64	87	L63 and nfc	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 08:39 AM
L65	160	L63 and online	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 08:39 AM
L66	62	L64 and L65	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 08:39 AM
L67	43	(Artificial Intelligence) Similar to: 17/528,073 with 0 CPC Selections and 0 Text Selections Text: (US-20210304187-A1 OR US-11176538-B2 OR US-20220207517-A1 OR US-20190325428-A1 OR US-10810579-B2 OR US-20220270077-A1 OR US-20210027276-A1 OR US-11328286-B2 OR US-10339520-B2 OR US-10628820-B2 OR US-20220318784-A1 OR US-20160148190-A1 OR US-20170132616-A1 OR US-9430765-B2 OR US-9760884-B2 OR US-10013693-B2 OR US-20190197520-A1 OR US-20150213351-	(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, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN))	OR	ON	ON	2022/11/05 01:38 PM

		A1 OR US-20140263627-A1 OR US-20150213437-A1 OR US-9022286-B2 OR US-20180247300-A1 OR US-9224083-B2 OR US-10332101-B2 OR KR-102395069-B1 OR US-11341470-B1 OR US-20110240745-A1 OR US-10248949-B2 OR WO-2008035174-A3 OR US-20190188687-A1 OR US-5564486-A OR US-20210272091-A1 OR NL-2004464-B1 OR NL-2004464-A OR TW-200705350-A OR US-7328840-B2 OR US-10528941-B2 OR US-9830598-B2 OR WO-2006134545-A3 OR US-10984407-B2 OR US-20170109738-A1 OR US-20180005226-A1 OR US-8998096-B2 OR US-9183480-B1 OR US-20150186877-A1 OR GB-1446170-A OR WO-2018011630-A1 OR EP-3482366-A1 OR CN-111899412-A OR NL-2002671-C2).did.					
L68	35	"528073"	(US-PGPUB; USPAT; EPO; JPO)	OR	ON	ON	2022/11/05 01:45 PM
L69	39353	(G06Q20/341 OR G06K19/06206 OR G06K19/0716 OR G06K19/07749 OR G06Q20/06 OR G06Q20/065 OR G06Q20/223 OR G06Q20/24 OR G06Q20/346 OR G06Q20/347 OR G06Q20/352 OR G06Q20/3827 OR G06Q20/385 OR G06Q20/4012 OR G06Q20/409 OR G07F7/0873 OR G07F19/00).cpc.	(US-PGPUB; USPAT; EPO; JPO)	OR	ON	ON	2022/11/05 02:30 PM
L70	336	69 AND dynamic$6 SAME generat$4 SAME nfc	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2022/11/05 03:37 PM
L71	161	card SAME issu$4	(US-PGPUB; USPAT;	OR	OFF	OFF	2022/11/05

		SAME dynamic$6 SAME generat$4 SAME nfc	EPO; JPO)				03:38 PM
L72	66	69 AND 71	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2022/11/05 03:38 PM
L73	38	(US-0044510-$ | US-0269005-$ | US-0275761-$ | US-0402811-$ | US-0423942-$ | US-0454728-$ | US-0460314-$ | US-0505277-$ | US-0516208-$ | US-0540647-$ | US-0546291-$ | US-0592893-$ | US-0680322-$ | US-0699266-$ | US-0713646-$ | US-0796299-$ | US-0803452-$ | US-0862718-$ | US-0902390-$ | US-0929851-$ | US-0990954-$ | US-0990959-$ | US-0998620-$ | US-1004075-$ | US-1017399-$ | US-1042855-$ | US-1061698-$ | US-10736322-$ | US-1074581-$ | US-1100431-$ | US-1107047-$ | US-1127010-$ | US-1129018-$ | US-11967211-$ | US-1227278-$ | US-1232339-$ | US-1321701-$ | US-17528073-$ | US-7528073-$ | US-9846866-$).DID.	(US-PGPUB; USPAT; EPO; JPO)	OR	ON	ON	2023/01/28 04:09 PM

PE2E SEARCH - Search History (Interference)

There are no Interference searches to show.

PE2E SEARCH - Search History (Similarity Search)

Ref #	Application Number	Text Selections	CPC Selections
L67	17/528,073	No selections	No selections

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

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. 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	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

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	9600808		2017-03-21	Gomez, Sr.; William et al.	
	2	9098846		2015-08-04	Gill; Sara et al.	
	3	7690580		2010-04-06	Shoemaker; Austin William	
	4	8499334		2013-07-30	Doughty; Ralph O. et al.	
	5	11100431		2021-08-24	Mullen; Jeffrey D. et al.	
	6	8255323		2012-08-28	Casey; Brandon J et al.	
	7	8423462		2013-04-16	Amacker; Matthew W. et al.	
	8	10460314		2019-10-29	Hird; Geoffrey R. et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	9	9846866		2017-12-19	Royyuru; Vijay	
	10	6736322		2004-05-18	Gobburu; Venkata T. et al.	
	11	7967211		2011-06-28	Challa; Nagesh et al.	
	12	8628012		2014-01-14	Wallner; George	
	13	8690059		2014-04-08	Wallner; George	
	14	8814046		2014-08-26	Wallner; George	
	15	9361613		2016-06-07	Wallner; George	
	16	9454679		2016-09-27	Wallner; George	
	17	9652642		2017-05-16	Wallner; George	
	18	9864994		2018-01-09	Huang; Enyang et al.	
	19	10044510		2018-08-07	Kwon; Eun Young et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	20	10269005		2019-04-23	Lee; Woo-Sup et al.	
	21	10275761		2019-04-30	Lee; Woo-Sup et al.	
	22	10402811		2019-09-03	Park; Yong Man et al.	
	23	10423942		2019-09-24	Lee; Woosup et al.	
	24	10454728		2019-10-22	Huang; Enyang	
	25	10505277		2019-12-10	Lee; Woosup et al.	
	26	10516208		2019-12-24	Lee; Woo-Sup et al.	
	27	10540647		2020-01-21	Park; Yong Man et al.	
	28	10546291		2020-01-28	Kim; Eun Jik et al.	
	29	10592893		2020-03-17	Lee; Hee-Dong et al.	
	30	10680322		2020-06-09	Lee; Woosup et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	31	10699266		2020-06-30	Lee; Hee-Dong et al.	
	32	10713646		2020-07-14	Lee; Hee-Dong et al.	
	33	10796299		2020-10-06	Lee; Woo-Sup et al.	
	34	10803452		2020-10-13	Kim; Eun Jik et al.	
	35	10862718		2020-12-08	Huang; Enyang	
	36	10902390		2021-01-26	Lee; Woosup et al.	
	37	10929851		2021-02-23	Kang; Minkoo et al.	
	38	10990954		2021-04-27	Park; Yong Man et al.	
	39	10990959		2021-04-27	Lee; Woo-Sup et al.	
	40	10998620		2021-05-04	Lee; Woosup et al.	
	41	11004075		2021-05-11	Lee; Je Min et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	42	11017399		2021-05-25	Park; Yong Seok et al.	
	43	11042855		2021-06-22	Kim; Yu Hwan et al.	
	44	11061698		2021-07-13	Rhee; Injong et al.	
	45	11074581		2021-07-27	Kim; In Ho et al.	
	46	11107047		2021-08-31	Kim; Kibong et al.	
	47	11127010		2021-09-21	Cho; Boo Hyun et al.	
	48	11129018		2021-09-21	Kim; Ki Bong et al.	
	49	11227278		2022-01-18	Choi; Hoon et al.	
	50	11232339		2022-01-25	Lee; Woosup et al.	
	51	11321701		2022-05-03	Lee; Hee-Dong et al.	

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

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	20130124410		2013-05-16	KAY; Christopher Erin et al.	
	2	20080319905		2008-12-25	CARLSON; Mark	
	3	20100185545		2010-07-22	Royyuru; Vijay K. et al.	
	4	20130262305		2013-10-03	Jones; Andrew R. et al.	
	5	20060089171		2006-04-27	Yoo; Kyung-Min et al.	
	6	20090048971		2009-02-19	Hathaway; Matthew et al.	
	7	20130232083		2013-09-05	SMITH; Theresa L. et al.	
	8	20080126260		2008-05-29	Cox; Mark A. et al.	
	9	20080222047		2008-09-11	Boalt; Adam	
	10	20080172317		2008-07-17	Deibert; Doug et al.	

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	11	20090159701		2009-06-25	Mullen; Jeffrey D. et al.	
	12	20120317035		2012-12-13	Royyuru; Vijay K. et al.	
	13	20130166441		2013-06-27	Kobylkin; Egor et al.	
	14	20120310760		2012-12-06	Phillips; Simon et al.	
	15	20080302876		2008-12-11	Mullen; Jeffrey D.	
	16	20110186626		2011-08-04	Manessis; Thomas et al.	
	17	20150147065		2015-05-28	Civelli; Jay Pierre et al.	
	18	20140143785		2014-05-22	Mistry; Pranav et al.	
	19	20050043997		2005-02-24	Sahota, Jagdeep Singh et al.	
	20	20150178724		2015-06-25	Ngo; Hao et al.	
	21	20160132881		2016-05-12	LEE; Yang-Soo et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	22	20160253652		2016-09-01	JE; Seong-Min et al.	
	23	20160253657		2016-09-01	SOHN; Se Chang et al.	
	24	20190026725		2019-01-24	PARK; Yong Seok et al.	
	25	20190172051		2019-06-06	LEE; Hui Jae et al.	
	26	20190173290		2019-06-06	HA; Min Cheol et al.	
	27	20210311752		2021-10-07	Rhee; Injong et al.	
	28	20220005046		2022-01-06	KIM; Inho 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]	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	2478712	GB		2011-09-21	JACKSON, DAVID		
	2	2485442	GB		2012-05-16	CUBIC CORP		

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	3	00/62214	WO		2000-10-19	CLEARTOGO.COM et al.		
	4	01/57620	WO		2001-08-09	COMSENSE TECHNOLOGIES LTD et al.		
	5	2007145687	WO		2007-12-21	WEISS, KENNETH P.		
	6	2010043974	WO		2010-04-22	RICHARD, CHRISTIAN		
	7	2012154915	WO		2012-11-15	DYNAMICS INC et al.		
	8	2005119607	WO		2005-12-15	TYFONE INC 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.	T5
	1		

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

EXAMINER SIGNATURE

Examiner Signature	/SEUNG H LEE/	Date Considered	01/28/2023

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

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	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

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

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. 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	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

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]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	1	Motorola MotoACTV Smartwatch, http://www.manualplanet.com/pdf/watches/motorola/motorola-motoactv-gpsfitness-tracker-quick-start-guide.pdf, 2012, pp. 1-2.	
	2	PEREZ, "New NFC-Enabled Phones to Hit Europe," ReadWriteWeb, February 18, 2011, pp. 1-3.	
	3	WESTER, "New Samsung Galaxy S4 phone includes NFC, innovative barcode technology; New Samsung smartphone adds a number of features that may spur mobile payment adoption," Mobile Payments Today, March 15, 2013, Networld Media Group, pp. 1-2.	
	4	"NFC Focus: Which Smartphones Have NFC?," International Business Times News, August 9, 2012, pp. 1-3	
	5	"NFC for mobile operators; Maximizing opportunities in the mobile NFC marketplace," Gemalto, November 2009, pp. 1-2.	
	6	CATHELINAIS, "Nice, the first city to switch to contactless payment," 01net.com, May 21, 2010, pp. 1-6.	
	7	CLARK, "Orange to offer Samsung Wave 578 NFC across Europe - but not in the UK," NFC World, February 14, 2011, pp. 1-4.	
	8	CLARK, "Orange to roll out NFC services across Europe in 2011," NFC World, December 16, 2010, pp. 1-3.	
	9	"PayPal Credit Card Tokenization Extension - Magento Connect," Magento Extension Marketplace, http://www.magentocommerce.com/magentoconnect/catalog/product/view/id/18715/s/paypal-credit-card-tokenization-extension-4490/, October 5, 2013, page 1.	
	10	Nanninga, "PayPal Credit Card Tokenization in Magento," SitePoint, September 30, 2013, pp. 1-11.	
	11	"Payment Card Industry (PCI), Data Security Standard, PCI DSS Applicability in an EMV Environment, A Guidance Document, Version 1," PCI Security Standards Council, October 5, 2010, pp. 1-12.	

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	12	"Standard: PCI PIN Transaction Security Point of Interaction Security Requirements (PCI PTS POI), Version: 1.0, Information Supplement: ATM Security Guidelines," PCI Security Standards Council, January 2013, pp. 1-44.	
	13	"PayPal NVP API Developer Reference Enterprise Edition - eBay," August 28, 2012, pp. 1-382.	
	14	"Rambus' Bell ID to support Android Pay," Rambus, February 18, 2016, page 1.	
	15	"RIM implements Bell ID's Token Manager software for mobile payments," WMI Company News, January 23, 2013, World Market Intelligence Private Ltd., page 1.	
	16	LAI, "Samsung and Visa join forces to enable NFC mobile payment at 2012 Olympics," Engadget, April 1, 2011, pp. 1-6.	
	17	"Samsung and Visa Showcase Mobile Payments at the London 2012 Olympic and Paralympic Games," Business Wire, May 9, 2012, pp. 1-4.	
	18	WARREN, "Samsung and Visa Take NFC Mobile Payments Global," Mashable.com, February 25, 2013, pp. 1-2.	
	19	HASELTON, "Samsung and Visa team up for NFC mobile payments at London 2012 Olympics," Boy Genius Report, March 31, 2011, pp. 1-3.	
	20	"Samsung and Visa to Showcase Mobile Payments @ the London Olympics," Samsung Global Newsroom, May 9, 2012, pp. 1-3.	
	21	"Samsung Announces Launch Dates for Groundbreaking Mobile Payment Service: Samsung Pay," Samsung Global Newsroom, August 14, 2015, pp. 1-2.	
	22	GROTTA, "Samsung Begins to Phase Out Support of MST for Samsung Pay," PaymentsJournal, February 22, 2021, pp. 1-3.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	23	MURPH, "Samsung cooks up its own NFC module, destined for the Nexus S?," Engadget, December 1, 2010, pp. 1-2.	
	24	MOLEN, "Samsung Galaxy S III for Verizon Wireless review," Engadget, July 9, 2012, pp. 1-10.	
	25	TRENHOLM, "Samsung Galaxy S3 is Olympic phone for no-touch payments," CNET, May 9, 2012, pp. 1-2.	
	26	"Samsung Google Nexus S - Full Phone Specifications, Reviews: Royal droid," GSMArena.com (archive.org), November 2010, pp. 1-2.	
	27	"Samsung Google Nexus S review: Royal droid," GSMArena.com (archive.org), February 11, 2011, pp. 1-2.	
	28	"Samsung partners with FeliCa for Japanese NFC solutions, unveils 2012 Olympics' mobile payment app with Visa," Engadget, February 24, 2012, pp. 1-3.	
	29	CLARK, "Samsung picks NXP for S3," NFCW, May 14, 2012, pp. 1-2.	
	30	"SAMSUNG to Acquire LoopPay, Transformative Digital Wallet Platform," Samsung US Newsroom, February 18, 2015, pp. 1-2.	
	31	HEUN, "Samsung to Unveil NFC Smartwatch - Has Wrist-Payments' Time Come?," Payments Source, September 2, 2013, SourceMedia LLC d/b/a Arizent, pp. 1-2.	
	32	"Samsung's New Secu-NFC Chip Enables Secure Mobile Payment by Enhancing NFC with Security Features," Plus NEWS, November 30, 2011, pp. 1-2.	
	33	NANNINGA, "Save Credit Cards in Magento with Our New Paypal Extension," Classy Llama, August 15, 2013, pp. 1-4.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	34	"Shift4 Releases New Technology to Insure the Security of Its Merchants' and Partners' Payment Processing," Hotel Online (archive.org), October 5, 2005, pp. 1-2.
	35	"S-Pay: What is MST?," Samsung Levant, September 22, 2020, pp. 1-2.

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

EXAMINER SIGNATURE

Examiner Signature	/SEUNG H LEE/	Date Considered	01/28/2023

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

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	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

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

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. 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	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

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]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	1	Susan Pandy, "Securing Payments: Payments Tokenization in Primetime," Federal Reserve Bank of Boston Payments Symposium, January 20, 2016, pp. 1-20.	
	2	"SUMMARY OF ANS X9.119-Part 2 USE OF TOKENS TO PROTECT SENSITIVE CARD DATA," September 2017, pp.1-2.	
	3	Marianne Crowe et al., "Is Payment Tokenization Ready for Primetime?," June 11, 2015, pp. 1-51.	
	4	Terence Spies et al., "ANSI X9.119 Part 2: Using Tokenization Methods," 2013, pp. 1-20.	
	5	ASSORA et al., "A web transaction security scheme based on disposable credit card numbers," Int. J. Electronic Security and Digital Forensics, 2007, Vol. 1, No. 2, Inderscience Enterprises Ltd., pp. 146-155.	
	6	BOYD, "A pragmatic approach to temporary payment cards numbers," Int. J. Electronic Security and Digital Forensics, 2009, Vol. 2, No. 3, pp. 253-268.	
	7	BUCCAFURRI et al., "Implementing disposable credit card numbers by mobile phones," Electronic Commerce Research, Feb. 23, 2011, Vol. 11, Springer Publishing, pp. 271-296.	
	8	JAVANI et al., "A new credit card payment system based on 3D-Secure using one-time-use transaction numbers," Information Assurance and Security Letters, 2010, Vol. 1, Dynamic Publishers, Inc., USA, pp. 060-065.	
	9	KILLORAN et al., "A New Secure Wireless Financial Transaction Architecture," EUROCON 2005, November 22-24, 2005, IEEE, pp. 1060-1063.	
	10	LI et al., "A security-enhanced one-time payment scheme for credit card," Mar. 28-29, 2004, IEEE, pp. 1-11.	
	11	MJØLSNES et al., "On-Line E-Wallet System with Decentralized Credential Keepers," Mobile Networks and Applications, 2003, Vol. 8, Kluwer Academic Publishers, The Netherlands, pp. 87–99.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	12	NARAYANASWAMI et al., "What Would You Do with a Hundred MIPS on Your Wrist?," RC 22057 (98634) January 22, 2001, IBM Research, pp. 1-10.	
	13	QASIM et al., "Interactive Shopping with Mobile Wallet," World Congress on Sustainable Technologies, 2012, IEEE, pp. 32-36.	
	14	HONIG, "A Week with Google Wallet," Endgadget, September 19, 2011, pp. 1-49.	
	15	KADAMBI et al.,"Near-Field Communication-Based Secure Mobile Payment Service," ICEC'09, August 12–15, 2009, pp. 1-11.	
	16	"A closer look at Google Pay and tokenization," Rambus Press, February 23, 2016, pp. 1-2.	
	17	GHAG et al., "A Comprehensive Study of Google Wallet as an NFC Application," International Journal of Computer Applications, November 2012, Vol. 58, No.16, pp. 37-42.	
	18	"Add any credit or debit card," Google Wallet Help (archive.org), 2012, page 1.	
	19	"Add any credit or signature debit card," Wallet Help, Google Wallet, September 20, 2012, page 1.	
	20	"Allynis Mobile NFC," Gemalto, September 2007, pp. 1-4.	
	21	"Allynis TSM for Transport," Gemalto, October 2009, pp. 1-2.	
	22	ADAMS, "Amex Plays a Major Role in Revamped Isis Mobile Wallet," Payments Source, November 15, 2013, Vol. 1, No. 1, SourceMedia LLC d/b/a Arizent, pp. 1-2.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	23	PEREZ, "Android Pay, Google's Apple Pay Rival, Arrives Today," DigitalOcean, September 10, 2015, pp. 1-8.	
	24	HEISLER, "Apple Pay: An in-depth look at what's behind the secure payment system," Engadget, October 2, 2014, pp. 1-7.	
	25	FEHR, "Apple Pay: How different is it from other Pay solutions, what role does tokenisation play, and to what degree can Card not Present payment benefit from Apple Pay in future," Technical Report RHUL–ISG–2018–3, April 3, 2018, Egham, Surrey, UK, pp. 1-79.	
	26	"ATMIA publishes contactless ATM best practices," ATM Marketplace, September 27, 2012, pp. 1-2.	
	27	POPPER, "Banks Did It Apple's Way in Payments by Mobile," New York Times, September 11, 2014, pp. 1-2.	
	28	"Bell ID Simplifies EMV Smart Card and NFC Application Management with Versatile New Platform," eBanking & Payment News, May 5, 2011, page 1.	
	29	"BofA pursuing contactless ATM patent," Mobilepaymentstoday.com News, September 20, 2012, Newstex LLC, pp. 1-2.	
	30	"Chip Advisory #20, Visa Recommended Practices for EMV Chip Implementation in the U.S," July 11, 2012, pp. 1-10.	
	31	"Commbank, Mastercard and Samsung collaborate to launch NFC payment service," MarketLine NewsWire (Formerly Datamonitor), December 13, 2013, pp. 1-2.	
	32	"Contactless Payment: Secure Enough?," Card Technology, September 1, 2005, SourceMedia, Inc., Section: SPECIAL ISSUE: CONTACTLESS TECHNOLOGY, Vol. 10, No. 8, page 36.	
	33	"Eligible Devices," Google Wallet Help (archive.org), November 18, 2012, page 1.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	34	MOTT, "EMV and Mobile Payments, Questions abound, answers divide," Payments Summit Workshop, February 4, 2013, pp. 1-22.
	35	"EMV Integrated Circuit Card Specifications for Payment Systems Book 2 Security and Key Management Version 4.1," May 2004, pp. 1-187.
	36	"EMV Integrated Circuit Card Specifications for Payment Systems. Book 2, Security and Key Management, Version 4.3," November 2011, pp. 1-174.
	37	"EMV Integrated Circuit Card Specifications for Payment Systems, Book 3, Application Specification, Version 4.3," November 2011, pp. 1-230.

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

EXAMINER SIGNATURE

Examiner Signature	/SEUNG H LEE/	Date Considered	01/28/2023

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

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	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

UNITED STATES PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

ACKNOWLEDGEMENT OF CHANGE TO SMALL ENTITY STATUS

APPLICATION #	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET #	REQUEST ID
17/528,073	11/16/2021	David WYATT	WYAT-0002-USD1C1C1C1C1C	64260

The entity status change request below filed through Patent Center on 02/13/2023 has been accepted.

Certifications

APPLICANT ASSERTING SMALL ENTITY STATUS. See 37CFR 1.27.

Signature

I certify, in accordance with 37 CFR 1.4(d)(4), that I am one of the signatories making the entity status change.

Signature	Name	Registration #
/Jose S. Garcia/	Jose Garcia	43628

Document Description: Application Data Sheet to update/correct info
Doc Code: ADS.CORR

CORRECTED ADS FORM

Application Number	17528073
Title of Invention	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Inventor Information

****If no data is shown, no data has been corrected****

	Data of Record	Updated Data
Order Number	1	
Name	David WYATT	
Residence Information		
Residency	us-residency	
City	~~San Jose~~	Austin
State	~~CA~~	TX
Country of Residence	US	
Mailing Address of Inventor		
Address 1	~~1314 Vanna Ct~~	1306 Norwalk Ln
Address 2		Apt 303
City,State/Province, Postal Code	~~San Jose CA 95131~~	Austin TX 78703
Country	US	

Document Description: Application Data Sheet to update/correct info
Doc Code: ADS.CORR

Application Information

	Data of Record	Updated Data
Title of Invention	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE	
Attorney Docket Number	WYAT-0002.USD1C1C1C1C1C	
Entity Type	Small	

Domestic Benefit/National Stage Information

****If no data is shown, no data has been corrected****

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121,365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S. C. 119(e) or 120, and 37 CFR 1.78(a).

		Data of Record	Updated Data
	Prior Application Status		
	Application Number		
	Continuity Type		
	Prior Application Number		
	Filing Date (YYYY-MM-DD)		
	Patent Number		
	Issue Date (YYYY-MM-DD)		

Foreign Priority Information

Document Description: Application Data Sheet to update/correct info
Doc Code: ADS.CORR

****If no data is shown, no data has been corrected****

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

		Data of Record	Updated Data
	Application Number		
	Country		
	Filing Date		
	Access Code		

Applicant Information

****If no data is shown, no data has been corrected****
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.

	Data of Record	Updated Data
Applicant Type		
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		
Applicant is an Organization		
Name		
Organization Name		
Address 1		
Address 2		

Corrected ADS 1.0

City,State/Province,Postal Code		
Country		
Phone Number		
Fax Number		
Email Address		

Assignee Information including Non-Applicant Assignee Information

****If no data is shown, no data has been corrected****
Providing this information in the application data sheet does not substitute for compliance with any requirement of part 3 of Title 37 of the CFR to have an assignment recorded in the Office

	Data of Record	Updated Data
Order		
Applicant is an Organization		
Name		
Organization Name		
Mailing Address		
Address 1		
Address 2		
City,State/Province,Postal Code		
Country		
Phone Number		
Fax Number		
Email Address		

Signature

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b).

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

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

Signature	/Jose S. Garcia/	Registration Number	43628
First Name	Jose	Last Name	Garcia

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
17/528,073	11/16/2021	2876	3750	WYAT-0002.USD1C1C1C1C1C	14	2

CONFIRMATION NO. 4809

CORRECTED FILING RECEIPT

136197
David Wyatt c/o Murabito, Hao & Barnes
111 North Market Street
Suite 700
San Jose, CA 95113

OC000000136862754

Date Mailed: 11/17/2022

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)
Austin, TX
David WYATT, ~~San Jose, CA~~;

Applicant(s)
CARDWARE, INC, San Jose, CA;

Power of Attorney: The patent practitioners associated with Customer Number 136197

Domestic Priority data as claimed by applicant
This application is a CON of 17/075,637 10/20/2020 PAT 11176538
which is a CON of 16/459,150 07/01/2019 PAT 10810579
which is a CON of 15/701,261 09/11/2017 PAT 10339520
which is a CON of 14/981,757 12/28/2015 PAT 9760884
which is a CON of 14/680,979 04/07/2015 PAT 9224083
which is a DIV of 14/217,261 03/17/2014 PAT 9022286
which claims benefit of 61/794,891 03/15/2013

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: 11/30/2021
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 17/528,073**
Projected Publication Date: Not Applicable
Non-Publication Request: No
Early Publication Request: No
**** SMALL ENTITY ****
Title

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Preliminary Class

235

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.

Electronic Acknowledgement Receipt	
EFS ID:	47512106
Application Number:	17528073
International Application Number:	
Confirmation Number:	4809
Title of Invention:	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE
First Named Inventor/Applicant Name:	David WYATT
Customer Number:	136197
Filer:	Jose S. Garcia
Filer Authorized By:	
Attorney Docket Number:	WYAT-0002.USD1C1C1C1C1C
Receipt Date:	10-FEB-2023
Filing Date:	16-NOV-2021
Time Stamp:	00:42:50
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet to update/ correct info	CorrectedADS.pdf	102555 87a8012224df8c08385be2eddb0830e64a3b53bd	no	5

Warnings:

Information:					
2	Request for Corrected Filing Receipt	WYAT-0002-13C12US_Filing_Receipt_Correction.pdf	227895 35b0059b8c0e1e5d2d8c0318ee672669d4e8e09d	no	4
Warnings:					
Information:					
			Total Files Size (in bytes):	330450	

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
17/528,073	11/16/2021	2876	3750	WYAT-0002.USD1C1C1C1C1C	14	2

CONFIRMATION NO. 4809

CORRECTED FILING RECEIPT

136197
David Wyatt c/o Murabito, Hao & Barnes
111 North Market Street
Suite 700
San Jose, CA 95113

OC000000136862754

Date Mailed: 11/17/2022

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)

David WYATT, Austin, TX ~~San Jose, CA~~;

Applicant(s)

CARDWARE, INC, San Jose, CA;

Power of Attorney: The patent practitioners associated with Customer Number 136197

Domestic Priority data as claimed by applicant

This application is a CON of 17/075,637 10/20/2020 PAT 11176538
which is a CON of 16/459,150 07/01/2019 PAT 10810579
which is a CON of 15/701,261 09/11/2017 PAT 10339520
which is a CON of 14/981,757 12/28/2015 PAT 9760884
which is a CON of 14/680,979 04/07/2015 PAT 9224083
which is a DIV of 14/217,261 03/17/2014 PAT 9022286
which claims benefit of 61/794,891 03/15/2013

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: 11/30/2021
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 17/528,073**
Projected Publication Date: Not Applicable
Non-Publication Request: No
Early Publication Request: No
**** SMALL ENTITY ****
Title

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Preliminary Class

235

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

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/528,073	**02/09/2023 11:19:57 PM ET**	**WYAT-0002.USD1C1C1C1C1C**

Title of Invention

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4809	FILED BY	Jose Garcia
PATENT CENTER #	61576291	FILING DATE	11/16/2021
CUSTOMER #	136197	FIRST NAMED INVENTOR	David WYATT
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 2

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
CorrectedADS.pdf	3	Application Data Sheet to update/correct info	70 KB
WYAT-0002-13C12US_Filing_Receipt_Correction.pdf	4	Request for Corrected Filing Receipt	223 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
CorrectedADS.pdf	1B1B34F3B58961AC151A192A146DCB79F1A229C64E171B8698

	63815BCF5E35D68BF7CD747614283FF95034DECCF6FB68366387FFA25A515FACF5A877FA45A29F
WYAT-0002-13C12US_Filing_Receipt_Correction.pdf	4889C75A123B8BA21E4F1CBA3970685B1D3408B25CA12FEEDF9F944657CC26C88CFC0A2D3C0D795E5C25AAECE2DD3CE5632070A46296BCDE6BDEA8AA4A515102

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 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

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

Corrected Application Data Sheet

17528073 : MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

~~Strike-through~~ indicates removal of data from existing record Underline indicates new data being added to the application If no data is shown, no data has been corrected

Inventor Information

Data of record	Updated Data
David WYATT	
Residence Information US Residency San Jose, CA UNITED STATES	
Mailing Address ~~1314 Vanna Ct~~ ~~—~~ ~~San Jose, CA 95131~~ UNITED STATES	**Mailing Address** 1306 Norwalk Ln Apt 303 Austin, TX 78703

Application Information

Title of Invention	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE	
Attorney Docket Number	WYAT-0002.USD1C1C1C1C1C	
Entity Status	~~Small~~	Regular Undiscounted

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), 386(c), or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.

Data of record	Updated Data
No data change in this section	

Foreign Priority Information

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the Application Data Sheet constitutes the claim for priority as required by 35 U.S.C. 119 (b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Data of record	Updated Data
No data change in this section	

Applicant Information

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.

Data of record	Updated Data
No data change in this section	

Assignee Information including Non-Applicant Assignee Information

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

Data of record	Updated Data
No data change in this section	

Signature

NOTE:

This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b).

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

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

Signature	First name	Last name	Registration #	Date
/Jose S. Garcia/	Jose	Garcia	43628	02/09/2023

UNITED STATES PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

Corrected Application Data Sheet

17528073 : MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

~~Strike-through~~ indicates removal of data from existing record Underline indicates new data being added to the application If no data is shown, no data has been corrected

Inventor Information

Data of record	Updated Data
No data change in this section	

Application Information

Title of Invention	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE	
Attorney Docket Number	~~WYAT-0002.USD1C1C1C1C1C~~	WYAT-0002-13C12US
Entity Status	Small	

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), 386(c), or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.

	Updated Data

Data of record

No data change in this section

Foreign Priority Information

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the Application Data Sheet constitutes the claim for priority as required by 35 U.S.C. 119 (b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Data of record	Updated Data

No data change in this section

Applicant Information

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.

Data of record	Updated Data
CARDWARE, INC --- --- ~~San Jose, CA 95130~~ UNITED STATES Phone : --- Email : --- Fax : --- Organization Applicant type : Assignee	111 Congress Ave Suite 500 Austin, TX 78701

Assignee Information including Non-Applicant Assignee Information

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

Data of record	Updated Data
No data change in this section	

Signature

NOTE:

This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b).

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

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

Signature	First name	Last name	Registration #	Date
/Jose S. Garcia/	Jose	Garcia	43628	02/09/2023

Doc Code: R46C.REQ
Document Description: Request under 37 CFR 1.46(c) to correct, update or change the applicant.

PTO/AIA/41 (04-15)
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 displays a valid OMB control number.

REQUEST TO CORRECT OR UPDATE THE NAME OF THE APPLICANT UNDER 37 CFR 1.46(c)(1), OR CHANGE THE APPLICANT UNDER 37 CFR 1.46(c)(2)
(FOR USE ONLY IN APPLICATIONS FILED ON OR AFTER SEPTEMBER 16, 2012)

Application Number	17/528,073
Filing Date	11-16-2021
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Practitioner Docket Number	WYAT-0002-13C12US

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

Applicant hereby **requests that the name of the applicant be corrected or updated under 37 CFR 1.46(c)(1), or that the applicant be changed under 37 CFR 1.46(c)(2),** in the above-identified application. **Requests under 37 CFR 1.46(c)(1) or (c)(2) cannot be submitted after payment of the issue fee or if the application has been patented.**

Please check the applicable box(es) below.

☐ 1. This request is to **correct or update the name of the applicant** (**under 37 CFR 1.46(c)(1)**) and includes:

☐ An application data sheet (ADS) in accordance with 37 CFR 1.76(c) with the corrected or updated information shown with markings (*e.g.*, underlining for insertions, strikethrough for deletions). A Corrected Web-based ADS may be used.

Note: Requests under 37 CFR 1.46(c)(1) may be filed to correct typographical errors in the name of the § 1.46 applicant, or for updating the name of the § 1.46 applicant (*i.e.*, where there is no change in the applicant itself but just in the applicant's name). See the Manual of Patent Examining Procedure (MPEP) section 605.01.

☒ 2. This request is to **change the applicant** (**under 37 CFR 1.46(c)(2)**) and includes:

☒ An application data sheet (ADS) in accordance with 37 CFR 1.76(c) that identifies the changes with proper markings (underlining for insertions and strikethrough for deletions). A Corrected Web-based ADS may be used.

☒ A Statement Under 37 CFR 3.73(c) (Form PTO/AIA/96 or equivalent). See MPEP 325.

I am the

☐ applicant* ☒ attorney or agent of record Registration number 43628 ☐ attorney or agent acting under 37 CFR 1.34 Registration number _____

Signature /Jose S. Garcia/
Typed or printed name Jose S. Garcia
Date 02/09/2023

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. *Juristic entities must be represented by a patent practitioner (See 37 CFR 1.31, applicable to any paper filed on or after September 16, 2012 that is presented on behalf of a juristic entity, regardless of application filing date). Submit multiple forms if more than one signature is required, see below**.

☐ ** Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.36. 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 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.

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.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/528,073	**02/09/2023 10:30:58 PM ET**	**WYAT-0002.USD1C1C1C1C1C**

Title of Invention

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4809	FILED BY	Jose Garcia
PATENT CENTER #	61576205	FILING DATE	11/16/2021
CUSTOMER #	136197	FIRST NAMED INVENTOR	David WYATT
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 3

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
CorrectedADS.pdf	3	Application Data Sheet to update/correct info	71 KB
WYAT-0002-13C12US_aia0041_Request_to_Change_Applicant.pdf	2	Request for Corrected Filing Receipt	235 KB
WYAT-0002-13C12US_aia0096_Statement_under_3_73c.pdf	3	Assignee showing of ownership per 37 CFR 3.73	206 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
CorrectedADS.pdf	1A33C7267A8D023270FD6E2B020D686A5E58F264598F8F5E74485D8388015307249FE1B9D933E1F4A18A864CCCFA682C67C20D59C58BDDC8AE90A1E377648660
WYAT-0002-13C12US_aia0041_Request_to_Change_Applicant.pdf	DDA42D25A1D83DD80DF20D7E4B149C92DD0ECA78949770726B66E1E62C74B42A9BB8AFAB8FB65A6FAF5950AFB55D26501FD947FAF166618D74641441540DE717
WYAT-0002-13C12US_aia0096_Statement_under_3_73c.pdf	ECAA0CB00E24AE36313253321C3465010A67EF77A7BA014A633FF497C86088A2F88E3BB6AFBBBD582D7EFF487B6F41777D07628194C5DFAC8E4AC2366FD3C4E3

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 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/AIA/96 (08-12)
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 displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: CARDWARE, INC.

Application No./Patent No.: 17/528,073 Filed/Issue Date: 11-16-2021

Titled: MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

CARDWARE, INC., a corporation

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☑ The assignee of the entire right, title, and interest.

2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):

   ☐ The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

   ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (*e.g.*, bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

A. ☐ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

B. ☑ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: David WYATT To: CARDWARE, INC.

   The document was recorded in the United States Patent and Trademark Office at

   Reel 058892, Frame 0036, or for which a copy thereof is attached.

2. From: CARDWARE, INC. To: CARDWARE, INC.

   The document was recorded in the United States Patent and Trademark Office at

   Reel 062030, Frame 0299, or for which a copy thereof is attached.

This collection of information is required by 37 CFR 3.73(b). 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 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450**.

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

PTO/AIA/96 (08-12)
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 displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☑ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Jose S. Garcia/	02/09/2023
Signature	Date
Jose S. Garcia	attorney for CARDWARE, INC.
Printed or Typed Name	Title or Registration Number

Privacy Act Statement

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

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

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

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. 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	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

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	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	1	"Isis NFC-payment from SXSW 2012," YouTube, https://www.youtube.com/watch?v=Z2MOAtUhR7k, March 10, 2012, pp. 1- 2.	
	2	"Isis NFC-payment from SXSW 2012," Transcript of YouTube, https://www.youtube.com/watch?v=Z2MOAtUhR7k, March 10, 2012, pp. 1- 3.	
	3	"NFC - Google Wallet and More - EE Times - Mobile World Congress," YouTube, https://www.youtube.com/watch?v=AgSk7L6HhVw, March 6, 2012, pp. 1-3.	
	4	"NFC - Google Wallet and More - EE Times - Mobile World Congress," Transcript of YouTube, https://www.youtube.com/watch?v=AgSk7L6HhVw, March 6, 2012, pp. 1-8.	
	5	"Paying With Google Wallet," YouTube, https://www.youtube.com/watch?v=jTeiISIzBPQ, February 6, 2012, pp. 1-2.	
	6	"Seinfeld - Google Wallet," YouTube, https://www.youtube.com/watch?v=baaCvgTRYsU, June 14, 2013, pp. 1-2.	
	7	"Technology: Google Wallet - The New York Times," YouTube, https://www.youtube.com/watch?v=I8JOT6ban7o, September 23, 2011, pp. 1-2.	
	8	"Using Google Wallet in McDonald's!," YouTube, https://www.youtube.com/watch?v= 1p6co4YIvbA, September 14, 2012, pp. 1-2.	
	9	"Virtual terminal- #1 storing credit card data with tokenization," YouTube, https://www.youtube.com/watch?v=eSXIIGbACew, February 28, 2011, pp. 1-3.	
	10	"What is Google Wallet?," YouTube, https://www.youtube.com/watch?v=iuvyN4iZiP8, August 9, 2011, pp. 1-3.	
	11	"What is Tokenization?," YouTube, https://www.youtube.com/watch?v=ypm5FFfEN34, January 17, 2011, pp. 1-3.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	12	"How Credit Card Number Tokenization can Reduce PCI Compliance Stress - File 1 of 3," YouTube, https://www.youtube.com/watch?v=FHD5XzAIKDI, Jul 28, 2009, pp. 1-3.	
	13	"How Credit Card Number Tokenization can Reduce PCI Compliance Stress - File 1 of 3," Transcript of YouTube, https://www.youtube.com/watch?v=FHD5XzAIKDI, Jul 28, 2009, pp. 1-12.	
	14	"HOW CREDIT CARD NUMBER "TOKENIZATION" CAN REDUCE PCI COMPLIANCE STRESS - File 2 of 3," YouTube, https://www.youtube.com/watch?v=t-fWpcLdb3o, Jul 28, 2009, pp. 1-3.	
	15	"HOW CREDIT CARD NUMBER "TOKENIZATION" CAN REDUCE PCI COMPLIANCE STRESS - File 2 of 3," Transcript of YouTube, https://www.youtube.com/watch?v=t-fWpcLdb3o, Jul 28, 2009, pp. 1-12.	
	16	"HOW CREDIT CARD NUMBER "TOKENIZATION" CAN REDUCE PCI COMPLIANCE STRESS- File 3 of 3," YouTube, https://www.youtube.com/watch?v=_CdoKEuEB9s, Jul 28, 2009, pp. 1-3.	
	17	"HOW CREDIT CARD NUMBER "TOKENIZATION" CAN REDUCE PCI COMPLIANCE STRESS- File 3 of 3," Transcript of YouTube, https://www.youtube.com/watch?v=_CdoKEuEB9s, Jul 28, 2009, pp. 1-8.	
	18	"Caixer contactless lacaixa," YouTube, https://www.youtube.com/watch?v=It2CpMcxQC4, April 4, 2011, pp. 1-2.	
	19	"Understanding Proximity Sensors - T-Mobile," YouTube, https://www.youtube.com/watch?v=npD48agt0xY, January 2010, pp. 1-2.	
	20	"Understanding Proximity Sensors - T-Mobile," YouTube, https://www.youtube.com/watch?v=npD48agt0xY, January 2010, page 1.	
	21	"Understanding Proximity Sensors - T-Mobile," Transcript of YouTube, https://www.youtube.com/watch?v=npD48agt0xY, January 2010, pp. 1-2.	
	22	"Google I/O 2012 - The Sensitive Side of Android," YouTube, https://www.youtube.com/watch?v=Q0V_Id7iNw4, June 29, 2012, pp. 1-2.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	23	"Google Wallet Overview," YouTube, https://www.youtube.com/watch?v=VuFVsaFCzsw, August 1, 2012, page 1.	
	24	"Google Wallet Overview," Transcript of YouTube, https://www.youtube.com/watch?v=VuFVsaFCzsw, August 1, 2012, pp. 1-2.	
	25	"Android 4.0 APIs | Android Developers," mit.edu, https://stuff.mit.edu/afs/sipb/project/android/docs/about/versions/android-4.0.html, 2011, pp. 1-23.	
	26	"EMV Integrated Circuit Card Specifications for Payment Systems, Book 2, Security and Key Management, Version 4.3," EMVCo, November 2011, pp. 1-174.	
	27	"Exploring Google Wallet using the secure element interface," nelenkov.blogspot.com, August 27, 2012, pp. 1-20.	
	28	GARSIDE, "Google Wallet mobile payments system launched to public," The Guardian, https://www.theguardian.com/technology/2011/sep/19/google-wallet-available-public, September 19, 2011, pp. 1-5.	
	29	PURDY, "How to grab a screenshot from iPhone, Android, and nearly any other smartphone," Computer World, April 20, 2012, pp. 1-6.	
	30	"Maximum failed passcode attempts in restrictions - what happens?," Apple Community, https://discussions.apple.com/thread/3690633, January 2012, pp. 1-3.	
	31	"Simplify, Organize & Pay with Loop by Will Graylin & George Wallner," Kickstarter, March 2019, pp. 1-13.	
	32	"Hands-on with ISIS Mobile Wallet," YouTube, https://www.youtube.com/watch?v=eOMqvGVKjmM, March 10, 2012, page 1.	
	33	"EMV Solutions," Paragon Application Systems, https://web.archive.org/web/20120818221214/http://www.paragonedge.com/solutions/emv-solutions.html, August 18, 2012, page 1.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	34	SULLIVAN, "The Changing Nature of U.S. Card Payment Fraud: Industry and Public Policy Options," Economic Review, Federal Reserve Bank of Kansas City, Second Quarter 2010, ProQuest Information and Learning, Vol. 95, No. 2, pp 101-133.
	35	"EMV Integrated Circuit Card Specifications for Payment Systems, Book 1, Application Independent ICC to Terminal Interface Requirements, Version 4.3," EMVCo, November 2011, pp. 1-189.
	36	"EMV Contactless Specifications for Payment Systems, Book B, Entry Point Specification, Version 2.1," EMVCo, March 2011, pp. 1-50.
	37	ETHERINGTON, "Android Pay Is Real, And Will Give Developers The Reins As An API," TechCrunch, https://techcrunch.com/2015/03/02/android-pay-is-real-and-will-give-developers-the-reins-as-an-api, March 2, 2015, pp. 1-7.
	38	"PCI DSS Version 2.0 Information Supplement: PCI DSS Tokenization Guidelines," PCI Security Standards Council, pcisecuritystandards.org, https://listings.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf., v 2.0, August 2011, pp. 1-23.
	39	"EMVCo Updates Payment Tokenisation Specification to Introduce 'Payment Account Reference,'" www.emvco.com, March 29, 2016, pp. 1-2.

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	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

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	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

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.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/528,073	**01/12/2023 02:47:58 AM ET**	**WYAT-0002.USD1C1C1C1C1C**

Title of Invention

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4809	FILED BY	Jose Garcia
PATENT CENTER #	61424685	FILING DATE	11/16/2021
CUSTOMER #	136197	FIRST NAMED INVENTOR	David WYATT
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 44

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
WYAT-0002-13C12US_IDS_transmittal_form_5.pdf	7	Information Disclosure Statement (IDS) Form (SB08)	1236 KB
Paragon_Application_Systems_EMV.pdf	1	Non Patent Literature	159 KB
passcode_attempts.pdf	3	Non Patent Literature	1011 KB
Paying_Google.pdf	2	Non Patent Literature	746 KB
PCI_Compliance.pdf	3	Non Patent Literature	1345 KB
PCI_Compliance_Stress.pdf	12	Non Patent Literature	204 KB

PCI_Tokenization_Guidelines_Info_Supplement.pdf	23	Non Patent Literature	638 KB
Proximity_Sensors.pdf	2	Non Patent Literature	629 KB
REDUCE_PCI.pdf	3	Non Patent Literature	1473 KB
REDUCE_PCI_STRESS.pdf	12	Non Patent Literature	206 KB
screenshot.pdf	6	Non Patent Literature	1897 KB
Android_API.pdf	23	Non Patent Literature	18175 KB
Android_Pay_Is_Real_TechCrunch.pdf	7	Non Patent Literature	5242 KB
B_Entry_Point_Specification_v2_1_March2011.pdf	50	Non Patent Literature	328 KB
CARD_NUMBER.pdf	3	Non Patent Literature	1439 KB
Changing_Nature_of_US_Card_Payment_Fraud_Industry_and_Public_Policy_Options.pdf	33	Non Patent Literature	446 KB
contactless_lacaixa.pdf	2	Non Patent Literature	634 KB
CREDIT_CARD_NUMBER.pdf	8	Non Patent Literature	135 KB
EMV_v4.3_Book_1_ICC_to_Terminal_Interface.pdf	189	Non Patent Literature	1027 KB
EMVCo_Updates_Payment_Tokenisation_Specification.pdf	2	Non Patent Literature	127 KB
Exploring_Google_Wallet.pdf	20	Non Patent Literature	12200 KB

Google_Wallet_Overview.pdf	1	Non Patent Literature	300 KB
Hands_on_with_ISIS_Mobile_Wallet.pdf	1	Non Patent Literature	205 KB
Isis_NFC.pdf	2	Non Patent Literature	753 KB
Isis_SXSW.pdf	3	Non Patent Literature	42 KB
Mobile_World.pdf	3	Non Patent Literature	1511 KB
Mobile_World_Congress.pdf	8	Non Patent Literature	137 KB
New_York_Times.pdf	2	Non Patent Literature	779 KB
Using_Google_Wallet.pdf	2	Non Patent Literature	782 KB
Virtual_terminal.pdf	3	Non Patent Literature	1469 KB
Wallet_mobile_payments.pdf	5	Non Patent Literature	2498 KB
Wallet_Overview.pdf	2	Non Patent Literature	21 KB
What_Google_Wallet.pdf	3	Non Patent Literature	1334 KB
Will_Graylin.pdf	13	Non Patent Literature	4632 KB
Security_Key_Management_1_of_5.pdf	35	Non Patent Literature	12146 KB
Security_Key_Management_2_of_5.pdf	35	Non Patent Literature	14749 KB
Security_Key_Management_3_of_5.pdf	35	Non Patent Literature	17761 KB
Security_Key_Management_4_of_5.pdf	35	Non Patent Literature	17097 KB

Security_Key_Management_5_of_5.pdf	34	Non Patent Literature	16191 KB
Seinfeld.pdf	2	Non Patent Literature	705 KB
Sensitive_Side.pdf	2	Non Patent Literature	655 KB
T_MOBILE.pdf	1	Non Patent Literature	277 KB
Tokenization.pdf	3	Non Patent Literature	1541 KB
Understanding_Proximity_Sensors.pdf	2	Non Patent Literature	291 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
WYAT-0002-13C12US_IDS_transmittal_form_5.pdf	EB152BE38E8F14A1D1022A1EB20CAAB1E1AFA37556F759B0A9584EC443492165FA65C6C54BB3370D61F79B7C133F06B957104961BE509658FD8D89DD8C146F07
Paragon_Application_Systems_EMV.pdf	AF376E74FC80C73DC8BAEE41F09ECE67605F12E71111098FE1770819CD12E6AE7F3D3FAD34743C6B1D626EFFAB87C3E83C80EA79FB0B00327FCD066DE9DC145A
passcode_attempts.pdf	C9E4FC3CF7D261392F9A86402A2431190D534FB0BC622679C3778154B567459FC03B8D1C85FBB7A3996D61706FD5B413DB69508FABF58BFDD6D6823583D7F483
Paying_Google.pdf	601BCF273175710BE405124C4DA9B46C6B0F2DB06F9739012A31A50FD6B05D4B596410C4DDB111CE7617C7DD681149E95F7A88A60366046E77F0EE18BB7B9643
PCI_Compliance.pdf	3B8B4A36EB201D0FCF1C2CD9CB59D580AD571310E765CB535C92F0B3C2F4ABE94B483FD7C4415735C1EE9C019769056E7D63C98F690B40020D21BF09FA89B196

PCI_Compliance_Stress.pdf	0EF6F246F86CB5B7CAF15CAF7932B0ABDD4E150C8E12D5D158D5F5EA31F0DCD8053D77E85F7B02B59D2F7EF8609BFBAE93CB151CBE115E7A4840E3CA00003FE0
PCI_Tokenization_Guidelines_Info_Supplement.pdf	5FE7C5562730405694C5554CCC5F9926E15C0DFF68F6BB882657326C379CC845C2BD4AEE52DB72E8EF2054D1C3147A934C8F9A1477560D5F6CCEBA9F14B30581
Proximity_Sensors.pdf	8A40C7A3B9DCE6F7446FD7BFA67FF5501E9F023312A4BF6A31FC55C5B4D4BA2C31BB8E29A9A7475FB7016DBA680C459EEAB7FA4D24C5089C003836D525002388
REDUCE_PCI.pdf	4C35268DC06DF30510C90BFF65CB19013F131F06A0B13355B36CF3909DFAF67783EC798BBB6067567EB151467D79D26C37240D9A58CC2F6239B924C3AAE3D471
REDUCE_PCI_STRESS.pdf	A556B8E60973E1948D21AA39563968AF4EA5EAC790150BCE437DC0B84E09E6AB49D4A64D1EFBFB1D1B9816B8BF04E0CB89149B084204A68DC2BCCC067F160113
screenshot.pdf	51EFBD790AF43DBEDF9BD006BD9C8C4D5A30F7F8D54074C173C8AB65E59885C3856E71F2ECE9686E85C792D947408DEBA603B7B9DEE9FD463CF4BE9F7840EE4D
Android_API.pdf	D299177B4ED333463CAB066AA0D24F59369B3E220270A6D3875193983396969C84E68671D3E31574AD90AB6921335A9A265935D8DC368AEB2D1A10277A41CDE0
Android_Pay_Is_Real_TechCrunch.pdf	C4F0DDC061BA696B63644BAADAE8FB6143DEB310A308A251662AB19E27A5D6290BFDC5CCE15140336F3A2CD78F4C5A38FD1167F363C69CBDDC3050ADA5600F00
B_Entry_Point_Specification_v2_1_March2011.pdf	7FEEA416D0E066BECAE398697FDD86EF827441D98F6BFA2089D5A42CB022BA6D0A453CE64DF76899FE54DC01DA10A910829F0657C4D987210B68356098C6EF7D
CARD_NUMBER.pdf	71812AF5700B57C1AB25A8FC556E185FBA6A7C1D79F08A4084821B3BFD3AA958A69D4A1030F0565E8DAB842BDD7215F071E0C7D29B7308A8FAEFB9B20874CFC9

Changing_Nature_of_US_Card_Payment_Fraud_Industry_and_Public_Policy_Options.pdf	327509AF153AD3CB176379B58448415B7119BE7D946D01C4B4C71FD7A1DB0FFA12BB6C383A09297C453AB16193A8C2DEEF43618A3D4BCCA2BCB0CCBDC287F1EE
contactless_lacaixa.pdf	E3B844123B8982BB27C07443F3C9021F2F8DD0271B149B18AB4C1F6F2004281DD7C38BC9002E832E836FF11F20FEB7244753A44CA7C947F3069F1E9251A8B278
CREDIT_CARD_NUMBER.pdf	AEA238B431E2F4108021379775865281863 9BF4DFA2D427A12C39615B250E7C463ED4B0F45B2DD2EF94391D6CBC12DAB7B0C644FDF40910B4E4A347188875ECC
EMV_v4.3_Book_1_ICC_to_Terminal_Interface.pdf	1E687B6A1F33CC017C0C90CE52A3F6D23FFA457B3F58380110635FA9F6901D5295DB5870A7BF949983BD920124FB518B86CC0E53BE978BA8839E7EEBDA0CE20F
EMVCo_Updates_Payment_Tokenisation_Specification.pdf	D15DB971C91EEE5A17D8FBB971D1DDDF748A532293769A462048C1035C798DE0050C186BC230531E097A7B198781AEC0F4BC227CA57A8E88A0D9CBA0C089CB82
Exploring_Google_Wallet.pdf	DF6C87563AFAE759ADE235C519F75F41EF468B3C4296C3FD379529107BBE25B28BAD5D776292C15873110DF15660240FA2D5847DBE5E63C3F036CF898FD99AD3
Google_Wallet_Overview.pdf	6410185709EEBDCCB8059DD7640EFC309FB0569B8EC76EA526E3B05F5EB155133D2D499F820C7A4C6FCA1F41B0BE37849D5EA12831775175ECEC92D07A0F4B8C
Hands_on_with_ISIS_Mobile_Wallet.pdf	F415943E01EFB6E850FBBF782B5A5F1EF50C90105D21552F02F5A9A6AEBC742F2BA54F8C4AE936A10524B4278666B11FA9438499B65E494111E352E7F3F835FA
Isis_NFC.pdf	3AC49AD9FDEF91F9B1200F424AFF6861D51FBB616FCD40D9D1745F7CC702A99311F52D95B575C9FB21046963AE18B3ACCAC1AD832822450828EA37AE753F5E97
Isis_SXSW.pdf	868CC0AECD79D60F8ECCC5DD916C9DC1915F9445B683694A63E3DE618C5EFC7FE56EA44FF6B16F2EE52A18A3966E5AAD340F0D7D759F13D6C2FDC6CAC994C19D

Mobile_World.pdf	74C72C18BD46A49569BDC41192294347FDD95BFEDB7923944CB86A1C2B1FDAC51F1D0FDD122221B2DEFAC0A4D3B3A3969D789A3500CA21BF5D98C2818CDFE558
Mobile_World_Congress.pdf	F0C2B759CB7755B651703DD68FB6460021D1D6518006FB887B5E9C0CFE3E4285C04C16CC18215CBE07A87B1F2998E2A08582DD57756BF544154808020597 0B0C
New_York_Times.pdf	72CE5D91AAD01B131EF53C98BBEC955CD2EBD1AF7297C1F595E9AB46BA36AE475011E0C45841BAC6B0F5F09E3FA526F7A39316402ED1D900C88857F0688339AB
Using_Google_Wallet.pdf	8A4A36DEBDE2D6AC68F5FCA96FD931ED22B2C88244AA20F0D83C4A8BB241BBB02E977D2835BC2A263FCF69DBE6E3B8412C74EBE57FA3EF23BAC2F18981163878
Virtual_terminal.pdf	EA989A5B6BC6A95F36CDA7702AED719D7A246F43D5A584695DB2E844A1DDE5D59E62D67C51BB8D7BBE1823C8A553B862B122F903BE689E9EFC581DD07061D084
Wallet_mobile_payments.pdf	5F86AB0325A6918D7A6BD31D32522099DCC56A90BC7BB6F69BC76E5EB668715CE41BB1BA800C92AFBA9D72DB5B90EF19B3217458650BA447917A02A0D18642E0
Wallet_Overview.pdf	5B74F1AD54B320354499D3E23D8A8C71299C630C78F3BA7F1D075900E338F2C4FFDF0D2A767A9D80D5DD9BD38ADC8B40D2A96FD3E9274FC8636E7E0630B7AA1A
What_Google_Wallet.pdf	ACE563AB3E52C0C2AA5F4DA3E9CA63A28734AEDB88E18B8E61672D5CAA7042BEBDCB6C1C5C42A20904610A1FFDAFEDD02F0F3E9B0522E33C4CAE5E4A8063246F
Will_Graylin.pdf	694DBBA98709129E04A695B85CCE8114D8949DAB0FC559A1DBABE15892053B0C85E5DB7B6306291BA2FD8971082ED5956E2CE41124606BB4B18809FDB04A8AB8
Security_Key_Management_1_of_5.pdf	2B5BE6BB0C5FC5C2AC07582D4C3763E66357010D8BE537D2FF1FC44183A9DCDFCDF962DF5EF39F4E59765AEB8CD6DCA6006620E8DE772057EB655EDD24BFC2CD

Security_Key_Management_2_of_5.pdf	1EE397678DB5A81A51358ADAF5FDE8849D93FE2C91FBB713362BFF56BD8AC5AE7799513A45D6E65C111B2D6E9242C121A953D1B3745DFEF1FDBEBC4CBB8AB89F
Security_Key_Management_3_of_5.pdf	A0733EDB9871753DED2B125B7FEC211EBCBFB1F1DB13A80BE5176A40FB40FF3FFDCB421D495D2178CD30B0BCC98BFA7A385B0D0714527B9869A7D40BB741F58E
Security_Key_Management_4_of_5.pdf	73D99B8583AABAC48C73B6FBAC0770B26FACAE3ACB0A60A48490C27C561BFB0968BD65BF18BA03827C9C67F7B336CC52D173E8C0F01F1D50AE59B2541BA63DE4
Security_Key_Management_5_of_5.pdf	BEEF6C4A4E316E20A91B761441763C8745BDB09D148E846E3F3FCCA69B825B9BD7DF8DC0C843142A2491310C610FEAFC024CAD2ADA84CA3AB6CC1086FD7F7C2D
Seinfeld.pdf	9F449A18E85956D7C28BFCD0CA63FDF6C1D4D5A30DA3DED18069FEAB4EA176ADE7D2BEE52924B3D91D5737F645329B5BF9629FC8617146E3FB53C52B4BC7C516
Sensitive_Side.pdf	317C4948BB4B63F43AEF2357780EDCB4233E3C2998F3A2EC2C57B232D4CCB72B89A04C37A873C83E7FDC20BDA6A8385DFD88A7620169D6D7144D38CB69CD8DC2
T_MOBILE.pdf	BB1994F921DD7982A6B3161056B45A3745BB61B535A92DA705DEEAA25D1C23EB61877914B2EBD91130B8BC525CE1D204E8536E7A0EA034EDC35A027658829317
Tokenization.pdf	7AE63B12CEB14F98A85D4139682F2DCCF49DBBC4AFCDE7AB961760D721D0AF4DA50D5FF7FFAD9A5F088D7A1D2B4E260D005E17DC8A9A9A19B8ABD2C0BC302F0D
Understanding_Proximity_Sensors.pdf	2E181A79CCCF26BD11387AE9D3A466722679EA7119AAEF64560195EC48FC5661D9C9A2F8A2E67DDF24F832EE8C62FDFB4A18B3F388371DA0B6DE3CFF312A7FEB

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 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 (01-22)
Approved for use through 05/31/2024. 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	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

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	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	1	"Standing Document (SD1): WG8 Projects: ISO/IEC 14443, Proximity Cards (PICCS)," ISO/IEC JTC1/SC17/WG8 (archive.org), October 25, 2010, pp. 1-6.	
	2	"Telefonica O2 Czech Republic prepares NFC payments," DmEurope, March 25, 2011, page 1.	
	3	MARKKANEN, "Telefonica, Samsung to Pilot SIM-Based NFC Payment Solution in Spain," IHS Global Insight, February 15, 2010, pp. 1-2.	
	4	"The Mobile Payments and NFC Landscape: A U.S. Perspective," Smart Card Alliance, September 2011, pp. 1-53.	
	5	"Tokenization Guidance: How to reduce PCI compliance costs, Version 1.0," Securosis, December 10, 2011, pp. 1-31.	
	6	"Tokenization: What's Next After PCI," RSA, 2012, pp. 1-8.	
	7	SEIFERT, "Verizon won't offer Google Wallet for the Galaxy Nexus because it uses a 'secure element'," The Verge, December 10, 2012, pp. 1-2.	
	8	"Visa and Google Sign Licensing Deal to Boost Mobile Payment Adoption," Visa, September 19, 2011, pp. 1-2.	
	9	"Visa Best Practices for Tokenization Version 1.0," Visa, July 14, 2010, pp. 1-4.	
	10	CROSMAN, "Visa Certifies BlackBerry, Samsung And LG Phones For PayWave NFC Payments," Payments Source, January 10, 2012, pp. 1-2.	
	11	"Visa Completes Acquisition of Rambus Payments Portfolio," Business Wire, October 22, 2019, page 1.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	12	"Convenience for customers. Profits for you," Visa PayWave (archive.org), January 2013, pp. 1-2.	
	13	"Verizon User Manual: Samsung Galaxy SIII," Verizon, January 2012, pp. 1-204.	
	14	"World leader in proven and efficient cards for EMV deployment," Gemalto, February 2010, pp. 1-2.	
	15	BECKER, "29C3: A Rambling Walk Through an EMV Transaction (EN)," YouTube, https://www.youtube.com/watch?v=VdNm9JJmCzg, December 30, 2012, pp. 1-2.	
	16	"ARQC and ARPC Generation and Validation," YouTube, https://www.youtube.com/watch?v=I1XTn175FFk, Paragon Application Systems, July 25, 2012, pp. 1-3.	
	17	"CardVault by 3Delta Systems - Securing Credit Card Payments for B2B and B2G through Tokenization," YouTube, https://www.youtube.com/watch?v=h3zuiLiF51k, February 1, 2010, pp. 1-3.	
	18	"CardVault by 3Delta Systems - Securing Credit Card Payments for B2B and B2G through Tokenization," Transcript of YouTube, https://www.youtube.com/watch?v=h3zuiLiF51k, February 1, 2010, pp. 1-3.	
	19	"Credit Card Processing with EPX BuyerWall Tokenization," YouTube, https://www.youtube.com/watch?v=_7E5hj9li4g, December 21, 2010, pp. 1-3.	
	20	"Credit Card Processing with EPX BuyerWall Tokenization," Transcript of YouTube, https://www.youtube.com/watch?v=_7E5hj9li4g, December 21, 2010, pp. 1-7.	
	21	"Find out how PayPal works," YouTube, https://www.youtube.com/watch?v=dn42Y-2uFQM, March 14, 2012, pp. 1-2.	
	22	"Google checkout," YouTube, https://www.youtube.com/watch?v=-UeYkxePW2c, June 29, 2006, pp. 1-2.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	23	"See Google I/O 2011: Google Checkout: A Foundation For Payments," YouTube, https://www.youtube.com/watch?v=7ts7Lkykn0E, May 13, 2011, pp. 1-2.	
	24	"See Google I/O 2011: Google Checkout: A Foundation For Payments," Transcript of YouTube, https://www.youtube.com/watch?v=7ts7Lkykn0E, May 13, 2011, pp. 1-64.	
	25	"Google I/O 2011: How to NFC," YouTube, https://www.youtube.com/watch?v=49L7z3rxz4Q, May 10, 2011, pp. 1-2.	
	26	"Google I/O 2011: How to NFC," Transcript of YouTube, https://www.youtube.com/watch?v=49L7z3rxz4Q, May 10, 2011, pp. 1-62.	
	27	"Google I/O 2012: Introducing Google Wallet Cloud APIs," YouTube, https://www.youtube.com/watch?v=tpEGuSwv1fY, June 29, 2012, pp. 1-3.	
	28	"Google I/O 2012: Introducing Google Wallet Cloud APIs," Transcript of YouTube, https://www.youtube.com/watch?v=tpEGuSwv1fY, June 29, 2012, pp. 1-40.	
	29	"Google Nexus S by Samsung at CES 2011," YouTube, https://www.youtube.com/watch?v=5ZjtXH9S9KM, January 11, 2011, pp. 1-2.	
	30	"Google Nexus S by Samsung at CES 2011," Transcript of YouTube, https://www.youtube.com/watch?v=5ZjtXH9S9KM, January 11, 2011, pp. 1-2.	
	31	"Google Payments Live - Google Wallet updates," YouTube, https://www.youtube.com/watch?v=1pxkQ1mFjNA, August 23, 2012, pp. 1-2.	
	32	"Google Payments Live - Google Wallet updates," Transcript of YouTube, https://www.youtube.com/watch?v=1pxkQ1mFjNA, August 23, 2012, pp. 1-40.	
	33	"Google Wallet Demonstration," YouTube, https://www.youtube.com/watch?v=6tBAB5ls5vM, May 26, 2011, pp. 1-2.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	34	"Google Wallet Demonstration," Transcript of YouTube, https://www.youtube.com/watch?v=6tBAB5ls5vM, May 26, 2011, pp. 1-2.	
	35	"Google Wallet Hands-On - Engadget," YouTube, https://www.youtube.com/watch?v=5s9wYEkRAgs, May 26, 2011, pp. 1-3.	
	36	"Google Wallet - How to Setup and Use this Exciting NFC Technology," YouTube, https://www.youtube.com/watch?v=_ay1FfLCsHs, July 26, 2012, pp. 1-3.	
	37	"Google Wallet - How to Setup and Use this Exciting NFC Technology," Transcript of YouTube, https://www.youtube.com/watch?v=_ay1FfLCsHs, July 26, 2012, pp. 1-7.	
	38	"Google Wallet Make Your Phone Your Wallet by Google," YouTube, https://www.youtube.com/watch?v=qRVQTQlJV0g, February 18, 2013, pp. 1-2.	
	39	"Google Wallet Make Your Phone Your Wallet by Google," Transcript of YouTube, https://www.youtube.com/watch?v=qRVQTQlJV0g, February 18, 2013, page 1.	
	40	"Google Wallet Product Launch," YouTube, https://www.youtube.com/watch?v=am8t6iZ7up0, May 27, 2011, pp. 1-3.	
	41	"Google Wallet Product Launch," Transcript of YouTube, https://www.youtube.com/watch?v=am8t6iZ7up0, May 27, 2011, pp. 1-56.	
	42	"Google Wallet Walkthrough," YouTube, https://www.youtube.com/watch?v=xmbRSXYdFFs, February 13, 2012, pp. 1-2.	
	43	"How does Google Wallet work? Really well!," YouTube, https://www.youtube.com/watch?v=jY2p-pNkjHA, December 7, 2011, pp. 1-2.	
	44	"How does Google Wallet work? Really well!," Transcript of YouTube, https://www.youtube.com/watch?v=jY2p-pNkjHA, December 7, 2011, pp. 1-2.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	45	"How Does PayPal Work?," YouTube, https://www.youtube.com/watch?v=MdrPOCCFQ2k, July 24, 2012, pp. 1-2.	
	46	"How To Use Google Wallet On Android," YouTube, https://www.youtube.com/watch?v=6DeiEVBIBcs, October 28, 2011, pp. 1-2.	
	47	"How To Use Google Wallet On Verizon Galaxy Nexus - Pocketnow," YouTube, https://www.youtube.com/watch?v=AZ8t757ZfUs, April 20, 2012, pp. 1-2.	

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	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

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	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

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.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/528,073	**01/12/2023 02:28:24 AM ET**	**WYAT-0002.USD1C1C1C1C1C**

Title of Invention

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4809	FILED BY	Jose Garcia
PATENT CENTER #	61424667	FILING DATE	11/16/2021
CUSTOMER #	136197	FIRST NAMED INVENTOR	David WYATT
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 50

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
WYAT-0002-13C12US_IDS_transmittal_form_4.pdf	8	Information Disclosure Statement (IDS) Form (SB08)	1236 KB
Google_Wallet_Cloud.pdf	3	Non Patent Literature	1396 KB
Google_Wallet_Demonstration.pdf	2	Non Patent Literature	775 KB
Google_Wallet_Hands.pdf	3	Non Patent Literature	1438 KB
Google_Wallet_updates.pdf	2	Non Patent Literature	807 KB
Google_Wallet_work.pdf	2	Non Patent Literature	22 KB

How_PayPal_Work.pdf	2	Non Patent Literature	789 KB
How_to_NFC.pdf	2	Non Patent Literature	764 KB
MARKKANEN.pdf	2	Non Patent Literature	772 KB
NFC_Technology.pdf	7	Non Patent Literature	124 KB
Paragon.pdf	3	Non Patent Literature	1278 KB
PayPal_works.pdf	2	Non Patent Literature	776 KB
Pocketnow.pdf	2	Non Patent Literature	820 KB
RSA.pdf	8	Non Patent Literature	5143 KB
3Delta.pdf	3	Non Patent Literature	47 KB
BECKER.pdf	2	Non Patent Literature	810 KB
BuyerWall.pdf	7	Non Patent Literature	112 KB
CardVault.pdf	3	Non Patent Literature	1472 KB
CROSMAN.pdf	2	Non Patent Literature	729 KB
DmEurope.pdf	1	Non Patent Literature	515 KB
EPX.pdf	3	Non Patent Literature	1305 KB
Exciting_NFC_Technology.pdf	3	Non Patent Literature	1298 KB
Foundation_For_Payments.pdf	2	Non Patent Literature	810 KB
Google_API.pdf	40	Non Patent Literature	746 KB
Google_checkout.pdf	2	Non Patent Literature	795 KB

Google_Checkout_Foundation.pdf	64	Non Patent Literature	1183 KB
Google_NFC.pdf	62	Non Patent Literature	1150 KB
Google_Payments_Live.pdf	40	Non Patent Literature	751 KB
Wallet work.pdf	2	Non Patent Literature	823 KB
Wallet_by_Google.pdf	1	Non Patent Literature	15 KB
Wallet_Demonstration.pdf	2	Non Patent Literature	28 KB
Wallet_Google.pdf	2	Non Patent Literature	849 KB
Wallet_Launch.pdf	56	Non Patent Literature	1025 KB
Wallet_On_Android.pdf	2	Non Patent Literature	784 KB
Wallet_Product_Launch.pdf	3	Non Patent Literature	1312 KB
Wallet_Walkthrough.pdf	2	Non Patent Literature	754 KB
WG8_Projects.pdf	6	Non Patent Literature	4118 KB
World_leader.pdf	2	Non Patent Literature	1906 KB
Samsung_CES.pdf	2	Non Patent Literature	22 KB
Samsung_CES_2011.pdf	2	Non Patent Literature	823 KB
Securosis.pdf	31	Non Patent Literature	9201 KB
SEIFERT.pdf	2	Non Patent Literature	779 KB
Smart_Card_Alliance.pdf	53	Non Patent Literature	22963 KB
Verizon_1_of_3.pdf	70	Non Patent Literature	15740 KB

Verizon_2_of_3.pdf	70	Non Patent Literature	16395 KB
Verizon_3_of_3.pdf	64	Non Patent Literature	14961 KB
Visa_and_Google.pdf	2	Non Patent Literature	1100 KB
Visa_Best.pdf	4	Non Patent Literature	870 KB
Visa_Completes.pdf	1	Non Patent Literature	709 KB
Visa_PayWave.pdf	2	Non Patent Literature	811 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
WYAT-0002-13C12US_IDS_transmittal_form_4.pdf	5E70D693D28972B92B219403B10E9073E2D866E13075ECCDDC5CD34275B1DF17B0D0E4D22E47620EF11388E751E3BFD6208192E93AD9693CCE61F632BE057297
Google_Wallet_Cloud.pdf	B6F206DBCC53DD0CC7972D397A54DFE1452E43EEED4B4D18CF22D3F5A86D62931990CE2617FA530A9377EE221D5B2D5727435A83D23E2C868EFA1AEC502381A5
Google_Wallet_Demonstration.pdf	CDF5E3E39689FDFF4505A68CE3500BD63A443ACB80E22691EF26505C4ABA564306AF35D24ED429545F39CE392010A9CEB4E87CF3E41BAE1FEE4C0507FFBBAC0B
Google_Wallet_Hands.pdf	F46B216F42A7A7BFBB67B6BCC5DCADFFF3D3F14C9BA313C7089CCAB9627894E56F4A5C9CF32737F1E37D1D5BA899DF765D5109F2228C5955C4749D63150BCEA7
Google_Wallet_updates.pdf	49BA06569961F8F3EB65593933B07CA67589DEEF5D1675BA6BE5DAC44C89C31868B99266E16B789C4966026D2E5B4DEBBA6A30F298BEE6C5D44F206120D19050
Google_Wallet_work.pdf	828A4D631937EBF37AC47EF3141F381AACAD491A908FC6102DE3C565AA3F811538344B6DC29EBAF87A95A8DD18ED5162D

	A0826DB678EBE3029D62A48884D3083
How_PayPal_Work.pdf	035B5005566DB198EC1EDFA5FEFEF19E6DD3E30A3FCB92A16305E364F8108AE86EA3670F7ADDD3C4D429D3027CAAE144968335248BF3C0D5F80EECD1C1748684
How_to_NFC.pdf	397A3713D95403C73A600EB29202AD7AFF64DAF1F332CAA762CFC3042519D9FDED5276A2272107ABB8B3CC1E5BC7C5AC5564B99E31654C56EC94DEBBB26D40E8
MARKKANEN.pdf	96E9C15ECE817D004BE536A2DBFA538018C936C0232A69C7F457E555B786240770AF10B69765AF3EE55F436FF16D247759B5383EA6B935B443F655059407579E
NFC_Technology.pdf	21BDC2275F639A45771600E656F9737AA6B12CF3AE477D4336FD3CCD80FD8C57D4280900FCE4A4627F6041828B83233105DE5683693D7763CACAB085B5C310B9
Paragon.pdf	0B87C16EFD6DBF194FABA3861A3C19195825F83A5B69DB480402C8D634F45F38190EF6FB67B133EAF424C5F4892B8D0135A5386719AD5BB6152DD11189545417
PayPal_works.pdf	A69C192BAE071C5A253C1BE11BC964161F1F67AF1FDD14927A3B850BF1004FC0871C5E11729E3B4D076B706DDD7B5441CA1846AD075772412A7C1CF15CAC6618
Pocketnow.pdf	B7010092212F97F7209D641CDE35B9EFBFD4A592CE2AFA9EBA24390B3DDBE059697D4E1C6C8375542DAB76FA247F215D7DB1887DDA59E43B933D1C4AEC8DD3AA
RSA.pdf	7DE349EF70CBE408BD36C605E88072A7640DCFD802E6AF264B602DA955A58362223E553FB13CE7370DFAC2DC77DEFFA50771662E378012E3CE2402C0C343AC7A
3Delta.pdf	5F58BF76E0A65E05FC7A09B1DDD2A3C23B2954248DB941337FC8E7F700F8EC601B7CB134D1774C0A0D1F949B43ADB8282C809CC9A8C336691BBB15AAB2FA44B5
BECKER.pdf	7AE3168987BC803BF6021F4321284813FB5D5E65C14977C0B5A6A3CBC5963F29337C1BC0F0DA67626497ECA363C8F97E1F4

	8531217F359EF9BB5EAF0681C1050
BuyerWall.pdf	176A7116AFC2B862606470EE7E266B280E2BD452E21658D1A CB7FA65FBE9B086C8B26C07FB053984CF4D5C65B16F1A0A2 C3C387C43FEF85DBA58F220A87D3B64
CardVault.pdf	3EBC0558D09B9D98E4BB26775641CD309F394C5ACC8C14074 B7FC477E5A544F9463EED1A2AD7C82C3A488AAD6FD5CBCD 0BC039FC5CE6366AE7CDFF1D8E91691D
CROSMAN.pdf	79CE5973DB99844D147A1E6A600283347F9F28F1F464906FA0 CA9251E8B95BE3A12608C11DB3C45970C78C620CCCBC8C88 79CF1DFADFC0339B0991B420277445
DmEurope.pdf	D0193DFD7FF6542DBFD4542CA950AA08BD85C7F7473622E6B 7C3B2CB0A184E12AF18FBA4552611FD51243CFCC04F4484D8 9E1C3C5C1130AD38FACA3684DEEEF2
EPX.pdf	FC2AD534B54D2DD40ADAEDD7EBDA2A9E1DBBC5A8241E2E2 FFAC139EBD828E6C0E282E78C708F322A07AD018E398C49C7 AC2A4C07D8D9848B6A10C2D12E3781DB
Exciting_NFC_Technology.pdf	685F9940825018B8E2341557224608CAF6AA32041B5F13DC6C 26F856E8C64C4C782D5F69FB3654FA417CEC2BD00B156D0E3 1255849B9AEECFFA5C015CB67BFCD
Foundation_For_Payments.pdf	797359B1EF874B7BB1C6C21F0AFE7D10E1C52D3544EF8779B 080A6D9C3EE57F53A484B9741A0568ABC97D23D97D616B084 768B2B6B9D2706EFC600CD3BC3EA4D
Google_API.pdf	D62D83D2418C28439D5D885D267180506669A59785B882A87B 5EA250F2BD43AAA9AD7C764D846A49A9773F57B3754ED8657 A03A38A3B9A68C63C6602F5CEE728
Google_checkout.pdf	8E87C7C4A286876577F861B84EDE72639133271E5DCEB2B4E B2C88EC293024EF2DD27F53137BCE5F1E2CB52FE089AEB45 E8872F6C2160B95E5032F01847A5C7C
Google_Checkout_Foundation.pdf	19C9D87386B08AA4FD0077E52123F86675A593B42E5E287742 C9E431F2B52AD74C21F7BB992AB012AA6D026F79B56225E75

	3302143EA60D805E77492386F4E37
Google_NFC.pdf	0499C68DAD4A7F65FE610E9786FAEF18B8689DCD17EA0012E7BCE20D30283CFC1CC58E1F6A60715EE0E0A2D10ACD5D6EAF30A4F3C708B2CA4CD5BFAC7AA07D99
Google_Payments_Live.pdf	3194CC69D59F5CAF93E304819107E7DAC26C20685EC1E9CF05E8CF2F7C076CA53FB0A94A06FB38725E1FF42F6917C18A13D6C7211968E6360438AB63E625A5A3
Wallet work.pdf	0371B369633DDCA25DD348EEFF0F93A4721B33787F5A8C7C7EBD3892774950A2A7C56DEEE310503210FC532638958FB3A7A696F2E52A3E8D80CE0C31648F6986
Wallet_by_Google.pdf	847808F7887C8445CC3E7158CCB4BCF0D0C9E4C0AB3F2567025FA20A9DB7033C73D436A3A804BD0132C4C302FA12193E1ACCA290B6340122BF4C03DE53DE24FF
Wallet_Demonstration.pdf	D74DAA4ADDEFAC9E0E2564BCF70DB5D481F036DA823B07190D9A03372B6AE1D251DA2ACC98820453A3B9C4C827EF145DE1613B466764D2D9F92529521A6A3C70
Wallet_Google.pdf	8B79366116A8C3BBC5869EAF1BFE11981BE0DC9DE7C1095C6BCDD35F1B9A69199439A4710F8C2DDFF1FE95B45955A7563B31B1AD5C08CC018A8C68F79636D189
Wallet_Launch.pdf	02083F93DCFB96309CDE6CA1B2343DAAF2D8A2699D47128D4BDA695EACCED01A38782BBFDB6F66EA905BCE240CA596B958D91CFDB0969E26D475486A19449CF9
Wallet_On_Android.pdf	A353DAE20A3767618C03E997A9F5084B775D4FBD3542C83F966A54D655497448A153389B80FF51F3ACB42DD44FD8EB5679A2D5AFBE6652CE0AC65C72DB396B37
Wallet_Product_Launch.pdf	0F61528E884E682744497C155ACCEB542CC9682F9925647683ADF074611828D8A4BA9138E448F059B94BD2454FE96A2EDC6AD65EE291B9C674B38E661A5E437F
Wallet_Walkthrough.pdf	1153C63A606DCB1BC1EBB86C186F5BFE931A6045E00FF3679141B38F9722C2E080746CD2104FEB73F9C269B35A3D380EDF

	DC4BF2DE9729EB675347973D74E4B7
WG8_Projects.pdf	27A492D99A1D0A9086D45D113773E32CDC2BFF721FE98090B3A96A4E32AB61C3AD54782DCD3FE57385E4BC8CA25123C762B2BCF8E6FF82E1D6E3CECA7152ECD8
World_leader.pdf	3D8EB2B23D0F0E8B878986CCB252317CD30F08B9FAA1CC8534DDE7576CD0097EAC59F88FF194DB6B8CF029DC6EA54122FB946BE1BC442A950A17C5CCA0C04CDF
Samsung_CES.pdf	9B9BFD06BD02652E9C098E0B2BAB3AFE53E4FC406E080E2D9C8220383F1EF8784469BD3008C631E129D2E2EE4397C1DA0716E0608EC81E8C894B2339DB86F85F
Samsung_CES_2011.pdf	05BB81954FDB00527DE4D9304A420559ADB891292F2D631FEE6823691998D267072B02FC55B38CD1A7F43763E175586F975C298E22A124DC75B86AE099917667
Securosis.pdf	F270B900A99253A6269E7C36147DB4F6698CBBD29D3EB51BC06E65493EFE4FDB88A6560C77C38036A26A250EC012814A28D4AD20942C4D1140F05260054BB409
SEIFERT.pdf	737CE3D851358447FC0F73A90A454BAED0409CCD60E9FED1E39C2774550B3719D50B2B37A382A33257F5F9FB28E0DD9027EE61ADB12AA08F502923C541D1C053
Smart_Card_Alliance.pdf	98AB0621D0AF0B237C70DA5B48A493B54DE0055FC58CB4EDDCECD53AE2EC17349A36B20E47B33BD367EDDAFF9755346382ABEB2330DAEB44D12D61B56A9A903D
Verizon_1_of_3.pdf	2908F01FEA2A8F32FB71FB9409C7C165767ABD9B2F7743A08E45DABE28530F2E1A991FFA0CE93DA15A123D964B3DD8254345373A954E63D22DE7C21F423958A0
Verizon_2_of_3.pdf	0429CC0F0DBE0B76A1A17BFE6B6A2CAF856FCD71D601B446F3CFD5F2959D51686F0C38A2D452901018E74FF75B0618821A913374D1554C04541930FD7722292A
Verizon_3_of_3.pdf	7EFB00955B6DF940179F345523499EB22385BFC14A53012B223D62ABE4885406AE41F5982E6D8E5AD2C660C3B555CACF383

	6561AF2AEA10A49AD30D2A4CF07D4
Visa_and_Google.pdf	F4F4F8A0FE2734FE22127DBB67A34F8A87CCB77CF25946AF2770B72DC9E6475ABC4FDA422F2989B52BC16D2B359E7009473071B9A1EE3692870EE84615A29AAA
Visa_Best.pdf	092C0EAF5A90E7AFFA4E90C6B979317A42E71C9384C640D736CE76896B6578E186A45089FD790AC5871E2DE152C8B8AA3AB9A071DCDE2E094AAB5730AEAF83B7
Visa_Completes.pdf	61707E6231D3C5DA19A0E989AD084F71611C9DE5E02CCD0B8FAC82E1B056DDE2A63D509D6D0AE27F8791098FD61BE610C1E2F14364EEFA2500C053E9A4EDA94E
Visa_PayWave.pdf	C0FE1C7C3C50168EBCE5C979A38365CEAF943B4C822874DCB0E4248DD2AAABD78E15340ACE90EA1E9C078DDE4EC67E2AFD49CE6FE34C5490BAC0F9C56C4C2844

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 filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

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

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

New International Application Filed with the USPTO as a Receiving Office

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

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

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. 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	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

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	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	1	Motorola MotoACTV Smartwatch, http://www.manualplanet.com/pdf/watches/motorola/motorola-motoactv-gpsfitness-tracker-quick-start-guide.pdf, 2012, pp. 1-2.	
	2	PEREZ, "New NFC-Enabled Phones to Hit Europe," ReadWriteWeb, February 18, 2011, pp. 1-3.	
	3	WESTER, "New Samsung Galaxy S4 phone includes NFC, innovative barcode technology; New Samsung smartphone adds a number of features that may spur mobile payment adoption," Mobile Payments Today, March 15, 2013, Networld Media Group, pp. 1-2.	
	4	"NFC Focus: Which Smartphones Have NFC?," International Business Times News, August 9, 2012, pp. 1-3	
	5	"NFC for mobile operators; Maximizing opportunities in the mobile NFC marketplace," Gemalto, November 2009, pp. 1-2.	
	6	CATHELINAIS, "Nice, the first city to switch to contactless payment," 01net.com, May 21, 2010, pp. 1-6.	
	7	CLARK, "Orange to offer Samsung Wave 578 NFC across Europe - but not in the UK," NFC World, February 14, 2011, pp. 1-4.	
	8	CLARK, "Orange to roll out NFC services across Europe in 2011," NFC World, December 16, 2010, pp. 1-3.	
	9	"PayPal Credit Card Tokenization Extension - Magento Connect," Magento Extension Marketplace, http://www.magentocommerce.com/magentoconnect/catalog/product/view/id/18715/s/paypal-credit-card-tokenization-extension-4490/, October 5, 2013, page 1.	
	10	Nanninga, "PayPal Credit Card Tokenization in Magento," SitePoint, September 30, 2013, pp. 1-11.	
	11	"Payment Card Industry (PCI), Data Security Standard, PCI DSS Applicability in an EMV Environment, A Guidance Document, Version 1," PCI Security Standards Council, October 5, 2010, pp. 1-12.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	12	"Standard: PCI PIN Transaction Security Point of Interaction Security Requirements (PCI PTS POI), Version: 1.0, Information Supplement: ATM Security Guidelines," PCI Security Standards Council, January 2013, pp. 1-44.	
	13	"PayPal NVP API Developer Reference Enterprise Edition - eBay," August 28, 2012, pp. 1-382.	
	14	"Rambus' Bell ID to support Android Pay," Rambus, February 18, 2016, page 1.	
	15	"RIM implements Bell ID's Token Manager software for mobile payments," WMI Company News, January 23, 2013, World Market Intelligence Private Ltd., page 1.	
	16	LAI, "Samsung and Visa join forces to enable NFC mobile payment at 2012 Olympics," Engadget, April 1, 2011, pp. 1-6.	
	17	"Samsung and Visa Showcase Mobile Payments at the London 2012 Olympic and Paralympic Games," Business Wire, May 9, 2012, pp. 1-4.	
	18	WARREN, "Samsung and Visa Take NFC Mobile Payments Global," Mashable.com, February 25, 2013, pp. 1-2.	
	19	HASELTON, "Samsung and Visa team up for NFC mobile payments at London 2012 Olympics," Boy Genius Report, March 31, 2011, pp. 1-3.	
	20	"Samsung and Visa to Showcase Mobile Payments @ the London Olympics," Samsung Global Newsroom, May 9, 2012, pp. 1-3.	
	21	"Samsung Announces Launch Dates for Groundbreaking Mobile Payment Service: Samsung Pay," Samsung Global Newsroom, August 14, 2015, pp. 1-2.	
	22	GROTTA, "Samsung Begins to Phase Out Support of MST for Samsung Pay," PaymentsJournal, February 22, 2021, pp. 1-3.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	23	MURPH, "Samsung cooks up its own NFC module, destined for the Nexus S?," Engadget, December 1, 2010, pp. 1-2.	
	24	MOLEN, "Samsung Galaxy S III for Verizon Wireless review," Engadget, July 9, 2012, pp. 1-10.	
	25	TRENHOLM, "Samsung Galaxy S3 is Olympic phone for no-touch payments," CNET, May 9, 2012, pp. 1-2.	
	26	'Samsung Google Nexus S - Full Phone Specifications, Reviews: Royal droid," GSMArena.com (archive.org), November 2010, pp. 1-2.	
	27	'Samsung Google Nexus S review: Royal droid," GSMArena.com (archive.org), February 11, 2011, pp. 1-2.	
	28	'Samsung partners with FeliCa for Japanese NFC solutions, unveils 2012 Olympics' mobile payment app with Visa," Engadget, February 24, 2012, pp. 1-3.	
	29	CLARK, "Samsung picks NXP for S3," NFCW, May 14, 2012, pp. 1-2.	
	30	'SAMSUNG to Acquire LoopPay, Transformative Digital Wallet Platform," Samsung US Newsroom, February 18, 2015, pp. 1-2.	
	31	HEUN, "Samsung to Unveil NFC Smartwatch - Has Wrist-Payments' Time Come?," Payments Source, September 2, 2013, SourceMedia LLC d/b/a Arizent, pp. 1-2.	
	32	'Samsung's New Secu-NFC Chip Enables Secure Mobile Payment by Enhancing NFC with Security Features," Plus NEWS, November 30, 2011, pp. 1-2.	
	33	NANNINGA, "Save Credit Cards in Magento with Our New Paypal Extension," Classy Llama, August 15, 2013, pp. 1-4.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	34	"Shift4 Releases New Technology to Insure the Security of Its Merchants' and Partners' Payment Processing," Hotel Online (archive.org), October 5, 2005, pp. 1-2.
	35	"S-Pay: What is MST?," Samsung Levant, September 22, 2020, pp. 1-2.

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	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

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	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

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.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/528,073	**01/12/2023 02:09:45 AM ET**	**WYAT-0002.USD1C1C1C1C1C**

Title of Invention

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4809	FILED BY	Jose Garcia
PATENT CENTER #	61424648	FILING DATE	11/16/2021
CUSTOMER #	136197	FIRST NAMED INVENTOR	David WYATT
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 49

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
WYAT-0002-13C12US_IDS_transmittal_form_3.pdf	7	Information Disclosure Statement (IDS) Form (SB08)	1236 KB
MURPH.pdf	2	Non Patent Literature	1799 KB
Nanninga.pdf	11	Non Patent Literature	5410 KB
NFC_for_mobile_operators.pdf	2	Non Patent Literature	1832 KB
NFC_Smartwatch.pdf	2	Non Patent Literature	729 KB
NFC_World.pdf	3	Non Patent Literature	1717 KB

NFCW.pdf	2	Non Patent Literature	642 KB
Payment_Card_Industry.pdf	12	Non Patent Literature	7876 KB
Business_Wire.pdf	4	Non Patent Literature	1109 KB
CATHELINAIS.pdf	6	Non Patent Literature	2624 KB
CLARK.pdf	4	Non Patent Literature	2212 KB
Classy_Llama.pdf	4	Non Patent Literature	1389 KB
FeliCa.pdf	3	Non Patent Literature	1019 KB
GROTTA.pdf	3	Non Patent Literature	983 KB
GSMArena.pdf	2	Non Patent Literature	1073 KB
HASELTON.pdf	3	Non Patent Literature	1674 KB
International_Business_Times.pdf	3	Non Patent Literature	970 KB
LAI.pdf	6	Non Patent Literature	1345 KB
LoopPay.pdf	2	Non Patent Literature	561 KB
Magento.pdf	1	Non Patent Literature	388 KB
Mashable.pdf	2	Non Patent Literature	748 KB
PayPal_5_of_13.pdf	30	Non Patent Literature	16398 KB
PayPal_6_of_13.pdf	30	Non Patent Literature	19630 KB
PayPal_7_of_13.pdf	30	Non Patent Literature	12785 KB
PayPal_8_of_13.pdf	30	Non Patent Literature	5647 KB

PayPal_1_of_13.pdf	30	Non Patent Literature	15334 KB
PayPal_2_of_13.pdf	30	Non Patent Literature	17236 KB
PayPal_3_of_13.pdf	30	Non Patent Literature	22001 KB
PayPal_4_of_13.pdf	30	Non Patent Literature	22603 KB
PayPal_11_of_13.pdf	30	Non Patent Literature	16996 KB
PayPal_12_of_13.pdf	30	Non Patent Literature	11931 KB
PayPal_13_of_13.pdf	22	Non Patent Literature	15402 KB
PCI_PTS_POI_1_of_2.pdf	30	Non Patent Literature	18011 KB
PCI_PTS_POI_2_of_2.pdf	14	Non Patent Literature	8792 KB
PayPal_9_of_13.pdf	30	Non Patent Literature	17093 KB
PayPal_10_of_13.pdf	30	Non Patent Literature	16828 KB
Samsung_Pay.pdf	2	Non Patent Literature	964 KB
Shift4.pdf	2	Non Patent Literature	1706 KB
TRENHOLM.pdf	2	Non Patent Literature	1139 KB
WESTER.pdf	2	Non Patent Literature	890 KB
Plus_NEWS.pdf	2	Non Patent Literature	880 KB
Rambus.pdf	1	Non Patent Literature	715 KB
ReadWriteWeb.pdf	3	Non Patent Literature	1647 KB
RIM.pdf	1	Non Patent Literature	563 KB
Samsung_Galaxy.pdf	10	Non Patent Literature	5158 KB

Samsung_Global_Newsroom.pdf	3	Non Patent Literature	1692 KB
Samsung_Google.pdf	2	Non Patent Literature	892 KB
Samsung_Levant.pdf	2	Non Patent Literature	36 KB
Motorola.pdf	2	Non Patent Literature	946 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
WYAT-0002-13C12US_IDS_transmittal_form_3.pdf	E8F9662C840C33CF74178A92BD1829C7645747EB26A802ED12E1CDF6307F71904B95419B294EB20E078BEE49209BD45CE9EDF460301F3A713431337AAB1E019F
MURPH.pdf	3343EC02813F63AA251B29CCB759F410E7DA034EB61509565ACE5C9EFB123AEAF72763AA84F7C49FF21BD23F3C363C889D16EBBF249264F22730C98757B8C2BC
Nanninga.pdf	958C75487F5B101A3DF678BB33ECD2362EC70D1BB1E99FABF60F92FBB86C5E32EBE2ACB431B21C0FC3B99596EE2F29AED38D7D10FDA0D03AB4A851A1998F02A5
NFC_for_mobile_operators.pdf	68894F1EA5E57AFB428276AACEB67DCD87754F069DC06BE8C468402382602E46A6EF22F9B1E56929DAFD6071B57D0DD37C4C736D5ACECEE2C42DBCE88F2A0DFC
NFC_Smartwatch.pdf	7216E6FB9A7DBFA2E8C65E91A93623E3B7768ACBECBA0D1C5ECF5D6AF20D0A3CE3B46805B3AD220580186DA805E4FEA388EBCC888906FB1FF79261D1B2207285
NFC_World.pdf	9990DB3A91B2A162BE8A7131186E480FD515164903DC41D44B691329A44DA8A0148088C7102DFAE24355D1D5DF6C29BDC46067C259515B0A34AE3BCB543F3554
NFCW.pdf	0748C68CB295C0077BE7B8928744DED92BEB79BFA2E6D774

	E908A2AEEF7A4A9D6748A838206FB16F1E5C4295E044E61F2D3048568546686CD73C29BBE8D2FA4
Payment_Card_Industry.pdf	D548536D5AE1478E7351E8AAE2493CF8D203FF8D012F486EF1088DDCF885FBA6E70F5A8836711E8AC61B025E2D344E21F5171B54F1D8EEB7471FB13D2454F217
Business_Wire.pdf	9BBA328F64D067B28C7B507554458C1F8724977B81EA513E7E3BF45B90A68A1589DADA1C06AAFC4548A17BEACD5C3F2FAC9E180D40C6597C5805F8A53473C28F
CATHELINAIS.pdf	6E916ABFEE7615F6351CA0EE2774D195CAA14EABDC8DA1886EC415FC838AFFFFC9E5820F18109491 3BB9DA254A8E88B27DAB125AA0CB6F79BA313B36AAC3BCC1
CLARK.pdf	5542D017F144811C16CF888D6BBB7BF937D52EE45BAAC79445947646EF2CFEF1E289CE92E82BE16B6D177545AC495DF4B77FF43AF8A77FD40551ED6BB0F2376C
Classy_Llama.pdf	72B58E9ADC9D64B80D65D35E68476DE49AED4236C00680BC8AAC8D9849A6FEB3AFF61528270AAE548588993359408C15EA4DF7E053370311F3A4F8F59FB0CAB6
FeliCa.pdf	670F486FEC047C6C1A05C06ECEE07B5DB59E59999ED5D6F0D07CB42A663BDE44D62BA8124C00805BCCA25D2281511FE9DE077A1B5AE25FFC8BBCAEA458D2BAC7
GROTTA.pdf	FD48510D7BB56CA1A742C865728E869091FC6F2FC95539459F62C2CC299DFE18CFDA1E3CA4CBEBAF9948085D53DD91BEC83E1C4359ED9785F382C4A5EB235D68
GSMArena.pdf	F8AB00D2266A2F0638BF0DEEE9661533D41B7F3F1E02757A19C1E45523B10D894F323DAD77D3898BD9A68647F3614ECD542A905BABC187E19A0C0BC57479A3C7
HASELTON.pdf	3B7D85DE2D57659655D30DCA596E3C15B939FA21061DD1ABAC3031695BF7E0327E2979EE882A950F0C040D0D755A87E015047BF0E8E7FBBE6732B05F1DBFAD4C
International_Business_Times.p	591C8296C7326A16249AA877F4DF77F5FA1222CA14F49ECD1

df	3EEE469437C0869529539DA8E74FC2414298BF01CE7948FEC E28D4747812821499D614FDFE2FA81
LAI.pdf	3059934B176978C6E78F0C0FFC9F3B1CA3369EA0AE1291B518 0D3C009793D862B8B926ACEE4D027671DF0A4DDB46103914F 983126613D4694BAF81337131FFB1
LoopPay.pdf	7039BEEFF390C4B80E8AFFED67475DCDCBE0ECE48239F5B6 9CFEC0AF61457CA3E0CB46D8F2F52FF1B561BF840F17692D6 2D5FE6CB64B830BCD62791A79669F22
Magento.pdf	44AF16EA96332713F7D66853873ABB9F41D01E8CA30EB17FC C35C5F266C03B15DCB10425C21F0B7CDF1A57498136A6B343 6772372849322EB77B87F793066A9B
Mashable.pdf	3F0BA00846A5FCA74ECFF125CD4BC670652E67CBB6B4B1EA 4002C91634BBB681D6F408569CE24691BD2877D28667C30B22 6E67D782C07744F978BF9F5B3C2B34
PayPal_5_of_13.pdf	9CACF4F33E2096E277465D5963E5EE84B05C3BD88269101A5 80428F5463D0FC56D7281BEA8A6E6CE2F51BBD4F41317BD6E D333E0071F114AB9F74EBC8CE4C20A
PayPal_6_of_13.pdf	F7914E8F14A46A69FAE5D1B04F73DCD42BD7ECB560AE8C43 5D086A5F3B028D95D65C5151A476EEFD4C42822F609E91AF8 F3EE98A04E830DA6CE21368B5FDB108
PayPal_7_of_13.pdf	7CCBDDA691AB8E566F8B5119FDFE4528C0EE48A5A635BBE2 35EC5D2206E614F17F39EFFC674C7533BEA9F6A4840FFC537 422782BC1C94FD57C17C86E3BF121FC
PayPal_8_of_13.pdf	E27C2390D887B918E317E516BB462556ACFE0EA45F6DCAB50 5CC41F2A33BD16B0B3BD9B1131686908AAE8A7B97F336A92C 1712E183078ADFFF59D583AD575A95
PayPal_1_of_13.pdf	AC0FD0DE7855150CFFD10C179950A71811A00F4DFDDA72C4 1268C12A674B42E3CF9A01DD762BFB289E3678D3F005553396 CE3976FD1DC159820119642FC2E25E
PayPal_2_of_13.pdf	2C310F42691C9572B6CAF696A6AF5ED68CA7BD527685E7337

	58D9116A0DE0018A61402251695C2E458B629EE6367D254EE49ECB5BC8612CB9D9BCFE901D97760
PayPal_3_of_13.pdf	12B535B15206D4E8717E56AA41962AC82240A71075EFE1ADBC603E98753A52884D086476D3D285FEE6219107D844B60C55E1789953D65A10359A436CA290E475
PayPal_4_of_13.pdf	78315A5E792007E6F6142B05ECF1299D45B146C547EBBC14E7D7D841B7B3D298E3F0CE55D092B15951A5391E273194FD7964F6B4C5DE2E976D85BD2E038ECD19
PayPal_11_of_13.pdf	C6AFC974D2D88BF92CA5BBCC165E892141BC05DE02B95B0A327DFA058534261A4D206BCDB03AA724526433D425E4D0F36EC8E40C7B298A9D132BA89781F4FFCF
PayPal_12_of_13.pdf	05F22582C380EF3B605D38128FD1C8F5462123C46CC8227C71CA8C17D2012B87B4BAC78AB07E00A750ACB802CE14C3877CB2F057517D6F0F18745FE6277A86E9
PayPal_13_of_13.pdf	8CF0AB1E777DE8E0816A59757D3642EEC5E42929AF052936E7121818B3FE3868CE959249BE905466FFE8F6EE5F582BE06C83597CBA0BD788D31682B7CB2C4F2B
PCI_PTS_POI_1_of_2.pdf	C0B91A6103A6C07B88004B990A7D414E5913C9396630FC2CC244058EB58000E5B9A37F620883E47023FC67AA34E225EDCD7425793AA2DBD85187DC2BF20A9DA1
PCI_PTS_POI_2_of_2.pdf	FAF8888E206D4EE6F49A7FAC6C9853B5AA76FB6529797A8A98F86EEF5631E8927E3891AD31235B4F5EAC2EA329912C758F0ED8FDA450FAB62F885B76541A64FA
PayPal_9_of_13.pdf	58C0C122AD3BAF6747D0767190E7028CDF21432DDFC39D833FF603B3C868B37CF3E7C004E3EFA57396C5166256AB166F96F1572C029970825F6791858BAC587D
PayPal_10_of_13.pdf	26F5F95BEAB1B6A09781805A16344D399C7651F3CA87790583D7063930B5EE49EC8CD44389E0574DB9A19A1ADE2807D1BD71604358AE2F0787F7F22D4709A05E
Samsung_Pay.pdf	581D5F13A8CB2E23FEA45F0B826823C3CD9E92A8BB5CF3096

	C014191C7A99AD0CB2F7E15E58EAC39408DECC78B6E3D7EEDB91E85A10F146CC74353CAFD864C4A
Shift4.pdf	42F5EDB83F5B6F24A615A65FAA3075905F49A4E2CA85638BEBB17D75868E3B1431834668DEFD91F71A7AF3394C40A12C75A04DE24C27E8217B073ADEDEFA4D4D
TRENHOLM.pdf	D6E3A1ADDE798B4BE7AE403A39FC5C7FDF4E03AC0CDE0D564D8C1D31FE2204D57836A1DF056739A1AACEAC059539143E7DED32B80660A7DC0144182671042702
WESTER.pdf	206B8E60D15719ADCA9F5EE9A29F7FD7D5C64D261EDE01D91036A255713C93E7E58156E33D49199DFC5D10CE47D1C7D093F572495EE34CBE8CDBF25B6766AD0F
Plus_NEWS.pdf	C94575650FD55ECAE244F014B254DF475D23BECAE1F2BD7201DD5358D224239783AE873112734242B4B9FA6EB44FAEA9D5E4068F24AD36B2CBB106F7703F3506
Rambus.pdf	78310B3329B37D36B4842F7D1393C7792615E1676AB316E49CC95BA4498BDBF7AAFF2ED5D462DFB49AD57F02BF15F0EA0F83FF118C7C581FCFD6B474A501E2C6
ReadWriteWeb.pdf	A2A332300AED6C2E9517C2F7F5FF19ABCBA8C1BAFB15E9FC1A272377B938A7AE9BDBA49CFE1947A74C3543F6BB3647E33D5CC9D9A54876BE2177FA1F63D3CAA9
RIM.pdf	868BF8BE96D1E79F931C1BFC246DE2D6D91525D0962B3945D8D58FF12365DCF695B4F65C4B56B11066F01AB0ACD9CE3BE84C6A4AF7EDFCB3851F16D4487C6E32
Samsung_Galaxy.pdf	4257D3887702AD8610308A665E48511CEA9DE418B3FF3C956C08DFEBDC1B99A9B035708B201F5A369A762319C39CC13C3D713A3E2CB28CC5185386BED95A11C9
Samsung_Global_Newsroom.pdf	02507BBFF5B3F9948C806E2FC305B342085B008CC9A96227F0D10A9F69E401974C2197ADFE9933EC2246B9D92F761C29B101939C3DFA96A873CC7490588EE3C0
Samsung_Google.pdf	22BF35D2C3D91795D664F6742893B3DEB9C280C5297F36CFC

	C913CB022DC48F424F60BB78F13EDF7CAF283E94E1E8B2717780B92E52466261E9D42C1D39ACF0A
Samsung_Levant.pdf	F40563239657AFE4F2C1C636507E74190BE388D0246553B0159F720A82F6EA3F81635B3376E734E25CDEB73C9CC2DD0E0C83FD9F43F663BA811445C01676EFDA
Motorola.pdf	5A43B41EDECA9FCF0F787DA9B737A6E146C77E7B96386C1660EF71BF5BC8BB4F7276BB1055F0D4805B870AEE7DD55E523AFE932BD07E43F54E30040751 7B9763

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 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 (01-22)
Approved for use through 05/31/2024. 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	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

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	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	1	"EMVCO Publishes Technical Framework for its Payment Tokenisation Specification," EMVCO, March 11, 2014, pp. 1-2.	
	2	"Encryption and Tokenization: Which is best for your business?," Townsend Security, 2010, pp. 1-4.	
	3	MOLEN, "Engadget Primed: What is NFC, and why do we care?," Engadget, June 10, 2011, pp. 1-11.	
	4	"Exploring Google Wallet using the secure element interface," nelenkov.blogspot.com, August 27, 2012, pp. 1-11.	
	5	"Financial Cryptography," 5th International Conference, FC 2001 Proceedings, Grand Cayman, British West Indies, February 19-22, 2001, Paul F. Syverson (Editor), pp. 1-57.	
	6	"Gemalto to Provide Isis Mobile Commerce Platform with Trusted Service Manager (TSM) Solution," Business Wire, December 12, 2011, pp. 1-3.	
	7	"Google Checkout checks out, replaced by Google Wallet," Android Community, November 17, 2011, page 1.	
	8	"Google Checkout HTML API Short Attribute Reference," Google Checkout, Google Code (archive.org), March 27, 2012, pp. 1-4.	
	9	"Google Commerce: Building one wallet: Google Checkout is transitioning to Google Wallet," commerce.googleblog.com, November 16, 2011, pp. 1-2.	
	10	"Google Prepaid Cards," Wallet Help, Google (archive.org), October 3, 2012, page 1.	
	11	CLARK, "Google Unveils first Android NFC phone - but Nexus S is limited to tag reading only for now," NFC World, December 7, 2010, pp. 1-4.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	12	"Google Wallet launches officially on Nexus S 4G," Android Community, September 19, 2011, pp. 1-2.	
	13	GARSIDE, "Google Wallet mobile payments system launched to public," The Guardian, September 19, 2011, page 1.	
	14	BOULTON, "Google Wallet Mobile Payments Coming to New York, Francisco; Google Wallet will launch this summer to enable consumers to pay for goods by tapping their Samsung Nexus 2 4G Android phones at NFC-fitted sales terminals at Subway, Macy's and other retailers," eWeek.com, May 26, 2011, pp. 1-2.	
	15	FINGAS, "Google Wallet reaches the web, reminds most of us that it exists," Engadget, October 4, 2012, pp. 1-6.	
	16	RAPHAEL, "Google's Eric Schmidt spills clues about Android Gingerbread," ComputerWorld, November 15, 2010, pp. 1-3.	
	17	"Handset makers line up behind Isis NFC payment platform," Old GigaOm, September 27, 2011, pp. 1-2.	
	18	"How it Works," Wallet Help, Google (archive.org), March 12, 2013, page 1.	
	19	"How to find out IMEI number on Google Nexus S phone," Tech Notes Desk, January 10, 2013, page 1.	
	20	"La Caixa," Annual Report, 2010, Barcelona, Spain, pp. 1-190.	
	21	"INSIDE Contactless to Equip KTFMobile Payment Project Mobile Phones; Korean Manufacturer Confirms INSIDE's NFC Maturity by Embedding MicroRead into LG Electronics and Samsung Electronics Mobile Phones for its Mobile Payment Project," Business Wire, July 16, 2007, pp. 1-2.	
	22	CLUCKEY, "Is a contactless ATM inevitable? Bank of America seems to think so; the FI has filed a patent application for a 'Contactless Automated Teller Machine,'" ATM Marketplace, September 20, 2012, pp. 1-3.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	23	"Isis™ Launches in Austin and Salt Lake City; As Many as 20 Isis Ready™ Handsets to Be Available by Year End," Business Wire, October 22, 2012, page 1.	
	24	PEREZ, "Isis Revealed: Carrier-Led Mobile Payments Venture Shows Off Its New App, Announces Banking Partners," TechCrunch, February 27, 2012, pp. 1-6.	
	25	SADEWO, "Isis to officially launch on Oct 22, more supported devices announced," androidauthority.com, October 18, 2012, pp. 1-2.	
	26	"MasterCard Approves NFC Phones from HTC, Intel, LG Electronics, Nokia, RIM, Samsung Electronics and Sony," Professional Services Close-Up, May 10, 2012, Close-Up Media, Inc., pp. 1-2.	
	27	"MASTERCARD INC, FORM 10-K (Annual Report)," Filed February 28, 2007, for the Period Ending December 31, 2006, pp. 1-204.	
	28	"MasterCard, Visa and American Express Propose New Global Standard to Make Online and Mobile Shopping Simpler and Safer," Global Hub, Engagement Bureau, Press Release, October 1, 2013, pp. 1-2.	
	29	"Fact Sheet: Mobile Commerce: A New Way to Pay: MasterCard Mobile Commerce," May 26, 2011, pp. 1-4.	
	30	"McDonald's testing e-payment system," USA Today, May 29, 2001, pp. 1-3.	
	31	"Mobile Contactless Payments Trialled Live at Mobile World Congress 2010; GSMA, Samsung, Telefónica and Visa, with Giesecke & Devrient, Ingenico, ITN International and La Caixa, collaborate across industries to give Congress attendees an opportunity to experience NFC," Business Wire, February 15, 2010, pp. 1-3.	
	32	"Mobile Payment Bringing value to payments on mobile," Gemalto, November 2011, pp. 1-4.	
	33	WOO, "Mobile PayPass Meets Cloud in Google Wallet," Global Hub, August 1, 2012, pp. 1-2.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	34	HEUN, "Mobile Wallet Consortium Strives Cautiously In 2012; The telco joint effort proceeded more slowly than expected, but its leaders maintain that the mobile wallet business is big enough for lots of players," Section: MOBILE: ISIS, January 1, 2013, Page 47, Vol. 2, No. 1, SouceMedia LLC d/b/a Arizent, pp. 1-3.
	35	BELL, "Mobile's Gains Prompt More Banks To Move Beyond Cards For ATM Access," Payments Source, Section: DEBIT: Vol. 1, No. 1, May 12, 2011, pp. 1-4.

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	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

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	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

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.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/528,073	**01/12/2023 01:46:45 AM ET**	**WYAT-0002.USD1C1C1C1C1C**

Title of Invention

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4809	FILED BY	Jose Garcia
PATENT CENTER #	61424625	FILING DATE	11/16/2021
CUSTOMER #	136197	FIRST NAMED INVENTOR	David WYATT
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 50

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
WYAT-0002-13C12US_IDS_transmittal_form_2.pdf	7	Information Disclosure Statement (IDS) Form (SB08)	1237 KB
Global_Hub_Engagement_Bureau.pdf	2	Non Patent Literature	1475 KB
Google Prepaid.pdf	1	Non Patent Literature	376 KB
Google_Checkout.pdf	4	Non Patent Literature	3470 KB
Google_Commerce.pdf	2	Non Patent Literature	732 KB
HEUN.pdf	3	Non Patent Literature	1732 KB

How_it_Works.pdf	1	Non Patent Literature	451 KB
INSIDE.pdf	2	Non Patent Literature	916 KB
Isis.pdf	1	Non Patent Literature	757 KB
Android_Community.pdf	1	Non Patent Literature	467 KB
BELL.pdf	4	Non Patent Literature	1164 KB
BOULTON.pdf	2	Non Patent Literature	906 KB
CLARK.pdf	4	Non Patent Literature	2713 KB
CLUCKEY.pdf	3	Non Patent Literature	1441 KB
EMVCO.pdf	2	Non Patent Literature	1685 KB
Financial_Cryptography.pdf	57	Non Patent Literature	3150 KB
FINGAS.pdf	6	Non Patent Literature	3940 KB
GARSIDE.pdf	1	Non Patent Literature	884 KB
Gemalto.pdf	3	Non Patent Literature	878 KB
GigaOm.pdf	2	Non Patent Literature	1035 KB
La_Caixa_6_of_6.pdf	30	Non Patent Literature	17444 KB
La_Caixa_1_of_6.pdf	32	Non Patent Literature	21513 KB
La_Caixa_2_of_6.pdf	32	Non Patent Literature	22815 KB
La_Caixa_3_of_6.pdf	32	Non Patent Literature	23969 KB
La_Caixa_4_of_6.pdf	32	Non Patent Literature	23751 KB
La_Caixa_5_of_6.pdf	32	Non Patent Literature	22026 KB

MASTERCARD_6_of_10.pdf	23	Non Patent Literature	17955 KB
MASTERCARD_7_of_10.pdf	11	Non Patent Literature	9661 KB
MASTERCARD_8_of_10.pdf	23	Non Patent Literature	22363 KB
MASTERCARD_9_of_10.pdf	11	Non Patent Literature	5409 KB
MASTERCARD_10_of_10.pdf	68	Non Patent Literature	2896 KB
MASTERCARD_1_of_10.pdf	16	Non Patent Literature	15168 KB
MASTERCARD_2_of_10.pdf	18	Non Patent Literature	20531 KB
MASTERCARD_3_of_10.pdf	17	Non Patent Literature	17524 KB
MASTERCARD_4_of_10.pdf	9	Non Patent Literature	8309 KB
MASTERCARD_5_of_10.pdf	8	Non Patent Literature	5521 KB
Nexus.pdf	2	Non Patent Literature	571 KB
Professional_Services.pdf	2	Non Patent Literature	862 KB
RAPHAEL.pdf	3	Non Patent Literature	2247 KB
SADEWO.pdf	2	Non Patent Literature	534 KB
Tech_Notes_Desk.pdf	1	Non Patent Literature	404 KB
TechCrunch.pdf	6	Non Patent Literature	2920 KB
Townsend_Security.pdf	4	Non Patent Literature	3446 KB
WOO.pdf	2	Non Patent Literature	991 KB
McDonald.pdf	3	Non Patent Literature	1042 KB

Mobile_Commerce.pdf	4	Non Patent Literature	934 KB
Mobile_Contactless.pdf	3	Non Patent Literature	1066 KB
Mobile_Payment_Bringing.pdf	4	Non Patent Literature	2643 KB
MOLEN.pdf	11	Non Patent Literature	6042 KB
nelenkov.pdf	11	Non Patent Literature	7576 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
WYAT-0002-13C12US_IDS_transmittal_form_2.pdf	BA5830495ECB05C97C396842A418096913A6E649F75664D3958C60D9CB72FBCD84283D12C381C98A5D1F8300B27A2E65DFB0144E59DDF6C3BEC22FC610CC32E7
Global_Hub_Engagement_Bureau.pdf	1B2860549A9F1865136D4CE3E063C0FE6E3A4FAF018910007863734D65E5C569F0CFECF996FA01A0019C2B9A76CB689B9DEB760C764B665434789199C46603D7
Google Prepaid.pdf	8B959C8B9FF29691DA36109A27CA0546D1E5ED86E05C7C2D718BF7233732E5971CA4EC9838E68135651FD99EE59DFE227D3C1E4BB8953AD92156FEF958C1D03D
Google_Checkout.pdf	DE1F2BCF81860AE1700F454C78CB662CB8F2012C4BF435FBF9386171224F5A2374259149A295785CD3CB53F7CED26AEE8CD6E79BF92FDDC6D0778EABF6EFE3CD
Google_Commerce.pdf	D6A206586977D368963108F750504B9C64DF513A0277AA7DF4443390E8082E29D3CAB008CF227C7954E187BD02E65015A25FF3085AF9872EAE071C681F4D067D
HEUN.pdf	4518A78961CBC9DD99CC0245FA7782798E5599CE9D9FF2C40943E617400FADFB527A60B372B9839BC2CAC96FCD3ED7893CFCBAEB9685E874459A29FAB1558E25

How_it_Works.pdf	6A1075DBE81FC8DFFA36D02EC494923AF1949AF433B4C1ED6C2BDC0F74ED79F0D2D34B51A9E6B84EFC136F91DFD756E1865AE2C1E5BBD6661859ED884D80649B
INSIDE.pdf	06D31CC4E819EDF91CFB310231189A1DA08355775DFCDDF4EE9E253F98B94CEA1756F1296F3400EB146B0C24C3C6B3B87A862FF81C3B98A70D9130AE4190F406
Isis.pdf	0B1F28A30106AC28361C50B4C69409BE601C7A4FFE4A6DA75867F09CC2FC8062DFB32A49C3488C2218D96BBEABA26CCC7631994B1A1E8AB6E97C09378C65514C
Android_Community.pdf	C3BC9C2062C05D56BA3660C9F2D60486B0BEB99D18E73A594875AECC931B2634A7544F3FB23E57F1710789F76019F9AC8DC71F618DF2D18F6D854682C51537EE
BELL.pdf	315832184105E00308AAD8A29B95A000D6749F8CB7C65041F9566C441DD3162D1FC7A19009D00668D356569BBC482284FFFEDCEA7F1CFEE4F075B0AB357DA480
BOULTON.pdf	E6D39974975D00C9AB39E25494338B6DC0EEDB4F1D0D4DF00AB2B703A05F8FCD8D56657CDD2A7A603C4438CBAAFFF69ED36231A0A0679374E351C8B3927C19BA
CLARK.pdf	384376E17AF5B596674C2AC229D494E0F5ACC90454A41EC94C18184774A65C56ECAB0F4172F969E862E0B1544FB152BE402516752757C829747A0E56C46631F2
CLUCKEY.pdf	81DE99B649A5FAB49D3418750A508E9F1F6DF25034531987F96B6D18987D1AF0DEFCF0B7C5ABAC710815DBC8783FDF0530C0D2263CBC4E0E2C172D80D6170DD1
EMVCO.pdf	E49043EA9DE6EAB0687459483 8EFBF040F38176620AAD582C2EAA7AF1CC9ED9F5EC83021DEF43C8067A779F52D900B042896438A6C9AD9A50226F411ACD7095E
Financial_Cryptography.pdf	8AD5653B2E0B3E6D48A3A006BCDA86D880D9DC1DDDBE9CB2DFCA329662729C3497F2744875FF09CCF031E72EC1116C7F5A4425C24EAA7099CFBEFD6C4B4E0449

FINGAS.pdf	F5F5A38053FDCD7C45275A7CC8F5B1DF3178E0F710A9B443C0367EE949B9D01CF79A1F9440DB7D9444F744C68037ACD0D46841CE792929FD5B6FB364CF179E90
GARSIDE.pdf	CF87ECE84BC9B4ABA95B312829C5F63D0B681E82700761A0D2C40116CEC37B7EAAA27EEDD13D40A2FE6DD20AECD59AF4480F423F9FD46A2C3E1ABAC5E9F6E6F0
Gemalto.pdf	3D6D9B0AB8B7880DC398814B53D29D703969763EA27B3FC1857D3F7751313A5620E42EF0480F18B4B5BA4FBDC76B8CBFE833E9D80C5A11262D0A57D2FBD385A5
GigaOm.pdf	1350964A54E57749A04DF79088AE54D805D398FAD47C2196517DCC1FEB5398916789DE59319492D14578F7DDE32AF54C6931F60D26758A39B5DA607ACEEF0A53
La_Caixa_6_of_6.pdf	B985241C5F6784FC20C29002A7A7AF3D8F612BD40ED122824A6C1F5F6AC598952B6A997280F03FE5C8D815141A6270DF94913BE22320F63B77BC7FE47AAAA789
La_Caixa_1_of_6.pdf	6067EC177712DA341ACE17FCDFC84CC30E24FF87E635F26BF2F96FE9CB3B82FEADD90C94FE02CD9AB91CE35BF932C01D45B0B485DE6D04EB49A3E9CEC1D67FE7
La_Caixa_2_of_6.pdf	EF8BE7810751C2D53CDB859E9D4177268EAD1B4A05C8CD5D559846A1CDF5162D4E3DA4D3124BA3414196118AE05D3532573B91831742F2FDE10A4CCF3F107263
La_Caixa_3_of_6.pdf	9F15E16381D20F1AE4DD17CCCDB4D1B0CF9DA6D7ECB795527A97FA3BA6F4CD299F577DFBB9464B2DE61B074DFDA093258FA720376A3D187AD6D0B71CD55528FE
La_Caixa_4_of_6.pdf	A7403E4E11CFCB0348C4A5E248246A9DC0BCB87466201A2C4DC8EBBDC6335F360E9849235295B6C977A8E636FDE5D13F1E9D18924F010975EB5A01D1FE6CB78B
La_Caixa_5_of_6.pdf	B70D3D3DA9361727698707DD052C2F4379DD4A752D79B0B06737CDC44052618EAB10253E4B9D3D2B03D10ACC61665E930613D1F7A867D924DDE413B1B339A008

MASTERCARD_6_of_10.pdf	FDA16A567C7AD537B8F913F79E9F710BD2FA86F0F28DC3CE5A21546F31B02D24D8A9FD529A74E71006F1346F7726E9BF657A6445606D9BFE87E9A3FAF807DBCC
MASTERCARD_7_of_10.pdf	69B212D15BAC37F3163786A6F720DD1686351F62076E47FA201CD90F441173DBBFDE18B7B5765AD9D3325CCCFBEFD3754A830FFF06CE34C488BE5AB5A9DB0628
MASTERCARD_8_of_10.pdf	F7228FEFE4EB74FA3DB9A137027494961B592F3860A0682849CA771838EDDD45A034B8C008C571D26F5E5DAB54B9A2E93358BC639D9B05F955A5CB28A87BB5EB
MASTERCARD_9_of_10.pdf	C065FE1371A60E2A6C7407E5D8BB6D0394195A54796C70D1FF25CB3CCC99D8BC6B31EABDC6E1B17FCB01FFC11CE432A6BADEBDD85D5CE286C3915394FFCEB0BB
MASTERCARD_10_of_10.pdf	86C8EBC3B75FDCC84C2FE3E2AB2ABEC0DAA1CBF8391C0574D363AFDE5F889CF4149609E0BEE685EA21FC1B965C72417AE78A282C998D6A27C150DC8C267D190B
MASTERCARD_1_of_10.pdf	7AE810B5E952B26E945BED3DFF552935360682F39E99CA6989D99CC20921CB9ABD2D3DC2D9FB80450034F260D9E8E6C1B899847612B9FE06143BA36ACB225013
MASTERCARD_2_of_10.pdf	0E8A605D28CBE07995AE1652D69FCE321DEB5C1307576C42735560DFDF0ED540FCE9B8F637C963C95E9D9782D623A29033DE9FD7C2A9B0BFA6F34FCCEEBC6B69
MASTERCARD_3_of_10.pdf	F5B7FD326B1E4A5C7725ADC75EC7D614C0388311A63F82349A0AB673B98B08AF2C7984649EB4F722A12AC6A611E52615BAF9F34D7A7A8B5604494E4E4E5621B1
MASTERCARD_4_of_10.pdf	24406E095B1C7D490FFE0CB8C1258C03E8752468EDDC38680815988BC9CDCF625828C5E5E6F9AB5846122D9AF6FB82AE3345A24F41EEBF5F336D9EDA1A84950D
MASTERCARD_5_of_10.pdf	4CA7B532789C799CA62C239737A7586FFD2A4DD8AD9999DD8910E659D80CB5E30F37A6C504C810A34E222C893C160913C5713FC996A06605B6FE18816B7EEE94

Nexus.pdf	CD282E7EB93402841F3598C1ABF9323875831FC28BC5C38869538B099FF1ADF3251DCBC6944C57CC9DC480032807212CA8A8F1B1A79CA3D20F46D69235B1E282
Professional_Services.pdf	8CF1A963590524130C097DB5B2B4B5890D7A04FC91400CF1D026B4B94C3129C7EE6DFAFA8172F846E40B276760D3EBB7F766E6DD68CF1B40D89908314E08E74F
RAPHAEL.pdf	233867F75F5A66CC2E307DDB2F9454BDDA5CF6276DC1038A2D4CD3750E2CF0E5F746B7801AC979F5D9FAD49C0CE2C638CA5A6D915D2DE75ADA795F4ADC025BA6
SADEWO.pdf	81450CBFEE8BC606808F7CCF9CF2E91DCAC75A91F44CE662E2DFFF88FD5EA7CE429CD3225C048A8A6BBD1689CC3DF3B8AEB788B54F41424C03A4FFA67B926D9A
Tech_Notes_Desk.pdf	6983DE0BBC7E54384E3180638091F493CCB954E76A4CB98A20F4F4D2EF379CCCAB748D6FE86BDBEB4E83A50C2110265A2F6D6BF55F0EE95D3B278A2C479F6266
TechCrunch.pdf	6F15C32BC38897983129699DDBA3B8F066B911CF4174D4FCB6DF3D7687D639EDAA4F0AFFA409AFF581AB1ACDAEB42BD27209ABA831831B36FBAB9A54C9EB1473
Townsend_Security.pdf	0FFA78E14FD633D718F240117AD1CDD22780404495877A3F83841834AA4A81C3238E580C9267DF46433445C610657AE1127DAFD4CDDA10B5C46FF1829E99A62C
WOO.pdf	5515199EAF19479E8EB34185F3050DE852A2DABE1D7515C140AD39FA93034B77A9EA3A23A8D1D2B7FD4528CBE2F52CD0F82D8A02ADA1516A5B7CF209B6BF6B50
McDonald.pdf	FF3C99784A6AC857ACEE5F64B2ACB7940FCF7DA7F752A38CFC60EB7773FEFEEC63F34106FC94BF8B5830919C173C73A95A7F2487B673065028807C05C07C09CC
Mobile_Commerce.pdf	0C444481F5FAF77E1A024752C687615FEF5B3540D496D12BBE8F7D9738C6E541B472EC16FC621FF600423C138BA7E5AEBE59185E6BCB6C5891C0D475FDE5809B

Mobile_Contactless.pdf	449F08C62980BE2BE60DA53B29F7A0C80EFC4C85C63A4C595A12836E103D1329E8F0C7B5BEC56DC54634861E264463B535EF6A08A939E4789D74679F9F40DB78
Mobile_Payment_Bringing.pdf	848523007D735C5E54C5F4B4DB6664458D511C4F7F5F803DB695C7B27BD373C155FA94D594FE6B9698B6F40F254D6D3453DB4C64BA64B88A1F91C7D9BBC76A8C
MOLEN.pdf	2DC48712A930C9EEED6A6AE3DF301005B13B3F9A539FFC0B681DFC9D4D613B745FC0FC1D07CA00BCA7CCCC1C731568892D309F5D3154206D8D93CEFB4CB8775E
nelenkov.pdf	F808120F02058F894E7E039FA3136A5EFD52AD3AB88AEA3DD05314D11F36FB64AD149608CB9C76129FE688CF82606CD781000AD235E837E49656926D7A5F43A

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 filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

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

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

New International Application Filed with the USPTO as a Receiving Office

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

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

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. 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	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

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	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	1	Susan Pandy, "Securing Payments: Payments Tokenization in Primetime," Federal Reserve Bank of Boston Payments Symposium, January 20, 2016, pp. 1-20.	
	2	"SUMMARY OF ANS X9.119-Part 2 USE OF TOKENS TO PROTECT SENSITIVE CARD DATA," September 2017, pp.1-2.	
	3	Marianne Crowe et al., "Is Payment Tokenization Ready for Primetime?," June 11, 2015, pp. 1-51.	
	4	Terence Spies et al., "ANSI X9.119 Part 2: Using Tokenization Methods," 2013, pp. 1-20.	
	5	ASSORA et al., "A web transaction security scheme based on disposable credit card numbers," Int. J. Electronic Security and Digital Forensics, 2007, Vol. 1, No. 2, Inderscience Enterprises Ltd., pp. 146-155.	
	6	BOYD, "A pragmatic approach to temporary payment cards numbers," Int. J. Electronic Security and Digital Forensics, 2009, Vol. 2, No. 3, pp. 253-268.	
	7	BUCCAFURRI et al., "Implementing disposable credit card numbers by mobile phones," Electronic Commerce Research, Feb. 23, 2011, Vol. 11, Springer Publishing, pp. 271-296.	
	8	JAVANI et al., "A new credit card payment system based on 3D-Secure using one-time-use transaction numbers," Information Assurance and Security Letters, 2010, Vol. 1, Dynamic Publishers, Inc., USA, pp. 060-065.	
	9	KILLORAN et al., "A New Secure Wireless Financial Transaction Architecture," EUROCON 2005, November 22-24, 2005, IEEE, pp. 1060-1063.	
	10	LI et al., "A security-enhanced one-time payment scheme for credit card," Mar. 28-29, 2004, IEEE, pp. 1-11.	
	11	MJØLSNES et al., "On-Line E-Wallet System with Decentralized Credential Keepers," Mobile Networks and Applications, 2003, Vol. 8, Kluwer Academic Publishers, The Netherlands, pp. 87–99.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	12	NARAYANASWAMI et al., "What Would You Do with a Hundred MIPS on Your Wrist?," RC 22057 (98634) January 22, 2001, IBM Research, pp. 1-10.	
	13	QASIM et al., "Interactive Shopping with Mobile Wallet," World Congress on Sustainable Technologies, 2012, IEEE, pp. 32-36.	
	14	HONIG, "A Week with Google Wallet," Endgadget, September 19, 2011, pp. 1-49.	
	15	KADAMBI et al.,"Near-Field Communication-Based Secure Mobile Payment Service," ICEC'09, August 12–15, 2009, pp. 1-11.	
	16	"A closer look at Google Pay and tokenization," Rambus Press, February 23, 2016, pp. 1-2.	
	17	GHAG et al., "A Comprehensive Study of Google Wallet as an NFC Application," International Journal of Computer Applications, November 2012, Vol. 58, No.16, pp. 37-42.	
	18	"Add any credit or debit card," Google Wallet Help (archive.org), 2012, page 1.	
	19	"Add any credit or signature debit card," Wallet Help, Google Wallet, September 20, 2012, page 1.	
	20	"Allynis Mobile NFC," Gemalto, September 2007, pp. 1-4.	
	21	"Allynis TSM for Transport," Gemalto, October 2009, pp. 1-2.	
	22	ADAMS, "Amex Plays a Major Role in Revamped Isis Mobile Wallet," Payments Source, November 15, 2013, Vol. 1, No. 1, SourceMedia LLC d/b/a Arizent, pp. 1-2.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	23	PEREZ, "Android Pay, Google's Apple Pay Rival, Arrives Today," DigitalOcean, September 10, 2015, pp. 1-8.	
	24	HEISLER, "Apple Pay: An in-depth look at what's behind the secure payment system," Engadget, October 2, 2014, pp. 1-7.	
	25	FEHR, "Apple Pay: How different is it from other Pay solutions, what role does tokenisation play, and to what degree can Card not Present payment benefit from Apple Pay in future," Technical Report RHUL–ISG–2018–3, April 3, 2018, Egham, Surrey, UK, pp. 1-79.	
	26	'ATMIA publishes contactless ATM best practices," ATM Marketplace, September 27, 2012, pp. 1-2.	
	27	POPPER, "Banks Did It Apple's Way in Payments by Mobile," New York Times, September 11, 2014, pp. 1-2.	
	28	'Bell ID Simplifies EMV Smart Card and NFC Application Management with Versatile New Platform," eBanking & Payment News, May 5, 2011, page 1.	
	29	'BofA pursuing contactless ATM patent," Mobilepaymentstoday.com News, September 20, 2012, Newstex LLC, pp. 1-2.	
	30	'Chip Advisory #20, Visa Recommended Practices for EMV Chip Implementation in the U.S," July 11, 2012, pp. 1-10.	
	31	'Commbank, Mastercard and Samsung collaborate to launch NFC payment service," MarketLine NewsWire (Formerly Datamonitor), December 13, 2013, pp. 1-2.	
	32	'Contactless Payment: Secure Enough?," Card Technology, September 1, 2005, SourceMedia, Inc., Section: SPECIAL ISSUE: CONTACTLESS TECHNOLOGY, Vol. 10, No. 8, page 36.	
	33	'Eligible Devices," Google Wallet Help (archive.org), November 18, 2012, page 1.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	34	MOTT, "EMV and Mobile Payments, Questions abound, answers divide," Payments Summit Workshop, February 4, 2013, pp. 1-22.
	35	"EMV Integrated Circuit Card Specifications for Payment Systems Book 2 Security and Key Management Version 4.1," May 2004, pp. 1-187.
	36	"EMV Integrated Circuit Card Specifications for Payment Systems. Book 2, Security and Key Management, Version 4.3," November 2011, pp. 1-174.
	37	"EMV Integrated Circuit Card Specifications for Payment Systems, Book 3, Application Specification, Version 4.3," November 2011, pp. 1-230.

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	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

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	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

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.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/528,073	**01/12/2023 01:27:56 AM ET**	**WYAT-0002.USD1C1C1C1C1C**

Title of Invention

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4809	FILED BY	Jose Garcia
PATENT CENTER #	61424604	FILING DATE	11/16/2021
CUSTOMER #	136197	FIRST NAMED INVENTOR	David WYATT
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 51

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
WYAT-0002-13C12US_IDS_transmittal_form_1.pdf	7	Information Disclosure Statement (IDS) Form (SB08)	1236 KB
BOYD.pdf	16	Non Patent Literature	1484 KB
BUCCAFURRI.pdf	26	Non Patent Literature	18760 KB
Card_Technology.pdf	2	Non Patent Literature	1400 KB
Chip_Advisory.pdf	10	Non Patent Literature	4354 KB
Commbank.pdf	2	Non Patent Literature	915 KB

ADAMS.pdf	2	Non Patent Literature	1268 KB
Allynis.pdf	4	Non Patent Literature	2218 KB
Allynis_TSM.pdf	2	Non Patent Literature	1429 KB
ASSORA.pdf	10	Non Patent Literature	525 KB
ATMIA.pdf	2	Non Patent Literature	829 KB
Bell.pdf	1	Non Patent Literature	50 KB
BofA.pdf	2	Non Patent Literature	972 KB
EMV_Version4_1_5_of_5.pdf	35	Non Patent Literature	21890 KB
EMV_Version4_3_1_of_6.pdf	44	Non Patent Literature	18367 KB
EMV_Version4_3_2_of_6.pdf	22	Non Patent Literature	10609 KB
Eligible_Devices.pdf	1	Non Patent Literature	359 KB
EMV_Version4_1_1_of_5.pdf	38	Non Patent Literature	16276 KB
EMV_Version4_1_2_of_5.pdf	38	Non Patent Literature	20147 KB
EMV_Version4_1_3_of_5.pdf	38	Non Patent Literature	20660 KB
EMV_Version4_1_4_of_5.pdf	38	Non Patent Literature	21751 KB
EMV_Version4_3_Book_3_2_of_4.pdf	58	Non Patent Literature	17652 KB
EMV_Version4_3_Book_3_3_of_4.pdf	58	Non Patent Literature	19875 KB
EMV_Version4_3_Book_3_4_of_4.pdf	56	Non Patent Literature	17117 KB

EMV_Version4_3_3_of_6.pdf	22	Non Patent Literature	14463 KB
EMV_Version4_3_4_of_6.pdf	22	Non Patent Literature	12252 KB
EMV_Version4_3_5_of_6.pdf	22	Non Patent Literature	12697 KB
EMV_Version4_3_6_of_6.pdf	42	Non Patent Literature	22311 KB
EMV_Version4_3_Book_3_1_of_4.pdf	58	Non Patent Literature	14723 KB
MJØLSNES.pdf	13	Non Patent Literature	1222 KB
MOTT.pdf	22	Non Patent Literature	12395 KB
NARAYANASWAMI.pdf	10	Non Patent Literature	2820 KB
PEREZ.pdf	8	Non Patent Literature	3975 KB
FEHR_1_of_2.pdf	40	Non Patent Literature	16209 KB
FEHR_2_of_2.pdf	39	Non Patent Literature	12433 KB
GHAG.pdf	6	Non Patent Literature	1711 KB
Google_Wallet.pdf	1	Non Patent Literature	595 KB
HEISLER.pdf	7	Non Patent Literature	4135 KB
HONIG.pdf	49	Non Patent Literature	6061 KB
JAVANI.pdf	6	Non Patent Literature	4074 KB
KADAMBI.pdf	11	Non Patent Literature	6408 KB
KILLORAN.pdf	4	Non Patent Literature	3277 KB
LI.pdf	11	Non Patent Literature	2268 KB

Summary_of_X9_119_Part2.pdf	2	Non Patent Literature	79 KB
tokenization_prime_time.pdf	51	Non Patent Literature	930 KB
Wallet_Help.pdf	1	Non Patent Literature	588 KB
X9_Tokenization_Webinar.pdf	20	Non Patent Literature	572 KB
POPPER.pdf	2	Non Patent Literature	992 KB
QASIM.pdf	5	Non Patent Literature	2677 KB
Rambus_Press.pdf	2	Non Patent Literature	994 KB
Securing_Payments_Payments_Tokenization_in_Primetime_Susan_Pandy.pdf	20	Non Patent Literature	1814 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
WYAT-0002-13C12US_IDS_transmittal_form_1.pdf	4F0C61245B9B943C8CDD1980604C62915688BD2FB91ED153113BB7F505135EE0E56F14A31D9412F4C8E6A7FB5F0611AEB88CB24D3652D38E0338895D9253C4F4
BOYD.pdf	D39B5EA68D301627A34756AD9BD1B06CA843EED22AB642B4A876FB74C8AB1DEC0F5AE064DE5007D5DAEC8E15F8B120FA8419966594726C29DD2741D4A08B84A7
BUCCAFURRI.pdf	0A03D387FF0B573B3D44288C20DA995EA07BBB7131D4966B500AE4E9936C64E407DCE7B3D23A7179B9206733F06FF9524E9712AD50CE3D1B91F1AC9870CE2AA4
Card_Technology.pdf	0809D4A22C921A988D89D6F68E953187CCF21D33A66525F04C26A70249ECA367A7C5931BDD42838D1F6D842A4033F05BFD

	BC3F5A0250F2E0D99E4CCAEB277E50
Chip_Advisory.pdf	3BF42C638C86E4CCE628BAE2FEB50602C48DDB1A618BDE703DC8AA70C22FF8656616532811 60FC4A31EA6F335BF789B897473CD2017CF095ED8FDB11117499BF
Commbank.pdf	3F783425E0CD95911F262080166 4B942C6052C062D6BBB0A7D166DD2BEA9B0909ACADA35C1E4F6427EEBA1B11C1A987D3C06E5407AC2339F5656D210AA8DE8A5
ADAMS.pdf	5538A8606D81EDB46E767776C89CBC10DBE56E87CE7D75DBCA999C1E6B0C145FBF2497EC3CF335E8B558F3BD00F9A9B004038120791D8D10F3C6EED942CED267
Allynis.pdf	AE1ED03818B28EFA0A821437DFB702B2F12B64199C77B38993CFCC0E24812B6D8D73D57D72085004133C2D27B4B303F09097F666A043E93743532AF53FFB8589
Allynis_TSM.pdf	B59AE47468827AF15EA3731015D7531260D0614D26D57E5E2FD965DCAD55541EE8B1126BF5D50BD6467B5EF8D79A9D7A937121155068BB19D0CC665034BE897D
ASSORA.pdf	72152DD9C6DA5F3F4B76822DC8EAA9E9EEAF01D772804D70796B7A58EA7619D48E9103E844F97839729D3B2785B3E61E0106CAA97D4E32AEA14639AEF5780D8C
ATMIA.pdf	0211530F0CB6627EE4E37AE62337AC066512E89EF5B4ECE51627B15ADCA344A6B92C2D1578095A5CBA79B3986E3DDCD49FC7955A75437465B8DE32517DC6FDCF
Bell.pdf	8064F8F28BF156C8D715B4E3DD393729D85784F6826A8EC6A93BEF703B8275D6F92F259B048FB26BC2A4FC46ED9F3D52C32BCB6068ADB5F7315F5A08BA610ED2
BofA.pdf	B9C51D87CBD3E127E48A4FC323A5C9A4F879C8829F33908A47F584F3F722F35C4C5BC77994C3838382FC2F59C938CD35579B740E8E5986CBC26A31C13EA68335
EMV_Version4_1_5_of_5.pdf	09E8648272DD8B8A94C796DB06AB8A089115D2C23723F66468923A63872D3BF86953A6BEB638D487AC9D6295D2513B469C7

	D845452DDD783BB4DDC0A7ED73B7A
EMV_Version4_3_1_of_6.pdf	6A683BE6E45691E5B837EEC4F7390552050760 6ACA25EE9871EA1BB6A7F3A3E38CCA80B795821BD1106D35C761259B02099F3AFEF6D15211F86EFEF896CDEFE5
EMV_Version4_3_2_of_6.pdf	6AFB6443D402596DB9B44C3420A4E016E52B510D9B4447859712CF58A231D11AE27A0432B0A8118E2C163C55DBC4C3D97FB6615542E972A3F532FE37BF0D3C3A
Eligible_Devices.pdf	E7485117B1C2B03C3E57978C24C80F344996A0BF6557E4F3E90F451A3C500BFC4BFE9CA24FA7752FF1B0E9F0250E9C30564140A1AF528334590AB968FED09A03
EMV_Version4_1_1_of_5.pdf	C881DF5451E974C752DA52A2E2A562AB265F57EBAE2774E9E53E331226548481C121353F6139084E7919DDCF580273AC0187351A32511E68D9A1EBD240BFDB87
EMV_Version4_1_2_of_5.pdf	8DBABA99D5CD6B530FDFDCF28D2317C470922190A30F560E03FB89A8342B16D587AB65D0FD63354872D176E5095531EFE144E00779A6FE26B62C19EFB699C731
EMV_Version4_1_3_of_5.pdf	91E406A620A19206E31ACAC834F41A166493704F2D57E20CC50D535C8C4C40EBEBB3D94097A92C35CF6EA82A099FAFC491D329C676BC6F77E0ECF8A32434E936
EMV_Version4_1_4_of_5.pdf	95675B681FDF86E36D4A8B0344D06DAF1E0F2C5D3937C02520F842A987462F85EE8C5B31F299EFDF5DD7431C745535605633C3E8C756EA1FB14A8DA22175A2F8
EMV_Version4_3_Book_3_2_of_4.pdf	BB2AD512AEDF46C95CFA42BE7C6277998D6184EF60B52539CD4E5EDE27E506D90FC11BB3A2CE12291E04E208B3DEF94B078F3A357A3C5DD7ED96AB765576D512
EMV_Version4_3_Book_3_3_of_4.pdf	BAEA77F15EB89EF675EBF883C1F5F32AF04A38EE434A47301928684B540883BFEB6240205DD7B31DCC25D35B4AC6448D479A32D69D120026DC4364E11E90734F
EMV_Version4_3_Book_3_4_of_4.pdf	877FF29B90A238E12574539C7D37CDFE609378ADEEA723394B7DEB6010C5101B7484D0BFD2AA59F29C88753D20E91BB4BF

	DEF8EE81F26673F046C013CFCE1DA9
EMV_Version4_3_3_of_6.pdf	DD5243F6F4744D9BF7E4150AF33414BC0A1F63296836B91141 7F792DB28AC797ED52EEA5258B861462FCB1B63E1DC193E8F 7EB9328B91A4D79773FAF762FB7B5
EMV_Version4_3_4_of_6.pdf	A0CBF5DE048BB65A28342200AA90D2DB67518FB008402A154 9FE93C35D25646C3EA8893A36EBA38637123047B15F01ADE0 F40C9F6CACEC52F6D8365B96E1AF5A
EMV_Version4_3_5_of_6.pdf	EFDDAF48C250F6B032202793A25FDCCA391B321E4DAFF8D0 C4996D16C4224F3C80C3F5B7D6E06DE65F26040D8D0F9DC97 A21180AFA4F3F7A3806E1F8EA2C25D0
EMV_Version4_3_6_of_6.pdf	CCB68CAA90AB233F7A81EB8F0FADE2E709869436A22CEB6A 193D5EF1B88FB0BA25925173DF9C63741D99525CB8C895E50 1944A012E4A57891934C4ED15938229
EMV_Version4_3_Book_3_1_of _4.pdf	6930BDEDACE65535E0B1CE174B42C865A1A3C89352C0C9AB 7F76AFBC4E156DFFBDBFE45F4012A00BF2CB17EC782ECB8A 0FF9EC4169CB4432769374BF89F91488
MJØLSNES.pdf	09D5809D62DD012C6ADEE666A17D3182F18B22AF9B8DDFB7 F7398D10FB60242B48F30404B8F6B0DE4D3390511D03F310C 0547287EC3FCE7A7EFCE19769D5AE0
MOTT.pdf	F5787F4B247AE378139D1974886D273B671EFCA194DC5FF1E D6B1042123433DA4645B7FEC6D27414D143831D29ABCC930F 9006D5FE9C30577465965562E9D566
NARAYANASWAMI.pdf	1F01E07A4118809664E0D9CC83FC20A6B960A9AFF640C1752F 7F5CD80BF49CF293A8B00AC0140898CE6CAAB2FF8CA551AF 0DADA899EFB9B74F6368245E993795
PEREZ.pdf	338F26C8F06091EA9D3BBC34096CF77DF4E11F23D432D66CB 5775D98DE781A68804BA5E436D31C561B8B643B1171C22B4D 0C93FC5F1E5B3DA12DA5B535C922FC
FEHR_1_of_2.pdf	85FFB2B011773749EDC984747130C968BDA51C0260966D1FE0 44F389270F548C01A44ECCC5BAFC2FEE2DE83A022EFBF057

	B7F2EDA4D651C8DAB11F066B049B5A
FEHR_2_of_2.pdf	7900EC82C6BE4655B37103766DE66F86E5F6E5C12D3BFD8C05BE0547E53E684DE6D10C38D4362E0C399194C2BE5CD3CB148F05ABE3653DA24D73E5014BEC0DBB
GHAG.pdf	954672BA13D15FA8ABC894A85FA1FDAA59C8D856E871460C1C5B95DB127B63B415127F3F04315362904D3C35C02CCF82696EC8A7C706337175A277A404356253
Google_Wallet.pdf	8DE6568D7B8A287E65F9A5F38DAFE05157D68838BECF7D5C9A39077B87AA9C2603AFFBB7D5D8089105BE7C8E50A44CB11ABF434A46703A917F25857DB21F9336
HEISLER.pdf	0E16D814795430518BA5A076A2E7E9B9BD3FE9634A06F6244938DE72238F52193449D709F2AB1038F861D111C47136E1EB04707564ED39AF1BA37EB4A8E34E7C
HONIG.pdf	A2884CD2EC73B871CA75F215B7BCBAA9499D4BC858336EAE80AD7D60DB03890910554D16C790E802FEBF3B7CFD4329056557D99134401E90100FBF42214068E8
JAVANI.pdf	C1C1C6016E392BE5703EE23C81F44301C270112C39F70E46BF154EC418C795EB1D58752408E78114556D07AB4F625631BB93AD0989701617823O2BE80FF9E7FC
KADAMBI.pdf	55DDD4E83880ADE76EAC158D99CFF5CBA4F5F19788B43599DD9F25CCCAEFB4A47D3EE87763CF0DE37BBE0D29A60E14AF6EE32AB836EB0793194BC576334A21E9
KILLORAN.pdf	31D22C0393C99C2464F7E79D35CD518E2D8BE96574C00C6E052BAA2FE4658D25DE3E026CF660C67217EDAA58C43431136600996FAA4D959D210B95488FEBA2B3
LI.pdf	A5D9430B1149889FAE605EE6A9BCF8F3ACA84E058B1ECE680EF9F5BB967BB48862D1C09ADC185AFCA1442C77FA356C82B37FC19D6ECAB8027A5ECC285E0646C8
Summary_of_X9_119_Part2.pdf	869F6F2AFA594E838EF6B0589B11819DE452077F807B36F28C5C961E0CD26E9ACD6B6603C18F908D5194429A78A419349889

	ED7018FD23D8B59D629A223C34BA
tokenization_prime_time.pdf	B8AE3162E55ED2C8A346653417 4D192DF3C5CD0D92CA3C6A FE7D55A6214EA2C66EC8137D326C3AB62BD50B10D0B918EE B2423781024213532A1BB6C33B8FACCC
Wallet_Help.pdf	093CF9F287C812670504368F67CCAEE14CCA99405365B2812 6FD67E0852A79FC2B32E4C24D202DEA6E271A07A5ED194BD 7ABE31317FC62F107F13373A0E60BA
X9_Tokenization_Webinar.pdf	0AF132928B9667E9A7A146D1990C6E6C3A1A7D667A170C3D6 036A151B1244C339D26937084A01AAA44A1876E5A08DB9BAF4 6B6FF1F70CD8883DAD2DEE005B8B3
POPPER.pdf	14723D8F1788F840B6227D379A0D6D637AF2BEFC5B0456B12 D6215F3753F9226E3C13654E415148049527205B68F19D410E7 566A8542FEC22F09FFB4B0E6C7BE
QASIM.pdf	412CA0030F07729AE1E0C74E6A24C962E33CF30397E768FF63 D3ADEE0EA94F20BCC39E2051F29F663F877639D52BF20A4A3 1376E0B78EC5DD4495927C1382178
Rambus_Press.pdf	333A954C9E71DC993BCDD386494DAB6D5F1C92FD923D4E38 06843911D2A9F98CD7CAD0CA34DB71FE25444833F221BE3F1 325D49EF2A1F72F8C64A42A061D6B67
Securing_Payments_Payments _Tokenization_in_Primetime_S usan_Pandy.pdf	875973E804A5800330E6FFCB7D5FC3E9BB11D2BC66F10838C 7342F8E4E48BA0FC2762F20E1408C6DC2931DFBD824D1A11C 6799593DAECD4DCB09435D707AA4A5

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 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 (01-22)
Approved for use through 05/31/2024. 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	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

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	9600808		2017-03-21	Gomez, Sr.; William et al.	
	2	9098846		2015-08-04	Gill; Sara et al.	
	3	7690580		2010-04-06	Shoemaker; Austin William	
	4	8499334		2013-07-30	Doughty; Ralph O. et al.	
	5	11100431		2021-08-24	Mullen; Jeffrey D. et al.	
	6	8255323		2012-08-28	Casey; Brandon J et al.	
	7	8423462		2013-04-16	Amacker; Matthew W. et al.	
	8	10460314		2019-10-29	Hird; Geoffrey R. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	9	9846866		2017-12-19	Royyuru; Vijay	
	10	6736322		2004-05-18	Gobburu; Venkata T. et al.	
	11	7967211		2011-06-28	Challa; Nagesh et al.	
	12	8628012		2014-01-14	Wallner; George	
	13	8690059		2014-04-08	Wallner; George	
	14	8814046		2014-08-26	Wallner; George	
	15	9361613		2016-06-07	Wallner; George	
	16	9454679		2016-09-27	Wallner; George	
	17	9652642		2017-05-16	Wallner; George	
	18	9864994		2018-01-09	Huang; Enyang et al.	
	19	10044510		2018-08-07	Kwon; Eun Young et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	20	10269005		2019-04-23	Lee; Woo-Sup et al.	
	21	10275761		2019-04-30	Lee; Woo-Sup et al.	
	22	10402811		2019-09-03	Park; Yong Man et al.	
	23	10423942		2019-09-24	Lee; Woosup et al.	
	24	10454728		2019-10-22	Huang; Enyang	
	25	10505277		2019-12-10	Lee; Woosup et al.	
	26	10516208		2019-12-24	Lee; Woo-Sup et al.	
	27	10540647		2020-01-21	Park; Yong Man et al.	
	28	10546291		2020-01-28	Kim; Eun Jik et al.	
	29	10592893		2020-03-17	Lee; Hee-Dong et al.	
	30	10680322		2020-06-09	Lee; Woosup et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	31	10699266		2020-06-30	Lee; Hee-Dong et al.	
	32	10713646		2020-07-14	Lee; Hee-Dong et al.	
	33	10796299		2020-10-06	Lee; Woo-Sup et al.	
	34	10803452		2020-10-13	Kim; Eun Jik et al.	
	35	10862718		2020-12-08	Huang; Enyang	
	36	10902390		2021-01-26	Lee; Woosup et al.	
	37	10929851		2021-02-23	Kang; Minkoo et al.	
	38	10990954		2021-04-27	Park; Yong Man et al.	
	39	10990959		2021-04-27	Lee; Woo-Sup et al.	
	40	10998620		2021-05-04	Lee; Woosup et al.	
	41	11004075		2021-05-11	Lee; Je Min et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	42	11017399		2021-05-25	Park; Yong Seok et al.	
	43	11042855		2021-06-22	Kim; Yu Hwan et al.	
	44	11061698		2021-07-13	Rhee; Injong et al.	
	45	11074581		2021-07-27	Kim; In Ho et al.	
	46	11107047		2021-08-31	Kim; Kibong et al.	
	47	11127010		2021-09-21	Cho; Boo Hyun et al.	
	48	11129018		2021-09-21	Kim; Ki Bong et al.	
	49	11227278		2022-01-18	Choi; Hoon et al.	
	50	11232339		2022-01-25	Lee; Woosup et al.	
	51	11321701		2022-05-03	Lee; Hee-Dong et al.	

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

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	20130124410		2013-05-16	KAY; Christopher Erin et al.	
	2	20080319905		2008-12-25	CARLSON; Mark	
	3	20100185545		2010-07-22	Royyuru; Vijay K. et al.	
	4	20130262305		2013-10-03	Jones; Andrew R. et al.	
	5	20060089171		2006-04-27	Yoo; Kyung-Min et al.	
	6	20090048971		2009-02-19	Hathaway; Matthew et al.	
	7	20130232083		2013-09-05	SMITH; Theresa L. et al.	
	8	20080126260		2008-05-29	Cox; Mark A. et al.	
	9	20080222047		2008-09-11	Boalt; Adam	
	10	20080172317		2008-07-17	Deibert; Doug et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	11	20090159701		2009-06-25	Mullen; Jeffrey D. et al.	
	12	20120317035		2012-12-13	Royyuru; Vijay K. et al.	
	13	20130166441		2013-06-27	Kobylkin; Egor et al.	
	14	20120310760		2012-12-06	Phillips; Simon et al.	
	15	20080302876		2008-12-11	Mullen; Jeffrey D.	
	16	20110186626		2011-08-04	Manessis; Thomas et al.	
	17	20150147065		2015-05-28	Civelli; Jay Pierre et al.	
	18	20140143785		2014-05-22	Mistry; Pranav et al.	
	19	20050043997		2005-02-24	Sahota, Jagdeep Singh et al.	
	20	20150178724		2015-06-25	Ngo; Hao et al.	
	21	20160132881		2016-05-12	LEE; Yang-Soo et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	22	20160253652		2016-09-01	JE; Seong-Min et al.	
	23	20160253657		2016-09-01	SOHN; Se Chang et al.	
	24	20190026725		2019-01-24	PARK; Yong Seok et al.	
	25	20190172051		2019-06-06	LEE; Hui Jae et al.	
	26	20190173290		2019-06-06	HA; Min Cheol et al.	
	27	20210311752		2021-10-07	Rhee; Injong et al.	
	28	20220005046		2022-01-06	KIM; Inho 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	2478712	GB		2011-09-21	JACKSON, DAVID		
	2	2485442	GB		2012-05-16	CUBIC CORP		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	3	00/62214	WO		2000-10-19	CLEARTOGO.COM et al.		
	4	01/57620	WO		2001-08-09	COMSENSE TECHNOLOGIES LTD et al.		
	5	2007145687	WO		2007-12-21	WEISS, KENNETH P.		
	6	2010043974	WO		2010-04-22	RICHARD, CHRISTIAN		
	7	2012154915	WO		2012-11-15	DYNAMICS INC et al.		
	8	2005119607	WO		2005-12-15	TYFONE INC 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.	T5
	1		

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

[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	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

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	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

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.

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
9 August 2001 (09.08.2001)

PCT

(10) International Publication Number
WO 01/57620 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number: PCT/US01/03882

(22) International Filing Date: 6 February 2001 (06.02.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/180,530	7 February 2000 (07.02.2000)	US
09/570,399	12 May 2000 (12.05.2000)	US

(71) Applicant *(for all designated States except US)*: **COMSENSE TECHNOLOGIES, LTD.** [IL/IL]; 3 Azrieli Center, 67023 Tel-Aviv (IL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **ATSMON, Alon** [IL/IL]; 131/2 Ben Guryon Street, Yahud (IL). **ANTEBI, Amit** [IL/IL]; 64 Marganit Street, Ramat-Gan (IL). **LEV, Tsvi** [—/IL]; Lisin Street 11, 62997 Tel-Aviv (IL). **COHEN, Moshe** [IL/IL]; Chovevey 47, Tsivon, Tel-Aviv (IL). **SPEYER, Gavriel** [US/US]; 11358 Chalon Road, Los Angeles, CA 90049 (US). **SEGE, Alan** [US/US]; Apartment #5, 1518 Euclid Street, Santa Monica, CA 90404 (US). **ALTIMAN, Nathan** [IL/IL]; Hachashmonaym Street 39, Tel Aviv (IL). **ANATI, Rami** [IL/IL]; Haetrog Street 16, 38244 Kfar Brandes Haders (IL).

(74) Agents: **CHOU, Chien-Wei, (Chris)** et al.; Oppenheimer Wolff & Donnelly LLP, 1400 Page Mill Road, Palo Alto, CA 94304 (US).

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

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

Published:

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

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

WO 01/57620 A2

(54) Title: PHYSICAL PRESENCE DIGITAL AUTHENTICATION SYSTEM (TRANSMISSION AND ROUTINE)

(57) Abstract: The interactive authentication system allows a consumer to interact with a base station, such as broadcast media (e.g., television and radio) or PC, to receive coupons, special sales offers, and other information with an electronic card. The electronic card can also be used to transmit a signal that can be received by the base station to perform a wide variety of tasks. These tasks can include launching an application, authenticating a user at a website, and completing a sales transaction at a website (e.g., by filling out a form automatically). The interaction between the base station and the electronic card is accomplished by using the conventional sound system in the base station so that a special reader hardware need not be installed to interact with the electronic card. The user is equipped with an electronic card that can receive and transmit data via sound waves. In the various embodiments, the sound waves can be audible or ultrasonic (which can be slightly audible to some groups of people).

PHYSICAL PRESENCE DIGITAL AUTHENTICATION SYSTEM
(TRANSMISSION AND ROUTINE)

BACKGROUND OF THE INVENTION

RELATED APPLICATIONS

This application is a continuation-in-part of PCT application PCT/IL99/00525 titled "Card for Interaction with a Computer," filed October 4, 1999, which is a 35 USC 119(e) application based on U.S. provisional applications 60/115,231 filed January 8, 1999, 60/122,687 filed March 3, 1999, 60/143,220 filed July 9, 1999, 60/145,342 filed July 23, 1999, and 60/153,858 filed September 14, 1999. This application is also a continuation-in-part of U.S. provisional application 60/180,530 filed February 7, 2000. This application is also a continuation-in-part of PCT applications PCT/IL98/00450 filed September 16, 1998, PCT/IL99/00470 filed August 27, 1999, PCT/IL99/00506 filed September 16, 1999, and PCT/IL99/00521 filed October 1, 1999, all filed in the Israel receiving office by applicant ComSense Technologies Ltd. and designating the United States, and PCT/IB99/02110 filed November 16, 1999 with the International Bureau. All of these applications benefit from a priority date of July 6, 1998. Reference is further made to and priority claimed from U.S. Patent Application Serial No. 09/570,399, filed May 12, 2000, entitled, "Physical Presence Digital Authentication System." The disclosures of all of these applications are incorporated herein by reference.

FIELD OF THE INVENTION

The present invention relates generally to electronic cards or device for interaction with another electronic card or device such as a computer and, in particular, to electronic cards that use acoustic signals for such communications.

DESCRIPTION OF RELATED ART

The Internet, and the World Wide Web (WWW) in particular, has grown in popularity in recent years. In addition to news and information, merchants and consumers alike have come to view the web as a virtually unlimited source for conducting business, in the form of sales of products, services, and information. Nevertheless, many computer users are still somewhat leery of conducting sales transactions over the web especially because credit cards are involved, along with the associated fear of widespread and unchecked dissemination of the credit card numbers. These same users may also be leery of conducting non-Internet related sales transactions using credit cards. After all, anyone can swipe a credit card number and use it later for unauthorized purchases. Assurances from well-meaning web (and non-web) merchants do not alleviate these concerns because the user would have to carry a credit card in his person, which can be easily stolen or lost (and thus found by an unscrupulous thief). What is needed is a secure purchasing mechanism that provides users with the peace of mind to make a purchase on the web (or any other form of electronic purchase or other secure

information access) without the fear of having his credit card number stolen by an interloper at any point in the transaction.

Typically, systems that provide security to such online users do so to the detriment of user convenience. Because the Internet is a mass-medium, the success of online services depends largely on preserving user convenience. Without such conveniences, users would become decreasingly tolerant resulting in a loss of business and social opportunities for both web merchants and users alike.

Traditional microprocessor credit cards, also known as "smart cards" or "chip cards," provide security. But while smart cards that work in conjunction with dedicated smart card readers have become prevalent (i.e., bank cards in Europe), they are ill-suited for deployment as widespread Internet access control devices. Deploying smart card readers to users in their homes, for example, and educating users on their installation and use, are cumbersome, expensive, and inconvenient.

The prior art smart card systems largely were developed for a disconnected world; that is, maintaining a constant connection between the smart card and some other entity was considered expensive, inconvenient, and largely unnecessary. Indeed, the telephone charge itself was significant enough in cost to warrant minimizing such connection times.

In the prior art smart card, a small computer apparatus was embedded into a credit card plastic. At the very minimum, that apparatus would authenticate a user's secret personal identification number that was manually entered by the user on an in-store keypad every time a card is swiped. This authentication process did not require the intervention of any other authentication network. One aim of the present invention is to provide authentication that is as secure as ordinary bank cards, but in a manner where the functionality associated with the card is accessed via a public network such as the Internet. Ideally, such cards that send a one-way authentication signal can be used anywhere the Internet is available.

Computer network components that communicate using radio frequency (RF), infrared (IR), and wires are well known. In addition, some home appliances are controlled using acoustic remote control. However, these networks and appliances needed dedicated hardware components to realize the communication protocol; that is, specific and specialized hardware whose sole purpose was to effectuate the communication was installed therein. If such communication were not needed, the specific and specialized hardware would not be needed at all. Installing such hardware on an existing computer, TV, or radio may be expensive and/or problematic. Further, some electronic and/or computer embedded devices, for example cellular telephones may be "sealed" products, to which it is impossible to add internal components. What is needed is an electronic device that communicates with existing infrastructure equipment without the need to further equip these infrastructure equipment with any special hardware such as a smart card reader.

PCT publications WO96/10880, WO94/17498, WO93/21720 and WO93/11619, the disclosures of which are incorporated herein by reference describe an electronic device which transmits coded information to a microphone of a telephone using a DTMF-like encoding scheme. A WWW page addressed "http://www.encotone.com/html/tech_def.html", suggests using such a device to transmit audible DTMF-like tones to a personal computer using the computer's sound card.

Two way communications using audible DTMF-like tones, between an electronic card and a telephone communication system is described in US patent 5,583,933, the disclosure of which is incorporated herein by reference. Thus, what is needed is a communication mechanism that allows the electronic card to communicate with a transmitter/receiver without the need for dedicated or special hardware. Use of existing components would facilitate the wide acceptance of this communication mechanism, particularly in the purchasing context.

The present invention provides such a system and method and provides solutions to the problems described above.

SUMMARY OF THE INVENTION

One object of the present invention is to provide an electronic system which allows users to easily interact with a merchant (web-based or otherwise) or some other entity.

Still another object of the present invention is to provide a credit card-sized electronic card that can interact with various electronic devices (e.g., computer) to transmit information as well as receive information.

Another object of the present invention is to provide such an interactive electronic system without the use of dedicated hardware; that is, existing hardware will be utilized resulting in little, if any, changes for the television, radio, and stereo system manufacturers.

A further object of the present invention is to require little or no change to the content (as opposed to the infrastructure equipment itself) generated by the existing infrastructure. Sound is an essential element of human communications. Therefore, the present invention is relatively immune from changing communications standards, and is mass scalable. Strictly speaking, implementing those two-way methods requires little or no infrastructure change or modification of existing sound content. Two-way implementations under the current invention provide widespread utility in situations removed from a network. For example, some embodiments described here enable users to "bookmark" sound content, and later use those sound bookmarks to retrieve desired content from a network or other receiving apparatus.

In accordance with one embodiment of the present invention, the interactive electronic system includes an electronic card. In one embodiment, the electronic card is a one-way card that has a transducer, receiver circuitry and software (i.e., DSP and operating system) to process the incoming data. In another embodiment, the electronic card is a two-way card with both transmission and reception circuitry. In a further embodiment, the electronic card is a one-way transmit-only card. In any of these embodiments, the electronic card also includes a display, such as a liquid crystal display (LCD) panel. Memory (ROM, EEPROM, and RAM), a bus system, and power source are also provided. Electronic card contacts may also be provided to allow the electronic card to interface with standard electronic card readers. One or more physical buttons are also provided on the electronic card itself to perform any of a number of functions: (1) transmit data from the electronic card, (2) transmit data followed by a short period in receive mode, or (3) turn on the power to receive data for a short period.

Generally, the electronic card works with the existing infrastructure; that is, no special dedicated reader is necessary for the electronic card to communicate with existing base stations. For example, one such base

station is a personal computer. The personal computer typically has sound devices installed therein and the electronic card of the present invention can communicate with the computer using this already existing sound system. However, in another embodiment, special readers can be used to provide various functionality – from reading the contents of the card (for those systems without a sound device) to adding bidirectional support for an otherwise one-way card to recharging the battery(ies) in the card. So, if the computer system is not equipped with a sound system, a special reader is provided to allow the electronic card to communicate with the computer system. As another example, the special reader can be an electronic device with a microphone to allow an otherwise transmit-only one-way electronic card to have two-way capability.

Without trading off security, the present invention provides substantially enhanced user convenience. For example, reader-free authentication devices are disclosed that enable "one-button" triggering of complex tasks such as connecting to a network and logging in securely to personalized network services.. The software that enables the reader-free communication can be stored permanently on the base station for enhanced functionality. But for enhanced portability, methods are described for outsourcing that communications software to a remote computer, so that the devices can be used at a broader array of base stations.

The spectrum of applications enabled by the electronic card is broad. For the various embodiments of the present invention, the applications can be grouped into seven different categories – (1) One-way Infrastructure-to-Card, (2) One-way Card-to-Infrastructure, (3) Two-way, (4) Card-to-Card, (5) Client Software Applications, (6) Card Distribution, and (7) Dedicated Systems.

BRIEF DESCRIPTION OF THE FIGURES

The above objects and description of the present invention may be better understood with the aid of the following text and accompanying drawings.

FIG. 1 shows a system level diagram of the various components of the interactive media system in accordance with one embodiment of the present invention.

FIG. 2 shows a high level view of the one-way transmit-only electronic card.

FIGS. 3(A) and 3(B) show high level views of a two-way electronic card.

FIGS. 4(A) and 4(B) show high level views of the receiver portion of the electronic card.

FIG. 5(A) shows the data stream format for the card-to-PC communication direction. FIG. 5(B) shows the data stream format for the PC-to-card communication direction.

FIG. 6(A) shows a flow chart of the transmission routine of the electronic card in accordance with one embodiment of the present invention. FIG. 6(B) shows a detailed flowchart of the transmission portion of the transmission routine of FIG. 6(A).

FIG. 7 shows a low level view of the circuitry surrounding the microcontroller in accordance with one embodiment of the present invention.

FIG. 8 shows a low level view of the voltage doubler circuitry in accordance with one embodiment of the present invention.

FIG. 9 shows a low level view of the power and switching circuitry in accordance with one embodiment of the present invention.

FIG. 10 shows a low level view of the electronic card connector.

FIG. 11 shows the key components of the client computer system, including the speaker/microphone, sound card driver, special client remote access software, and the web browser in accordance with one embodiment of the present invention. Note that the browser is optional and that the present invention is operational with just the special client remote access software.

FIG. 12 shows a high level block diagram of the electronic card's reception software in accordance with one embodiment of the present invention.

FIG. 13 shows a flow chart of the reception software in a personal computer.

FIG. 14 shows a signal decoder in accordance with one embodiment of the present invention.

FIG. 15 shows a signal detector in accordance with one embodiment of the present invention.

FIG. 16 shows an exemplary graph of the received signal and the sampled points therein to illustrate the moving average concept in accordance with one embodiment of the present invention.

FIG. 17 shows an alternative embodiment of the one-way Transmit card. This circuit can also be applied to two-way cards for the transmit portion.

FIG. 18 shows a detailed analog front end portion of the receiver circuitry for the electronic card in accordance with one embodiment of the present invention.

FIG. 19 shows a detailed digital core portion of the two-way electronic card in accordance with one embodiment of the present invention.

FIG. 20 shows a block diagram of the card architecture which implements analog recording in accordance with one embodiment of the present invention.

FIG. 21 shows a server architecture which implements the pattern recognition search engine and various databases including an account database, coupon database, incentive points database, merchandise database, and soundtrack database in accordance with one embodiment of the present invention.

FIG. 22 shows a high level block diagram of the pattern recognition search functionality in the pattern recognition search engine in accordance with one embodiment of the present invention.

FIG. 23 shows a high level diagram of a cable TV infrastructure and the manner in which the merchant data is mixed with normal programming.

FIG. 24 shows a high level diagram of a broadcast TV/radio infrastructure and the manner in which the merchant data is mixed with normal programming.

FIGS. 25(A), 25(B), and 25(C) show three embodiments of the component layouts for the electronic card.

FIG. 26 shows the layers of materials that make up the electronic card in accordance with one embodiment of the present invention.

FIGS. 27(A), 27(B), and 27(C) illustrate the transducer construction in accordance with three embodiments of the present invention.

FIG. 28 shows a state diagram of the multi-mode switch software in the electronic card.

FIG. 29 shows a system diagram for the E-Wallet system in accordance with one embodiment of the

present invention.

FIG. 30 shows a flow chart of the operation of the E-Wallet system in accordance with one embodiment of the present invention.

FIG. 31 shows a high level block diagram of the various entities that involved in credit card transactions.

FIG. 32 shows a flow chart of the on-line authentication operation in accordance with one embodiment of the present invention.

FIG. 33 shows the sequence of steps taken by the electronic card, PC, and the web merchant when the customer is attempting to check the trustworthiness of the web merchant via a challenge-response technique in accordance with one embodiment of the present invention.

FIG. 34 shows the sequence of steps taken by the electronic card, PC, and the web merchant when the web merchant is attempting to check the trustworthiness of the electronic card (and hence user) via a challenge-response technique in accordance with one embodiment of the present invention.

FIG. 35 shows the sequence of steps taken by the electronic card, PC, and the web merchant when both the web merchant and the customer are attempting to check each other's respective trustworthiness via a challenge-response technique in accordance with one embodiment of the present invention.

FIG. 36 shows a crypto service provider (CSP) scheme, the entities, and the sequence of steps taken by these entities in accordance with one embodiment of the present invention.

FIG. 37 shows one embodiment of the electronic card decoder when RF signals are used for the PC-to-electronic card communication path.

FIG. 38 shows another embodiment of the electronic card decoder when RF signals are used for the PC-to-electronic card communication path.

FIG. 39 shows another embodiment of the electronic card decoder when magnetic signals are used for the PC-to-electronic card communication path.

FIG. 40 shows another embodiment of the present invention where a hardware PLL technique is used in the electronic card for processing acoustic signals.

FIG. 41 shows another embodiment of the present invention where a software PLL/FLL technique is used in the electronic card for processing acoustic signals.

FIG. 42 shows another embodiment of the present invention where a mixer is used for baseband processing in the electronic card for processing acoustic signals.

FIG. 43 shows an embodiment of the present invention where a special driver is placed between the Windows Mulimedia interface and the default sound card driver so that multiple applications can run concurrently in the computer system.

FIG. 44 shows an alternative embodiment from the system described an shown in FIG. 43 where a special driver is placed between the Windows Mulimedia interface and the default sound card driver so that multiple applications can run concurrently in the computer system.

FIG. 45 shows a diagram of a secure purchasing mechanism in accordance with one embodiment of the

present invention where incentive points/mileage instead of cash can be used to purchase products.

FIG. 46 shows a high level abstracted view of some of the many applications that are enabled by the present invention.

FIG. 47 shows a high level view of another application where benefits are achieved using the versatile electronic card with the conventional magnetic stripe in a system that utilizes a central account database.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

At a high level, this patent specification provides detailed information on the system, the electronic card itself, the base station (e.g., personal computer), and various applications (which may involve various web servers). In particular, the patent specification is organized as follows:

1.0 SYSTEM SUMMARY
2.0 FREQUENCY RANGE
3.0 ELECTRONIC CARD
3.1 TWO-WAY CARD
3.2 CARD TRANSMISSION HARDWARE
3.3 CARD TRANSMISSION SOFTWARE
3.3.1 DATA STREAM
3.3.2 TRANSMISSION ROUTINE
3.3.3 MULTI-MODE SWITCH
3.4 CARD RECEPTION HARDWARE
3.5 CARD RECEPTION SOFTWARE
3.6 CARD MECHANICAL CONSTRUCTION
3.6.1 SHEETS-LEVEL CARD FABRICATION
3.6.2 COMPONENT LAYOUT
3.6.3 CARD LAYERS
3.6.4 TRANSDUCER CONSTRUCTION
4.0 BASE STATION
4.1 CLIENT COMPUTER SYSTEM
4.2 INSTALLATION AND INITIALIZATION
4.3 BASE STATION TRANSMISSION SOFTWARE
4.4 BASE STATION RECEPTION SOFTWARE
4.5 CONCURRENT OPERATION OF MULTIPLE RECORDING SOFTWARE
4.6 SERVER-BASED PROCESSING
5.0 APPLICATIONS
5.1 BROADCAST MEDIA
5.1.1 BROADCAST MEDIA INFRASTRUCTURE
5.1.2 BROADCAST MEDIA COUPON TRANSMISSION
5.1.3 BROADCAST MEDIA COUPON REDEMPTION

5.1.3.1 Password-based Internet Manual Redemption
5.1.3.2 Internet Automatic Redemption
5.1.3.3 Store Redemption
5.1.4 INTERACTIVE TV AUCTION
5.1.5 CONTENT RECORDING FOR SEARCH/REDIRECTION
5.1.5.1 Electronic card Hardware
5.1.5.2 Server Architecture
5.1.5.3 System Operation
5.1.6 BOOKMARKS FOR BROADCAST MEDIA
5.2 SMART E-WALLET SYSTEM
5.2.1 INSTALLATION
5.2.2 OPERATION
5.2.3 SECURITY
5.3 WEB TRANSACTIONS AND AUTHENTICATION
5.3.1 CREDIT CARD INFRASTRUCTURE
5.3.2 ON-LINE AUTHENTICATION
5.3.3 OFF-LINE AUTHENTICATION
5.3.4 PASSWORD GENERATOR
5.3.5 CHALLENGE-RESPONSE
5.3.6 CRYPTO SERVICE PROVIDER (CSP)
5.4 PLUG-INS
5.4.1 PLUG-IN SUBSERVIENT
5.4.2 PLUG-IN DOMINANT
5.5 POINTS/CASH PURCHASING MECHANISM
5.6 BAR CODE READER
5.7 CARD-TO-CARD INFORMATION EXCHANGE
5.8 WEBPAGE-DEPENDENT ACTIVATION
5.9 ELECTRONIC LOYALTY SYSTEM
5.10 ADDITIONAL SYNERGIES WITH VOICE
6.0 NON-ACOUSTIC EMBODIMENTS
6.1 RADIO FREQUENCY (RF)
6.2 MAGNETIC FIELD

1.0 SYSTEM SUMMARY

One embodiment of the present invention provides for a system that allows a user to interact with merchants and other entities via an electronic device, such as television, radio, or personal computer, to conduct transactions of various kinds (e.g., consumer purchase of products/services, security check). The transactions can involve transmitting information of various kinds (e.g., membership information, personal information) and

receiving information of various kinds (e.g., account statements, coupons, special sales offers, other sales information). The user is equipped with an electronic card that can receive and transmit data via sound waves. The interaction is accomplished by using sound from the electronic device's speakers when receiving data and emitting sound from the electronic card to the electronic device's microphone when transmitting data. In the various embodiments, the sound waves can be audible or ultrasonic (which can be slightly audible to some groups of people).

Note that in addition to the electronic card, the client software, and the various applications, the communications protocol itself also contains various unique aspects. The communications scheme can be between cards and between the card and the base station. The direction of the transmission can be one-way or two-way.

FIG. 1 provides a high level view of the interactive system in accordance with one embodiment of the present invention. At the core of the system is an electronic card 10 (or electronic card 10). As discussed in greater detail below, the electronic card 10 is a card that complies with standard credit card form factor requirements while containing some electronic circuitry and transducer(s) for processing data, storing data, transmitting data, and receiving data. In some embodiments, the electronic card 10 also contains an LCD display. The transmitted and received data are in the form of sound waves that are either audible or ultrasonic.

Although this embodiment requires the electronic card to adhere to ISO-compliant credit card form factor specifications, other embodiments do not require such compliance. Indeed, other embodiments involve large electronic devices that contain the logic and functionality described herein in this patent specification. Although a major advantage of the electronic card in accordance with one embodiment is its credit card form factor size, the spirit and scope of this patent application extends to any electronic device regardless of physical form factor.

In one embodiment, as illustrated in the general diagram of FIG. 1, the electronic card 10 can be used by the user to interact with almost any infrastructure electronic device, so long as the infrastructure electronic device is equipped with hardware that is not necessarily dedicated to interact with the electronic card 10 and supporting software. Thus, the electronic card 10 can transmit data to a radio 11 via sound waves 19a, television 12 via sound waves 19b, a computer 14 via sound waves 19c, and some electronic device in conventional store 13 via sound waves 19d. Of course, each of these infrastructure electronic devices must have corresponding microphones to receive the sound waves (e.g., microphone 14c for computer 14). In the case of the radio 11 and television 12, the electronic card 10 can emit infrared, RF, or magnetic signals, instead of sound waves if these devices do not contain a microphone. Also, the electronic card 10 is equipped with transmission circuitry, microprocessor circuitry, memory, and a transducer to generate the sound waves.

Conversely, the infrastructure devices can deliver data to the electronic card 10. Thus, the electronic card 10 can receive data from radio 11 via sound waves 19w, television 12 via sound waves 19x, computer 14 via sound waves 19y, and some electronic device in conventional store 13 via sound waves 19z. Each of these infrastructure electronic devices must have corresponding speakers to emit the sound waves (e.g., speakers 14a

and 14b for computer 14). The electronic card 10 is equipped with reception circuitry, microprocessor circuitry, memory, and a microphone to receive and process the sound waves.

When the electronic card 10 is used with a personal computer 14, other commercial opportunities open up. For example, the user could use the electronic card to interact with a web merchant 17 and a web portal 18 via the Internet 16. Of course, the average consumer would need access to the Internet via some Internet Service Provider (ISP) 15. The electronic card 10 could be used to facilitate the sales transaction between the web merchant 17 and the user. Furthermore, the electronic card 10 could provide a greater sense of security to various web players (i.e., web merchants, credit card issuers, acquiring banks, consumers themselves). These and other applications of the electronic card-based interactive system are detailed below.

The following is a sampling of the system specifications.

System Feature	Specification Description
Card transmission speed	Card-to-PC: 200 bps
EDAC mechanisms	Bytes transmitted with parity, with on-the-fly error correction and detection
Card lifespan	Up to 10,000 key presses
Card dimensions	0.76 mm x 85 mm x 54 mm
Robustness	Sustains bending and torsion; highly resistant to electromagnetic radiation
Range	1-2 feet from microphone
PC Operating System	Windows 95/98
System Requirements	Pentium 100 MHz; 32 MB RAM; 1MB free space on hard disk; sound card
Browsers	Internet Explorer 4.0 and higher; Netscape Communicator 4.0 and higher; AOL

The transmission technique is frequency shift keying (FSK), as described in more detail below. In other embodiments, the transmission technique is n-ary phase shift keying (PSK). However, in contrast to the FSK technique where magnitude was used in the DFT banks to select the two relevant frequency channels, nPSK relies on selecting a particular channel for detection and then determine phase drift and offset by examining the I and Q channels.

The spectrum of applications enabled by the electronic card is broad. From a complexity point of view, the applications may include, at one extreme, the simple task of providing information to a web merchant or store (i.e., "I am present.") to a medium complexity task of automating the process of filling out a form and, at the other extreme, performing a complicated series of tasks involving security, context sensitivity actions, and multiple modes. For the various embodiments of the present invention, the applications can be grouped into seven different categories – (1) One-way Infrastructure-to-Card, (2) One-way Card-to-Infrastructure, (3) Two-way, (4) Card-to-Card, (5) Client Software Applications, (6) Card Distribution, and (7) Dedicated Systems. Each of these categories of applications will be described in greater detail below.

2.0 FREQUENCY RANGE

In one embodiment of the present invention, the interactive system uses acoustic waves. Preferably, acoustic signals in the ultrasonic frequency band are used. In one embodiment of the present invention, acoustic waves in the ultrasound frequency range will be used. Ultrasound is in the 15-28 kHz frequency range,

and typically higher. Of course, the reader should realize that ultrasound has no fixed upper limit. In the preferred embodiment, the frequency range of 17-20 KHz has been selected for the ultrasonic acoustic signals. In particular, one embodiment uses 17.5 kHz for one FSK frequency and 18.5 kHz for the other FSK frequency. These numbers were selected because half (for Nyquist sampling) of the 44.1 KHz recording rate for CD-quality audio is 22.05 KHz. The upper limit of 20 KHz was selected because in most sound systems, sound above 20 KHz is filtered out sharply. Thus, this embodiment uses sounds in the frequency range that can be supported by the current sound systems that are installed in today's computer systems. In another embodiment, the sound waves can go down to 10 kHz while still retaining the benefits of the ultrasonic frequency signals.

Ultrasound has certain benefits over the audible frequency range. First, most people cannot hear ultrasound and when they do hear it, it is not noticeably loud. Normally, young people can hear in sounds in the frequency range of 0-20 kHz, adults can hear in the 0-18 kHz range, and the older senior citizens can hear in the 0-16 kHz range. Some animals, such as dogs, can hear sounds at much higher frequencies.

Second, ultrasound is less subject to interference. Most ambient noise is audible and audible sounds are omnidirectional. Thus, using audible frequencies would subject the electronic card to all sorts of unwanted interference. As the sound is at a higher frequency range (such as ultrasound), it also becomes more directional. In addition to the directionality, the higher frequency sounds travel shorter distances. Thus, ultrasonic noise sources, if any, need to be generally pointing directly at the microphone and be reasonably close to the ultrasonic electronic card to cause any interference.

Third, the bandwidth is greater at the higher frequencies. Therefore, more information can be transmitted per unit of time. This is important because the data transfer should not occur over an extended period of time.

Fourth, to implement ultrasound, the transducers are smaller than conventional sound transducers. Because the electronic card will comply with the major credit card standards, this small size is particularly important. The smaller size transducers will take up less space and if placed strategically in the card, the user will be able to bend the electronic card without any damage to the components therein.

Fifth, the ultrasonic electronic card can be used with existing non-dedicated base station infrastructure equipment. For example, the sound device (e.g., "Sound Blaster" sound card) in a personal computer supports the ultrasound frequency band. Accordingly, with no hardware modifications, additions, or subtractions of any kind, the electronic card of the present invention can interface with the existing base station infrastructure.

When ultrasound is used, the electronic card has a range of approximately 1-3 feet. Other frequency ranges, such as the audible frequency range, provide greater distances. Thus, the particular acoustics that the electronic card uses determines the transmission distance. Typically, the user (and hence the card) would be fairly close to a microphone to pick up the acoustic signals transmitted by the electronic card. This also applies to the reception of the acoustic signals by the electronic card.

Of course, the selection of the frequency range for the acoustic signal depends on the application. If the base station that communicates with the acoustic electronic card is a conventional telephone, for example, audible acoustic signals should be used since filters in the telephone network remove signals in the ultrasound

range. Thus, in one embodiment, the electronic card emits acoustic signals in the non-ultrasonic audible frequency range so that it can communicate with band-limited sound systems. In another embodiment, the particular audible frequencies that are used are based on the DTMF system.

3.0 ELECTRONIC CARD

The electronic card 10 (see FIG. 1) will now be discussed. Initially, a two-way card will be described, followed by individual transmission and reception components. Note that some embodiments require a two-way card, while other embodiments require a transmit-only one-way card or a receive-only one-way card. In all of these embodiments, at least one switch that is physically activatable by the user is provided on the card. In some embodiments, multiple switches are provided to provide additional functionality.

3.1 TWO-WAY CARD

A high level block diagram of a two-way electronic card will now be described with respect to FIGS. 3(A) and 3(B). For one-way transmit-only cards, the transmission portion of the two-way card is used. For one-way receive-only cards, the receiver portion of the two-card is used.

FIG. 3(A) shows one embodiment where a receive transducer and a separate transmit transducer are provided. In FIG. 3(A), memory unit 30 is coupled to processing unit 31, which is in turn coupled to reception unit 32 and transmission unit 33. The received signals in the reception unit 32 are provided to the processing unit 31. Also, the processing unit 31 determines what data to transmit with the transmission unit 33. The reception unit 32 is coupled to the receive transducer 36, while the transmission unit 33 is coupled to the transmit transducer 37. A power and switching unit that is identical to unit 24 of FIG. 2 is also provided but not shown in FIG. 3(A).

In contrast, FIG. 3(B) shows another embodiment where a single transducer is provided for both reception and transmission. Again, the memory unit 30 is coupled to the processing unit 31. The processing unit 31 is coupled to an input/output unit 35. The input/output unit 35 includes a reception unit 32, a transmission unit 33, and a switchable transducer 34. The switchable transducer 34 is under the control of the processing unit 31 since the processing unit 31 knows when the electronic card should transmit and receive. Any received signals detected by the switchable transducer 34 are provided to the reception unit 32, while any signals that need to be transmitted are provided by the transmission unit 33 to the switchable transducer 34.

Further details of the card's transmission and reception hardware units will be provided below. Also, the software in the microcontroller 31 includes:

(1) transmission software
(2) reception software
(3) encryption software
(4) memory retrieval and storage

These four parts of the card's software will be discussed further below.

3.2 CARD TRANSMISSION HARDWARE

The transmission hardware will now be discussed. In particular, the transmission hardware will be discussed in the context of a one-way transmit-only electronic card 10 as shown in FIG. 2. The electronic card

10 is essentially a portable device with a processing unit 21, memory unit 22, output unit 23, and power and switching unit 24. The processing unit 21 provides the computation and control necessary for operating system functionality, cryptography, communication, memory management, and code updates. This unit comprises a dedicated chip microcontroller, DSP functionality, a smartcard chip, and a bus system. Preferably, the processing unit used has sufficient power (a few MIPS), and includes some on-chip or off-chip memory for storing and/or generating a cryptographic signature. A Microchip 12C508, 12C672 or higher processing unit is preferred. In one embodiment, a Microchip PIC16F84 is used which uses an on-chip EEPROM.

Preferably, the microcontroller should satisfy the following requirements:

(1) working voltage of 2.2 V depending on the battery. Although 2.2 V is adequate for standard batteries, 2.0 V is preferable. A voltage of 3.0 V also works.
(2) low supply current of approximately 2 mA
(3) MIPS: at least 0.5
(4) Program memory of 2KBytes, although 2 K instructions is preferable
(5) EEPROM of 8 Bytes
(6) Data memory of 100 Bytes (although the Microchip PIC16F84 has 68 Bytes)
(7) Timer is desirable
(8) RC input for clock source in one embodiment, but an external frequency source can be used for some ASIC implementations
(9) Die
(10) Temperature tolerance of 0-50 degrees Celsius for working conditions and –10 to 70 degrees Celsius for storage
(11) Watchdog functionality to add reliability to the microcontroller (resets the microcontroller if it starts to malfunction)
(12) I/O: at least 4 I/O pins are needed with 2 spares.
(13) Sleep mode for reducing current after card operation has been executed
(14) Low cost

The memory unit 22 is used to store data relevant for the card user. The memory unit 22 comprises read only memory (ROM), random access memory (which may also be incorporated in the processing unit 21), and an EEPROM to permanently store externally received data. Specifically, the memory unit can contain data for security encryption, personal details, electronic coupons, and upgradeable software. In one embodiment, the memory unit 22 is a non-volatile memory. The digital ID stored therein is 8 bits long in one embodiment and after encryption, it becomes 32 bits (for main digital ID bits, checksum, CRC, header, etc.).

The output unit 23 physically creates the transmitted signal. It is preferably made from a metal plate with a piezo material (e.g., piezo ceramic material with a small thin metal plate) on it. Being very thin, these transducers produce the required intensity at the ultrasonic frequencies. It also comprises driver circuitry and amplification circuitry connected between it and the processing unit 21.

The power and switching unit 24 comprises a very thin battery with enough capacity and drain ability, or with recharge capabilities. A switch is provided for turning the card on or off and for changing states (or modes) of the card. Aside from a mechanical switch, the processing unit can also automatically turn the power and switching unit 24 off. The card may be programmed so that the system wakes up at the occurrence of certain wake-up events. Power supply amplification and filtration are also provided.

Referring now to FIGS. 7-10, a detailed low level description of the one-way card will now be provided. FIG. 7 shows the Microchip PIC16F84 microcontroller and surrounding circuitry. The processor is a PIC 16F84, which is fast and contains on-chip data EEPROM. The PIC 16F84 also provides for three options to provide the clock source – (1) external crystal oscillator, (2) external oscillator circuit, and (3) external RC circuit. Because of the size constraint of the electronic card, a crystal clock source could not be used. Also, an external oscillator circuit, while feasible, contains too many components. Accordingly, an RC circuit (R2 and C2) is provided at the OSC1/CLKIN input. With the particular values shown in FIG. 7, the clock frequency selected is 4MHz. Reset is provided at the MCLR input.

At the VDD input, the microcontroller is coupled to Vdd3, capacitor C1, and VDD-. The power supply, which is discussed later in conjunction with FIG. 9, provides 2-3 volts. The microcontroller however needs 4-6 volts the transmission circuitry and also because the microcontroller can operate faster with higher input voltage. A voltage doubler circuit of FIG. 8 provides the doubling needed to effectively operate the microcontroller.

The RA0 pin is used as an output pin. The voltage provided at this pin mirrors the voltage doubled input VDD- and is also provided to the power and switch unit which is described below in FIG. 9. Essentially, the RA0 prevents the operation of the electronic card during transient states (turning on or turning off).

The output at RB1 is coupled to buzzer LS1, which generates the acoustic signal. In one embodiment, this buzzer is an FT12-T.

Pins RB5-RB7 are used for programming and testing the microcontroller. In addition, the electronic card connector of FIG. 10 is used for programming and debugging.

The voltage doubler circuit will now be described with respect to FIG. 8. The voltage doubler is a high efficiency device. A charge pump scheme is used because of the big physical size of the needed inductors in other schemes. However, in other embodiments, the use of such inductors is feasible in the credit card-sized electronic card 10 of FIG. 1. The Maxim voltage converter MAX861 takes as its input at Vdd and outputs a doubled voltage VDD- at pin Out. The VDD- is provided to the VDD input of the microcontroller in FIG. 7. The additional circuitry of C4, C5, and Motorola diode MBR0503T1 provides protection to the chip from overvoltage at the input Vdd.

The power and switching circuit will now be described with respect to FIG. 9. The power source is a Varta LPF25 battery which is small, has low current drain, and provides just enough voltage for the rest of the card's circuits. In one embodiment, it outputs 2-3 volts.

A switch SW1 is provided. The switch is used by the user to enable the transmission of data in the electronic card. The user should keep the switch pressed for as long as the transmission requires, which is

usually a short period of time since the data transmission is relatively fast at 200 bits per second. However, sufficient protection circuitry is provided so that if the user releases the switch prematurely, the proper operational voltage is delivered to the processor so that the data can be transmitted without fail. When the switch SW1 is pressed, transistors Q1 (Fairchild Semiconductor MMBT2907A) and Q2 (Fairchild Semiconductor MMBT2222A) provides a smart switch function. After turning on, these transistors Q1 and Q2 are turned off by the Microchip processor of FIG. 7. Transistor Q1 passes the voltage from the battery to the voltage doubler circuit of FIG. 8 as voltage Vdd1. The capacitors C9 and C10 allow for the power to ramp up smoothly and to hold the Vdd1 voltage for some time period. The transistor Q2 receives a digital command from the processor and shifts voltage levels for transistor Q1 as needed. The discrete bipolar transistors are used because of their low leakage current, which can be as low as a few nAmps.

The combination of Q1, Q2, micro power voltage reference D2 (National Semiconductor LM385-2.5/SO), and their resistors are provided to confirm the validity of the signal. This circuit ensures that any signal above 4 volts from the processor via RA0 will deliver power to the power and switching circuit for its effective operation. However, any signal below 3 volts will be ignored so that latch-up of the circuit will be prevented during transient states (turning off or turning on). This circuit consumes less than 10 nA in the off state. An alternative circuitry for the LM385-2.5 can be a reset supervisor which will reset the microcontroller when the voltage drops below the allowed threshold. Such IC's can be the equivalent of MAX821 or MAX6326.

An electronic card connector J1 is also provided as shown in FIG. 10. The electronic card connector is used to program, test, and debug the electronic card. In alternative embodiments, however, the electronic card connector is not provided. Instead, the electronic card is programmed by the manufacturer of the microcontroller. In another embodiment, the card is programmed using the electronic card connector and then the circuits including the electronic card connector are laminated over with suitable material, including printed PVC.

An alternative embodiment of the card transmission hardware provides for two added benefits – lower power consumption and greater power output. With the lower power consumption, battery life is extended. With the greater power output, reliability is increased with lower bit error rate. A high level block diagram of this alternative embodiment is shown in FIG. 17.

In FIG. 17, a battery 190 is provided. This battery supplies 2-3 volts nominal voltage. In one embodiment, the battery is a single Varta LPF-25 battery that provides 2.7V nominal at 1 mA discharge (25 mAH).

A mechanical switch 191 provides the circuit connection when it is closed. In one embodiment, the mechanical switch is a dome switch. A silicon switch 192 is also provided for maintaining power after the user has activated the mechanical switch 191. The silicon switch 192 makes sure that the rest of the transmission circuitry in the card has enough power to function properly for a period of time after the user has activated the mechanical switch 191 in the event that the user lifts the mechanical switch 191 prematurely.

A voltage regulator 193 is coupled to the battery 190 via the mechanical switch 191 and the silicon switch 192. The voltage regulator 193 stabilizes the frequency of the microprocessor 194 and lowers the current consumption of the battery 190. The voltage regulator 193 is an LDO with low decoupling capacitors and low current. The output voltage is 2.2V. This IC can also be omitted in expanse to a lesser frequency stability. The voltage is provided to the microprocessor 194, which in one embodiment is a Microchip PIC16F84. An electronic card connector 197 allows for the microprocessor 194 to be programmed. Additional contacts are provided for factory testing and debugging.

A voltage multiplier and driver 195 receives signals from the microprocessor 194 and provides an output at 6Vpp to the transducer 196. An alternative circuit can double the battery voltage to 5Vpp, with fewer components. The voltage multiplier and driver 195 doubles the input voltage to generate a square of the power out. At the very least, the transducer needs twice the battery voltage to be driven. The transducer 196 exhibits approximately 5 nF of capacitance.

In contrast to the above embodiment where a single channel is used to transmit either f0 or f1 for this FSK scheme, two channels can be implemented to increase the bit rate. In one embodiment, the two frequencies to be transmitted are summed in the electronic card where the single transducer transmits the summed signal to the PC. In another embodiment, each frequency to be transmitted is associated with a transducer in the electronic card, where after being transmitted, the transmission medium (e.g., air) adds the two frequency components before being received by the PC. In a further embodiment, one transducer is associated with frequencies f1 and f2, while another transducer is associated with f3 and f4. At any moment in time during a transmission, each transducer transmits one bit so that the electronic card with two transducer essentially transmits two bits at the same time.

Accidental activation of the TX switch in the electronic card can potentially drain the power from the battery supply unless appropriate safeguards are taken. In one embodiment, circuitry is provided such that if the switch is pressed for more than a threshold amount of time (e.g., 1 sec), then the electronic card will turn itself off. No transmission will be possible unless the switch is deactivated first. In another embodiment, the microprocessor is programmed with a time-out logic so that if the TX is pressed for more than a threshold amount of time, then the microprocessor unit will turn off the power.

3.3 CARD TRANSMISSION SOFTWARE

The software in the electronic card primarily performs the following routines:

(1) read data (e.g., ID, sync byte) from memory
(2) write data (e.g., increment counter value) to memory
(3) perform DES3 encryption to calculate Series
(4) calculate checksum
(5) beep audible feedback to user
(6) initialization
(7) transmit data
(8) receive data

These and other related features of the card software will be described further below.

3.3.1 DATA STREAM

The software for the card resides in the microcontroller and is written in Assembly language. On activation of the card (i.e., press of the switch), the card transmits a data stream that comprises a header, data, a footer, and start/stop bits. The header, footer, and start/stop bits are fixed. However, the software calculates the data portion.

Referring now to FIG. 5(A), the data stream includes f0 (approximately 100 msec long or 24 bits), f1 (approximately 20 msec long or 5 bits), a synchronization byte, a known byte, the data portion (96 bits), and a checksum (CRC) byte. The portion of the data stream beginning with the synchronization byte to the checksum byte is divided up into bytes of data with start and stop bits inserted between the bytes. Thus, at the beginning of a byte is a start bit (e.g., logic 1) and the end of that same byte is a stop bit (e.g., logic 0).

The f0 and f1 portions of the data stream represent the two FSK frequencies employed by the system. The f0 and f1 portions are pure sinusoids of the base FSK frequencies and are transmitted first to allow the receiver to enable detection.

The sync byte is a sequence of alternating bits with some pattern (e.g., 01010101) that enables synchronization of the receiver with the received data stream. The known byte is a byte known to both the receiver and transmitter of the system. It assures the receiver that this signal is indeed a signal and not noise.

The data portion is the major part of the data stream where each bit is translated to a wave of frequency f0 or frequency f1 with a length of T msecs that determine the raw bit rate. The discussion below details how one embodiment calculates the data portion, which is denoted by the variable DataOut. In other embodiments, DataOut is calculated differently and can be any desired length depending on the functionality desired by the press of the TX switch.

The checksum (CRC Code 32) byte is transmitted to ensure no errors in the received data stream. Also, as mentioned above, start/stop bits are inserted into the portion of the data stream beginning with the synchronization byte to the checksum byte. This portion is divided up into bytes of data. Start and stop bits are inserted between the bytes. Thus, at the beginning of a byte is a start bit (e.g., logic 1) and the end of that same byte is a stop bit (e.g., logic 0). The start and stop bits are utilized for resynchronization. Because of the clock source in the card has errors, the transmitted signal drifts in frequency which results in missing a sampling point (or sampling the wrong point). The resynchronization provides for this correction.

Returning now to the data portion of the data stream, the software makes use of certain algorithms along with some numerical attributes of the card. Each card is associated with a group ID, individual ID, and a key. The group ID identifies this card with other similarly situated cards; that is, if ABC Corporation distributed the card to its members, the card would have ABC Corporation's group ID number. All cards distributed by XYZ Inc.'s web portal would be associated XYZ's group ID number. The individual ID is essentially the card's serial number and is unique to that card. The key is a secret private key. Note that the terms "private/public key" are from asymmetric crypto systems, but in the current embodiment, only one key is used and is usually referred to in the literature as "the key" or "the secret key". The microcontroller also

manages a counter in non-volatile memory, which in one embodiment, increments by one each time the card's TX switch is pressed. In one embodiment, the size of these card numerical attributes are:

Group ID: 32 bits

Individual ID: 32 bits (in another embodiment, 16 bits)

Key: 16 Bytes

Counter: 32 bits

Based on these numerical attributes, the microcontroller in the card creates a complex numeric series that is not easy to predict. One preferred series is:

Series = DES3(Key, Msg), where Msg = [Group ID, Counter]

DES3 represents the Data Encryption Standard (DES) cryptographic algorithm as defined by the U.S. Bureau of Standards (FIPS PUB 46-2, 1993 and FIPS PUB 74, 1981). Msg is the concatenation of the 32-bit Group ID and the 32 bit Counter value, which results in a 64-bit number. The Series is a 64-bit number. The microcontroller employs the algorithm in the encryption portion of the software to calculate this Series. However, what is actually transmitted for the data portion of the signal is:

DataOut = [Series, Individual ID]

Here, DataOut represents the concatenation of the 64-bit Series which is a DES3 encrypted number and the unencrypted 32-bit Individual ID, which results in a 96-bit number. On every activation of the card, the counter is incremented and the next code in the series is used.

In an alternative embodiment, security can be assured by storing identical sets of random numbers both on a memory unit in the card, and on the authentication server. That random number takes the place of the DES3 encrypted number element of the DataOut series described above. The advantages of such an embodiment are twofold. First, it clears processing resources on the card, or reduces the complexity of the processor needed, since the encryption algorithm no longer is practiced. Also, theoretically, a random number scheme is virtually impossible to decrypt.

3.3.2 TRANSMISSION ROUTINE

A high level description of the transmission routine in the electronic card will now be provided with respect to FIG. 6(A). The transmission routine begins at step 50. At step 51, the parameters Known Byte, Sync Byte, Series, Individual ID, and Checksum are placed in the send buffer. To perform this step, some of these parameters are either retrieved from memory (Known Byte, Sync Byte, Individual ID, checksum, and also the counter value) as well as calculated (Series). Step 52 requires that the base frequencies f0 and f1 in FSK are selected. Step 53 transmits the data. The transmission routine ends at step 54.

FIG. 6(B) illustrates a more detailed flowchart of the transmission process. This flowchart provides more details for steps 51 and 53 of the FIG. 6(A). The flowchart begins at step 60. At step 61, the microcontroller reads the counter value. At step 62, the microcontroller calculates the Series based on the Key and the Msg, as described above. For each press of the TX switch, the microcontroller increments the counter

value by one. At step 63, the microcontroller determines DataOut as the concatenation of the encrypted Series and the unencrypted Individual ID. Having calculated the data portion of the data stream, the microcontroller is now ready to transmit the data stream.

At step 64, the microcontroller transmits f0 for approximately 120 ms (or 24 bits) and f1 for approximately 20 ms (or 5 bits). At step 65, the start bit (logic 1) is transmitted. A byte of a portion of the data stream beginning with the synchronization byte and ending with the CRC bytes are then transmitted at step 66. The stop bit is transmitted at step 67. If any more data from the sync byte...CRC portion of the data stream is remaining, then the microcontroller goes back up to step 65 to transmit the start bit. It then transmits another byte of data, followed by the stop bit. If no more data is remaining to be transmitted, the process ends at step 69.

After the data has been transmitted, the card turns itself off to conserve battery power. In another embodiment, the card goes into receive mode for a few seconds after the transmission steps in anticipation of receiving data. Thereafter, the card turns itself off to conserve power. In still another embodiment, the card provides an audible feedback (e.g., beep) to alert the user that the data has been successfully transmitted. Some delay is provided after the beep to compensate for the case where the CPU turns off the power before the user lifts his finger off the switch. Then, the card turns itself off, or alternatively, goes into receive mode followed by power off.

Note that the system uses FSK to transmit the signals. In one embodiment, the system is capable of being modified so that the base frequencies (f0 and f1) are adjustable. This modification can occur in realtime and in automated fashion to ensure that the receiver receives a good signal. Similarly, automatic retransmission is also provided as a feature of the electronic card. For example, if the user presses the switch on the card longer than expected, this may imply that the transmission is bad because the user did not see the appropriate response from the PC (e.g., an audible beep from the PC to indicate that the signal was properly received). In this case, the card will, after some delay, retransmit the data stream possibly using a different set of FSK frequencies.

Some other design considerations should be taken into account. The program code necessary to execute the above process is relatively small to fit into the small microcontroller. The timing is very exact so as not to introduce errors and audible noise to the communication. Since a low cost processor is used (e.g., Microchip PIC16F84), PWM or DTOA units are not available; therefore, the digital output pins of the processor will be used for transmitting the signal.

In one embodiment, the bit rate for the transmitted data is 200-600 bits per second.

3.3.3 MULTI-MODE SWITCH

In accordance with one embodiment of the present invention, the electronic card contains one switch. To provide multiple functionality for the electronic card (and the client base station, such as a personal computer), the electronic card is equipped with multiple modes. Each mode is associated with some unique function apart from the other modes. In one embodiment, the mode of the card depends on the length of time that the switch is pressed by the user. To assist the user in determining what mode he has invoked, or

conversely, how long he has pressed the switch, an audible feedback such as a beep sound is generated by the electronic card. Thus, for every T seconds that the switch is pressed, a single audible beep is generated. In one embodiment, T is 0.25 seconds. A single beep indicates that the electronic card is in one mode, while two beeps indicate that the electronic card is in another mode.

Referring to FIG. 28, a state diagram is provided. At state 280, the electronic card is turned off. So long as the switch is not pressed, the electronic card is not operating.

When the switch is pressed, the power of the card is turned on. This is represented by state 281. The card may require the switch to be pressed for some minimum amount of time before it is recognized as a valid switch press. In one embodiment, this minimum amount of time is 0.25 seconds. When the switch is pressed for this minimum amount of time, the electronic card will provide an audible beep every T seconds (e.g., 0.25 seconds) so long as the switch is depressed. The number of beeps indicates to the user the mode of the electronic card. Of course, the user would already know what mode he wants to place the electronic card in and he holds down the switch until the desired number of beeps is produced.

When the user finally releases the switch, the number of beeps is temporarily stored in memory in the electronic card in state 282. This beep number can then be used by the electronic card to perform its function in accordance with the mode selected by the user. Alternatively, the number of beeps along with the card authentication data (e.g., Series, checksum, Individual ID) are transmitted to the client base station. The client base station can then receive the number of beeps and interprets the mode of the communication. At state 283, the CPU in the electronic card turns off the power to conserve battery power.

Some exemplary modes are as follows. A single beep indicates that the electronic card is in transmit mode. Whatever data that needs to be transmitted will be transmitted shortly. After the data has been transmitted, the electronic card turns itself off. In another embodiment, a reception period (e.g., 1 second) follows immediately after the transmission of data. This is then followed by power off.

A double beep indicates that the electronic card is in receive mode only for a short time period. In another embodiment, the electronic card sends the two beep indication to the client base station. The software in the client base station interprets the two beep indication as displaying a drop-down menu list of actions. The user can then select one of the listed actions. In one embodiment, these listed actions can be: (1) launch the browser, (2) launch the browser, if it is not already launched, and go to the user's designated home page (or the home page of the company sponsoring the electronic card); (3) launch the browser, if it is not already launched, and go to some designated website; (4) launch the user's email application, if it has not already been launched; (5) send email in the user's outbox and receive email from the user's mail server; (6) perform simple diagnostics by sending data to the electronic card, followed by receiving some data from the electronic card; and (7) perform any other series of actions (predefined or assigned by the user).

In another embodiment, the list of actions that are displayed on the client base station's monitor is context-sensitive. Thus, if the user's browser is already opened and displays the home page, one of the actions listed will not be to launch the web browser and go to the user's home page. Typically, one of the actions listed will be to fill out a form. So, if a user was shopping on the web and found some merchandise he would like to

purchase, he proceeds to the checkout line on the website where he encounters a form. The user presses the switch on his electronic card and waits for two beeps to sound before releasing the switch. The client base station receives the two-beep indication and proceeds to list action items in menu form. One of the action items is to "fill out a form." When the user selects this action on the list, the client base station proceeds to fill out the form on that web page to automate the purchasing process for the user. The client base station would have all the information necessary to fill out such a simple purchase form – name, billing address, shipping address, phone number, credit card number, credit card expiration date, etc. Once this form has been filled out, the user can use the browser in the conventional manner to complete the sales transaction. Form filling functionality details are provided below.

In another embodiment, three beeps indicate that the electronic card should reset. Similarly, three beeps could indicate that the electronic card should erase the contents of its battery backed-up RAM. If the RAM is used to store downloaded data off the Internet or some broadcast media device (e.g., TV or radio), this data is then erased.

In a further embodiment, a text-to-speech conversion feature is provided in the electronic card. An audio file is also stored in the electronic card. Each audio file is associated with one of the beep numbers; that is, an audio file is associated with a single beep and another audio file is associated with two beeps. Thus, the user need not remember what function corresponds to how many beeps. When the user has released the switch after N number of beeps, the electronic card plays the audio associated with the N beeps. For example, if the user selected two beeps, the played audio file says, "On-screen menu? One beep for YES and two beeps for NO." If the user did indeed want an on-screen menu list of actions to be displayed on the client base station monitor, he would press the electronic card switch until one beep sounds. Otherwise, he would press the switch until two beeps sound.

As described above, the electronic card can have one switch or multiple switches. Similarly, the audible feedback can vary from a single beep to multiple beeps. Based on the context or the action taken by the user, the audible feedback or alert can have different sounds (e.g., beep, buzz, ring). Additionally, the audible sound can be provided at the beginning or at the end of the action taken by the user. In other words, to use the example above, the beep can sound at the beginning of every T seconds instead of at the expiration of every T seconds.

One attractive application of either a multi-mode switch or of multiple switches on a single card relates to using the same card at base stations with diverse reception/transmission capabilities. For example, certain base stations, such as ordinary phones in a "Plain Old Telephone" ("POTS") network, are capable of receiving and passing on sounds in the audible, but not in the ultrasonic range. Where it is desirable to have a single card use audible transmissions in that environment, but ultrasound in other environments, a multiple switch or multi-mode switch as described above can be used. Specifically, in a multimode embodiment, a single press of the switch would activate an ultrasonic transmission terminated by an audible beep for user feedback. A longer press could result in (i) either the ultrasonic transmission or a simple pause, followed by (ii) either a terminating

"beep" for user feedback or none; and (iii) by an audible transmission for use over the phone or another similarly limited device.

There are a number of examples of the types of cards that would be attractive when implemented as cards tailored for use with highly functional acoustic base stations like computers or base stations that are more acoustically limited. For example, when implemented as a credit card, this multimode card would offer the cardholder the security of knowing that even a customer service representative does not get access to their credit card number, since it will sound like modem noise, which is actually transmitting a one-time code that cannot be reused (Described below). Just a few examples include frequent flyer or loyalty cards that can be used on the phone or via an Internet computer to accrue or spend points, car reservation services, and membership cards of all sorts.

3.4 CARD RECEPTION HARDWARE

The reception unit 32 will now be described in greater detail with respect to FIGS. 4(A) and 4(B). The primary objective of the analog front end of the reception unit is to detect the transducer's response to audio signals, amplify the transduced signals, filter them, and pass them to the microcontroller's A/D for digital processing. FIG. 4(A) shows a transducer 40 receiving the audio signal, transducing the acoustic signal to an electrical signal such as a voltage change, and delivering the transduced electrical signal to a pre-amplifier 41. The transduced electrical signal is at level of tens of microvolts (e.g., 10 microvolts).

The pre-amplifier 41 is a high impedance amplifier that amplifies the transduced electrical signal. It amplifies the signal 100 or 200 times the input. Thus, the output of the pre-amplifier 41 is at 1,000 microvolts or 1 mV. The pre-amplifier 41 then sends the amplified signal to a band pass filter 42.

The bandpass filter 42 is a filter with a Q of approximately 8 to filter the signal. In one embodiment, it passes signals in the 17-20 kHz range for the ultrasonic frequencies. A high pass filter is also provided on top of the bandpass filter to further attenuate speech. The design of the bandpass filter 42 accounts for the limited gain margin of the op-amps at the center frequency. The classic computation of Q should also be altered for compensation. The bandpass filter 42 passes the filtered signal to an automatic gain control (AGC) circuit 43, which then delivers the signal to the microcontroller 44.

The combination of the pre-amplifier 41 and the bandpass filter 42 uses a non-inverting MFBF scheme as a compromise to obtain the high Q and high input impedance. The pre-amplifier 41 needs a high input impedance, but the bandpass filter 42 with a high Q has very low input impedance. The gain in the lower frequency ranges is 1 (instead of decaying in 20 dB/dec), but this still leaves more than 40 dB of attenuation compared to the center frequency. The next blocks with the high pass filter (see FIG. 4(B)) deal with the further attenuation at lower frequencies.

The AGC circuit 43 will now be discussed with respect to FIG. 4(B). The AGC 43 keeps a fixed level of amplitude on the microcontroller's input and is located after the bandpass filter 42 to maintain a stable output (i.e., low phase shifts inside the AGC loop). The output of the AGC 43 is a frequency shift keying (FSK)

signal. In one embodiment, the dynamic range of the AGC 43 should be approximately 40 dB. Also, the AGC 43 works with low current and low voltages (e.g., 2 volts) with low amplitude variance at the output (input to the microcontroller 44). The microcontroller 44 determines whether the FSK signal is a signal at one frequency f0 or another frequency f1.

In the AGC 43, the signal at the output of the band pass filter 42 is provided to a divider 45, which outputs a signal at a relatively constant amplitude and low level. This signal is delivered to a gain and high pass filter circuit 46. The gain circuit is a constant gain amplifier with a fixed gain of approximately 300 dB determined mainly be the feedback resistors ratio. The input of this block is approximately 3.3 mVp-p and the output is approximately 1 Vp-p. This gain is large compared to the amplifier's open loop gain, and the amplifier has a relatively small gain margin at the desired frequency. This results in a reduced gain (compared to the lower frequency with the same resistors ratio), and a phase shift. However, the signal is not distorted. The high pass filter portion of the circuit 46 is realized by adding a capacitor to the feedback resistors. This high pass filter further attenuates speech frequencies. The output of the gain and high pass filter 46 is provided to the microcontroller 44 for further processing.

An amplitude estimator 47 is placed in a feedback loop from the output of the gain and high pass filter 46 to the input of the divider 45. The amplitude estimator 47 comprises two low end op-amps – an absolute value block and an integrator. The absolute value block estimates the output signal's amplitude. Other circuits (e.g., peak detector) may also be considered. The integrator locks the output amplitude on a predetermined value. This value is determined by the ratio of the resistors of the integrator. The gain of this integrator is determined by the multiplication of the feedback capacitor and the input resistor. This factor controls the speed of the loop and the ripple on the AGC's FET (the ripple is reduced by a LPF network after the integrator).

A tradeoff exists between the speed of the integrator and the signal distortion. When the gain is low, the FET receives a well-filtered signal that allows fine-tuning of the FET's resistance. When the gain is high, the output signal's final amplitude is reached quickly, but the signal will be distorted because of the fluctuations on the FET's gate. When Vgs/Vt is approximately 1, small fluctuations in Vgs result in large fluctuations in the FET's resistance. The ripple on the FET's gate is approximately 2 mV, based on a simulation.

Another tradeoff is between the time of settling and the final amplitude. The microcontroller prefers to have the largest amplitude possible (Vcc peak-to-peak). However, the integrator needs a spare of output amplitude in order to manufacture faster the error voltage for the FET. For now, the output signal is about a quarter (1/4) of the Vcc.

The constraints on the system include:

(1) low IC count

(2) low passive components count

(3) low current drain (< 2mA, not including the microcontroller)

(4) power supply is 4-6 volts, although the design works with 2-3 volts power supply with voltage multiplier circuitry

(5) low cost

(6) working temperature of 0-45 degrees Celsius

(7) robustness of design over device tolerances

(8) low noise level at the output

(9) input signal is tens of microvolts.

A more detailed view of the receiver in a two-way configuration is provided in FIGS. 18 and 19. FIG. 18 shows the analog front end and FIG. 19 shows the microcontroller unit. In FIG. 18, the power on switch block 198d provides for the batteries, where in this embodiment, two Varta batteries BT1 and BT2 are installed. These batteries provide power to the rest of the circuit via the switch SW1. The remainder of the circuitry provides for signal shaping and signal holding in a manner similar to the circuit of FIG. 9.

The transducer switch block 198a provides for both transmission and reception front end capabilities. The AnalogOn allows for the selection of input/output. The signal that should be transmitted is present on DigitalOut to pin 2 of the PI5A319A chip. If the transducer switch block 198a is in transmit mode, the signal is provided on pin 1 of the PI5A319A chip to the transducer pad TP1. If the transducer switch block 198a is in receive mode, the signal is provided to pin 1 of the PI5A319A chip from the transducer pad TP1. The received signal is then routed to pin 8 of the PI5A319A chip. The portion of the transducer switch block 198a that is associated with TP2 provides for noise immunity.

The received signal makes its way to the preamplifier and bandpass filter block 198b. After amplification and filtering, the received signal is provided to the high pass filter and AGC block 198c. The beginning portion of the circuit from resistor R2 to capacitor C7 provides for the divider function. The next portion of the circuit provides for the AGC function to generate the fixed amplitude. The bottom portion of the circuit provides for amplitude estimation. The processed signal is then provided to the microcontroller (e.g., Microchip PIC16F877 in a TQFP package) via AnalogIn.

The Vcc block 198e and Vref block 198f provide for the appropriate Vcc and Vref voltage sources that are used throughout the analog front end circuits. The additional circuitry 198g round out the analog front end.

FIG. 19 provides the pinouts and circuitry surrounding the digital core of the electronic card. The microcontroller/microprocessor 199a used in this embodiment is a Microchip PIC16F877 in a TQFP package. AnalogIn is the received signal to be processed. Conversely, DigitalOut is digital signal to be transmitted out of the card. The additional components like the connectors 199b and test point block 199c allow for programming and debugging of the microprocessor 199a.

Additional embodiments use different techniques for decoding the received signal in the electronic card. In one embodiment, a hardware phase-locked loop technique is employed. Referring to FIG. 40, transducer 400 receives the acoustic signal and makes the appropriate voltage conversions. The bandpass filter portion of unit 401 filters the signal in order to attenuate speech (or noise) signals. The preamplifier portion of unit 401 amplifies the signal to a minimum amplitude of a few milli-Volts. At this amplitude, most PLLs can lock onto the input signal. An AGC block 404 can be realized before the PLL 402 to increase the SNR.

In this embodiment, the PLL 402 is an XR215, XR2211, LMC568, or the like. The PLL 402 demodulates the audio signal as known to those ordinarily skilled in the art. The output of the PLL 402 can be a digital square wave of the decoded FSK signal. Alternatively, the output can be an analog voltage whose level is correlated to the input signal frequency. The microprocessor unit 403 accepts either of these forms of signals for further processing.

In another embodiment, software PLL/FLL decoding technique is employed to implement the locking of the input signal. Referring now to FIG. 41, the transducer 410 receives the acoustic signal and provides the necessary conversions. The bandpass filter portion of unit 411 filters the signal in order to attenuate speech (or noise) signals. The preamplifier portion of unit 411 amplifies the signal to a minimum amplitude of a few milli-Volts. The hard limiter block 412 produces a square wave from the analog output. The microprocessor unit 413 uses this digital input signal to implement the decoding. To increase the SNR, an AGC block 414, under the control of the microprocessor unit 413, can be realized before the hard limiter block 412.

In another embodiment, a mixer is used for baseband processing. Referring to FIG. 42, the components are similar to the above two embodiments corresponding to FIGS. 40 and 41 with the exception of a mixer 422. In this technique, the mixer 422 shifts the ultrasonic acoustic signal from around 20 kHz to baseband. Baseband processing is much easier to implement. An exemplary decoding method is squaring the analog output and processing the digital data. Another equally applicable method is conventional DSP algorithms for processing analog data.

3.5 CARD RECEPTION SOFTWARE

The goal of the receiver, whether hardware or software, is to detect and decode the FSK signal in real-time in a very simple processor with an erroneous clock. The receiver hardware received the acoustic signal, transduced it to an electrical signal, amplified it, and cleaned it before presenting it to the microcontroller. The receiver software in the microcontroller then processes the cleaned-up analog signal and attempts to decode it to extract the actual data therein.

The data stream transmitted by a base station (e.g., PC) comprises a header, data, a footer, and start/stop bits therein. The header, footer, and start/stop bits are fixed. The footer includes the checksum (CRC) byte. Referring to FIG. 5(B), the header includes an energy detector bit (1 bit) which includes contributions from two frequencies (sin(2*pi*f0*t) + sin(2*pi*f1*t)), a pure sinusoid with frequency (f0+f1)/2 (3 bits), a pure sinusoid with frequency f0 (3 bits), a pure sinusoid with frequency f1 (3 bits), and a known byte.

The data portion includes the actual data that the base station is trying to deliver to the card. This includes instructions, flags, and pure data for storage (e.g., coupons). The length of the data portion varies from one application to another.

Like the card-to-PC transmissions, start and stop bits are also used for this PC-to-card transmissions for resynchronization. The portion of the data stream from the known byte to the CRC byte is divided into bytes. Each byte is preceded by a start bit (logic 1) and appended by a stop bit (logic 0).

Referring to FIG. 12, the receiver downsamples the signal so that it could handle the otherwise large number of computations in real-time. This downsampling can be achieved in hardware with a bandpass filter

and an analog-to-digital (A/D) converter 120. For example, if the signals are between 18 kHz and 20 kHz, this portion of the spectrum can be prefiltered with the bandpass filter and then sampled at approximately 5 kHz (or 4900 Hz which is CD audio quality 44.1 kHz divided by downsampling factor 9). After the sampling, the signal will have moved to the 0-2 kHz band.

The energy detector 121 in the software then looks for a sharp rise in the signal energy. This energy detector 121 is used to determine whether an actual signal is present for processing. This can be accomplished by averaging the absolute power of the first bit (energy detector bit in FIG. 5(B)) of the received signal using a first order IIR filter of the form:

y[n] = a*abs(x[n])+(1-a)*y[n], where 0<a<1 and x[n] is the input signal

As mentioned previously, the signal comprising the energy detector bit is the addition of two sinusoids, where one sinusoid is at frequency f0 and the other sinusoid is at frequency f1. The reason why both FSK base frequencies are used is because there's a chance that one or the other frequency component will be DC after aliasing from the downsampling operation. If so, the high pass filter will remove it and the energy detector 121 will miss the beginning of the signal.

The receiver software samples one point. If the energy detector detects a high enough signal, then it's a signal. If not, the energy detector examines the next sample.

The next two blocks 122 and 123 correct for the card's clock errors. In contrast to the clock source in the card, the PC's clock source is more precise. Thus, the PC sends a constant and known frequency for the card to lock onto. The algorithm used by the card is a Least Mean Squared (LMS) on the following equation.

Any sine wave of the form x[n]=A*sin(2*pi*f0*n + phi) satisfies the difference equation:

x[n+1]*cos(2*pi*f0) = (x[n]+x[n+2])/2, for every n

Most notable about this difference equation is that it is second order, with at least one unknown parameter, b = cos(2*pi*f0), which can be interpreted as an unknown multiplicative constant. By defining an intermediate signal, b is determined by minimizing the mean squared error:

E{ (b *x[n] - s[n])^2 }

where E{} denotes statistical expectation. An LMS rule for determining the unknown coefficient b is given by the recursion

b[n+1] = b[n] - c*(b[n]*x[n]-s[n])

where c is a parameter that determines the rate of convergence ($0 < c < 2$), and the subtraction is used to implement the negative of the gradient (with respect to the parameter b) of the instantaneous cost C(b * x[n] - s[n]), as defined above. The frequency f0 can be estimated from b[n] by inverting the formula b[n] = cos(2*pi*f0[n]), most preferably in steady state (after convergence), and under the condition that -1 <= b[n] <= 1.

So, if the coefficent of x[n] is not known, an initial guess can be made and subsequently, the coefficient can be adaptively changed proportionally to the error as in any LMS algorithm. Here, the frequency adaptation bits are used. Referring briefly to FIG. 5(B), the 3 bits of (f1+f0)/2, the 3 bits of f1, and the 3 bits of f0 are used. For the first 3 adaptation bits, the average of f1 and f0 is used to minimize the risk that the correct frequency correction will be made. If only f1 or f0 is used, either f1 or f0 may flip over to the other side on the frequency spectrum during downsampling. When this happens, the receiver software will make a wrong correction of the frequency. By taking the average, the chance that the frequency will flip over is minimized and hence, the wrong correction will not be made.

After the frequency is adaptively selected in block 122, block 123 attempts to decode the first byte. If the decoding is bad, the receiver software returns to the A/D converter stage and starts over.

At block 124, the receiver software decodes the data to determine whether the received signal is a logic "1" or logic "0." Finally, block 125 checks for any errors using the checksum byte.

3.6 CARD MECHANICAL CONSTRUCTION

With respect to the mechanical construction of the electronic card, the electronic card complies with the credit card set of standards – ISO 7810, 7811-1 to 7811-6, 7813, 7816-1, and 7816-2. Some minor deviations from the standard are inevitable such as the location of the external switch and of course, the additional functionality provided by the card electronics. In other embodiments, no attempt is made to make the electronic card comply with the credit card standards. However, in the discussions below, the credit card standard-complying electronic card will be described.

The components in the card are miniaturized and placed on select locations in the card to optimize the use of such limited space. An external button is provided on the electronic card itself so that when it is pressed by the user, the electronic card encrypts the digital ID and transmits the encrypted digital ID via ultrasonic acoustic waves. The card also includes acoustic transduction elements, such as a microphone and a speaker, which serve as the acoustic antennae.

In a preferred embodiment of the invention, the card is thin (0.8 mm is a standard plastic card thickness), so the microphone should also be very thin. The acoustic receiver can be any microphone, such as a regular capsule microphone or an ultrasonic type microphone, which is possibly specific for a particular frequency or frequency range used. In some cases, special ultra-low power circuitry may be desirable. The acoustic transmitter can preferably generate a strong atmosphere wave. It is noted however, that only a small amount of power is required for short range transmissions.

The reception transducer is a capacitive microphone with two plates with a small air gap; that is, the distance between the two plates are small compared to conventional capacitive microphones. Any vibration on

the plate changes the capacitance which in turn changes the current to the reception circuitry. With a DC voltage applied across the plates, the resulting changing current signal is filtered, amplified, and then analyzed since the modulation of this signal is directly proportional to the information contained therein. The transmit transducer is a thin stainless steel/brass plate on a PCB with a piezo-ceramic material on top of it. The distance between the top surface of the piezo-ceramic material and the printed PVC layer is approximately 0.8 microns (micro-meters).

The electronic card's battery is small and is guaranteed to work in 0-60 degrees Celsius. Even if the electronic card is left inside a hot car, the battery will not be damaged. The battery also functions in temperatures down to –15 degrees Celsius. Up to 10,000 card activations (i.e., switch press) are possible for one embodiment of the present invention.

The electronic card is very robust to bending and has been designed to provide maximum bending protection. The electrical connection between the battery and the other components is soldered and subsequently covered with PVC, making the circuitry very resilient. Furthermore, components in the card have been placed in locations such that any bending of the card will not damage or otherwise impair the functionality of the electronic card.

With the current fabrication process, the electronic card can be laminated and embossed at 120 degrees for 10 minutes without damage to the card's circuitry or internal components. In other embodiments, the components, such as the transducer itself, are shielded so that hot lamination processes can be used.

The electronic card allows for conventional embossing in the area reserved for embossing cardholder information in compliance with ISO 7816. High pressure embossing is also possible in the card signature field since the electronic card does not have circuitry in this area.

Branding is also important for electronic card sponsors. The electronic card can be printed with any external features of the integrator's choice, including holograms and company logos.

3.6.1 SHEETS-LEVEL CARD FABRICATION

With current smart card fabrication techniques, the exposed nature of the smart card contacts complicates the assembly/lamination/printing process. Usually, assembly of the smart cards involves the manufacture of a plurality of smart cards in sheets. Each sheet is typically 7x12 cards (or 84 cards), although the exact dimensions of the matrix can vary depending on the type of smart card. However, for efficient and cost effective mass production, these smart cards are manufactured in large numbers to produce these sheets. Also, because these sheets contain smart cards, the smart card modules are exposed, which complicates the process. Also, sometime during this process of creating sheets, the individual smart cards are programmed. At some point, these sheets are cut into smart cards.

The current process for producing smart "bank" cards utilizes the conventional credit card fabrication more closely than that of the electronic card of the present invention. In fabricating smart cards, actual fully compliant "dumb" cards are produced in a credit card manufacturing operation. This includes the standard sheet printing/laminating/singulation processes. Once the "dumb" card is complete, it is further processed into a smart card. This is accomplished by machining a cavity into the body of the "dumb" credit cards and

implanting a smart card module into the body of the card. The subsequent personalization processes, therefore, do not represent a significant threat to the module.

During the lamination and printing stages, special machines (e.g., DataCard, Heidelberg) are needed to print the appropriate information (logos, numbers) around the exposed smart card modules. Heidleberg printing presses are used for the offset printing of the sheets, whereas the DataCard machines are for the personalization of individual cards, which can include thermal or dye sublimation printing. Without these special machines, the printing/lamination stage could potentially damage the exposed smart card modules and render the smart card useless. Also, special machines would also be needed to read and program the chips in the smart card. If additional personalization is needed (i.e., user name, user signature, user photo), these special machines would be needed again to print around the exposed modules as well as read and program the chips therein. Thus, the exposed modules in these smart cards complicate and otherwise makes costly the card fabrication process after the cards have been laid in sheets.

One embodiment of the present invention significantly improves this procedure. Not only do the electronic cards of the present invention contain "smarts," but these electronic cards do not expose the contacts or modules fabricated therein. The manufacturer programs these cards with the appropriate codes and IDs that are described throughout this patent specification. These cards are also laid out in sheets, where at some point, they are cut to produce the credit card-sized electronic cards. During the printing/lamination stage, standard credit card printing/lamination machines that are used on conventional United States-based "dumb" credit cards are utilized. No special machines are needed to print and laminate around the exposed smart card modules since the electronic cards of the present invention have no exposed modules. Also, since the electronic cards of the present invention have already been programmed, no additional machines are needed to read and program these cards. These cards are delivered directly to the user of the account.

To activate and personalize the card, the user would normally log into the card sponsor's website and press the button on the card. The website would process the data transmission and affiliate the card ID with the user's account. This is analogous to the user calling an 800 number to activate the card. In fact, the card can emit a signal usable over ordinary phone lines or cellular phones and thus, the cardholder's first activation of a card over that 800 number could also result in affiliating the card ID with the cardholder's account. Thus, the issuer need not worry about programming the electronic card since the affiliation of the electronic card with the user's account would occur at the backend after the user has activated the card by pressing the card button. The personalization of the card occurs upon the "first use" of the card in accordance with one embodiment of the present invention. In contrast, conventional technologies require some form of card-accepting device to be available and operational at the time of card registration or activation in order for personalization to occur.

Furthermore, according to the credit card standards, if smart card modules are exposed, the smart card must comply with the credit card standards organization's approved payment system. This involves additional components in the cards and additional programming to comply with the payment standard. By not exposing the modules in the electronic cards of the present invention, the manufacturer of these electronic cards need not

comply with this payment system standard. This allows the manufacturer to save on the cost of supplying, assembling, and programming the chips with the payment system standard-complying logic.

By preprogramming the electronic cards and not exposing any of the modules, the fabrication of these electronic cards provides efficiency improvements in fabrication (via the use of standard printing/lamination machines and no additional programming), cost (no additional logic needed to comply with payment system standard; no special machines needed to print/laminate around the exposed modules), and standards compliance (no separate payment system standard compliance issues). In essence, fabricating the electronic card of the present invention provides all the benefits of fabricating a standard credit card, in addition to the benefits described above.

3.6.2 COMPONENT LAYOUT

The component layout in the electronic card will now be discussed. Referring to FIG. 25(A), the substrate portion of the electronic card is shown. Here, the basic components and their placement in the substrate of the electronic card are illustrated. For the sake of clarity, trace conductors/interconnects are not shown; however, one ordinarily skilled in the art can determine the location and paths of trace lines based on the circuit diagrams described above.

Here, substrate 257 is shown superimposed on the outline of the final credit card form factor card 250. From this orientation, the magnetic stripe portion of a typical credit card is provided in region 258. On one side of the electronic card in this region is the magnetic stripe itself. On the other side of the electronic card in this region is the embossing area where credit card issuers normally place the name, social security number, expiration date, and other embossed information. On the same side is the logo of the credit card, and in some cases, the photo of the cardholder.

In this region 258, several components are also provided – switch 256 and transducers 254 and 255. The switch enables the electronics in the card to first transmit data in the electronic card and then followed by a short receive period. In other embodiments, of course, the single switch permits multiple modes where, for example, a single press indicates transmission and a double press indicates reception. In still other embodiments, multiple switches are provided on a single electronic card. Typically, the switch is a dome switch constructed of stainless steel material. A thin PVC layer also covers the switch. The switch is normally provided on the side opposite the printed PVC layer where the actual magnetic stripe is placed.

In this embodiment, two transducers are provided – one for transmit (e.g., speaker for acoustic signals) and the other for receive (e.g., microphone for acoustic signals). In other embodiments, only one transducer is used for both transmit and receive. Essentially, the transducer is piezo-ceramic disc on top of a small brass/steel plate. The entire structure is enclosed in a reverberation chamber. More details of this construction are provided below.

Outside of this magnetic stripe region 258, the battery 251, the chip and surface mount technology components 252, and electronic card connectors 253 are provided. In one embodiment, the battery is a Varta LPF-25. For smaller capacity, the battery is a Varta LPF-7. The chip and SMT components include the digital core (microprocessor and supporting circuits) as well as the analog front end.

Another embodiment of the component layout is shown in FIG. 25(B). Once again, the substrate 257 is shown superimposed on the outline of the electronic card 250. In this embodiment, two batteries 251a and 251b are provided. Part of the first battery 251a along with the chip/SMT 252 and the switch 256 are in the magnetic stripe region 258a. Outside of this region, the electronic card connectors 253, transducer 259 (which can provide both transmit and receive functions) and second battery 251b are provided.

In another embodiment, region 258b is the magnetic stripe area, instead of region 258a. In this embodiment, transducer 259 and part of the second battery 251b are placed in this region without affecting the magnetic stripe. Other components are outside this region 258b.

FIG. 25(C) shows a third embodiment of the component layout. In this embodiment, the switch 256 is the only component in the magnetic stripe region 258a. All other components including the two transducers 254, 255, the electronic card connectors 253, the digital core circuitry 252a, the analog front end circuitry 252b, and the battery 251 are placed outside this region 258a. Note that in this embodiment, the electronic card connectors 253 are placed below transducer 254. The magnetic stripe region 258a can also be used for embossing purposes.

In another embodiment, region 258b is used for the magnetic stripe. In this case, region 258a would be used for embossing.

As these three embodiments in FIGS. 25(A), 25(B), and 25(C) illustrate, the placement of the components in the electronic card is an important design criteria. Generally, the embossing area, which is also typically not the same area as the magnetic stripe region 258, should have as little components as possible. This allows embossing to be accomplished with relative ease while minimizing the concerns that credit card manufacturers may have on whether the embossing process might harm an electronic component. However, as components get smaller and smaller, the placement of some components (in whole or in part) should not affect the durability and reliability of the electronic card.

3.6.3 CARD LAYERS

The fabrication of the electronic card will now be discussed. FIG. 26 shows the various layers that make up the electronic card. At the heart of these layers is the substrate layer 260. This substrate layer includes a chip/SMT cavity 260a, battery cavity 260b, transducer cavity 260c, and switch cavity 260d, where the chip/SMT component 252, battery 251, transducer 254, and switch 256 are placed in these cavities, respectively. Some insulation material is used to cover the battery 251. Also, in some embodiments, the electronic card connectors (not shown in FIG. 26) are covered with PVC and other insulation material after the microprocessor in the electronic card has been programmed and debugged. In the portion of the substrate where silicon components are provided, some epoxy material is used to cover this area to prevent moisture from forming and to prevent this area from physically bending.

Surrounding the substrate layer 260 is the substrate "cap" layer 263 and the cavity layer 264. The substrate "cap" layer 263 is basically a very thin PCB where the underside (in the direction facing the substrate 260) has copper interconnects with special coating. The cavity layer 264 is a PVC material that is provided around the substrate 260 to artificially produce a fixed and constant height for the substrate 260 and its

components. Obviously, without the cavity layer 264, the placement of the various components in the substrate layer 260 results in different heights for the different regions of the substrate. This entire section which includes the substrate "cap" layer 263, the substrate layer 260 (with the components), and the cavity layer 264 are all filled with a material to fill in gaps to eventually even out the height of the entire section.

Above the substrate "cap" layer 263 is the printed PVC layer 262. The magnetic stripe is fabricated on this layer. Analogously, the other printed PVC layer 265 is provided below the cavity layer 264. The various images (e.g., credit card logo, bank logo), photos, and other information associated with credit cards are provided on this layer. Conversely, the magnetic stripe can be placed on printed PVC layer 265 and the other images and photos can be placed on PVC layer 262. A clear PVC outer layer 261, 266 are provided on the outer surface of each side of the electronic card.

3.6.4 TRANSDUCER CONSTRUCTION

The mechanical construction of the transducer will now be described with respect to FIGS. 27(A) to 27(C). FIG. 27(A) shows a cross-section of a circular transducer, like transducer 254 of FIG. 25(A), in accordance with one embodiment of the present invention. On the PCB 275, which is approximately 0.1 um (microns) in height of plastic, a brass/stainless steel plate 274 is provided. The brass/stainless steel plate 274 is approximately 0.1 um to 0.15 um in height. On top of the brass/stainless steel plate 274 is a small piezo-ceramic disc or element 273, which is approximately 0.15 um in height.

To provide some room for the vibration or movement of the piezo-ceramic element 273 to generate the acoustics, some space is provided around the piezo-ceramic element 273. Spaced apart from the piezo-ceramic element is the printed PVC layer 270. The distance from the top of the piezo-ceramic element 273 to the bottom of the printed PVC layer 270 is approximately 0.8 um. A wall 272 surrounds the piezo-ceramic element 273 and the brass/stainless steel plate 274 to create some enclosed chamber 271. The spacing of piezo-ceramic element 273 from the printed PVC layer 270 and the creation of a chamber 271 with the wall 272 also result in some form of a reverberation chamber for the acoustics. The acoustic signal is generally directed toward the PCB 275 (downward direction on FIG. 27(A)).

The resonant frequency of the acoustic signals generated by this transducer depends on the selection of the various parameters of the components in the transducer. The main parameters include the thickness of the piezo-ceramic element 273, and the thickness, stiffness, type of material, shape, and diameter of the brass/stainless steel plate 274.

FIG. 27(B) shows an alternative embodiment of the transducer construction. In this embodiment, the brass/stainless steel plate is not used. Instead, the piezo-ceramic element 273 rests on and uses the PCB layer 275 as a substitute plate. Additionally a portion of the printed PVC layer 270 protrudes into the chamber 271 so that the distance between the top of the piezo-ceramic element 273 and the bottom of the protruded printed PVC layer 270 remains at 0.8 um. In a variation of this embodiment, the piezo-ceramic element 273 can be made thicker so that the protruding portion of the printed PVC layer 270 would not be necessary. The additional thickness of the piezo-ceramic element 273 would be approximately 0.15 um (or the thickness of the

brass/stainless steel plate had such a plate been used). Thus, the distance between the top of the piezo-ceramic element 273 and the bottom of the unprotruding printed PVC layer 270 is 0.8 um.

The embodiments of FIGS. 27(A) and 27(B) show transducers which are fabricated as the entire electronic card is fabricated. In contrast, FIG. 27(C) shows a third embodiment of the transducer construction where the transducer is modular and not fabricated with the card. In this embodiment, the wall 276 also includes a cover portion 276a. The cover portion 276a and the wall 276 form the chamber or cavity 271. In one embodiment, the cover portion 276a and the wall 276 are made of either steel or plastic. In this configuration, the piezo-ceramic element 273 need not rely on the printed PVC layer to form the chamber. When this modular transducer is used in the fabrication process of the electronic card, other fabrication technology can be used. For example, the more widely available technique of hot lamination can be used in some of the fabrication steps. Without the modular transducer of FIG. 27(C), some components in the transducer cannot be heated too high without component failure.

4.0 BASE STATION

In one embodiment, the base station is a station that is part of a land-based infrastructure. Although it is usually part of some network, this is not a mandatory requirement. Thus, a personal computer, whether or not it is connected to a local area network or has access to the Internet, is a base station. Other exemplary base stations include televisions, radios, telephones, automated teller machines, card reader at the store checkout line, and the like. In one embodiment, the base station transmission software is similar to that of the electronic card.

In another embodiment, the base station is not necessarily part of the land-based infrastructure; rather, the base station can be portable. Thus, cellular phones, personal digital assistants (PDAs), portable radios, portable televisions, and the like can be base stations. Like the land-based base station, the electronic card in accordance with one embodiment of the present invention can communicate with the portable base station.

In either case, the frequencies for the acoustic signal are carefully selected to enable the electronic card to communicate with the base station. For example, if the base station is a personal computer with a sound system, the acoustic signals can be in the ultrasound range. If the base station is a telephone connected to the public telephone infrastructure, then the acoustic signals should be in the audible range so that they can pass through the filters effectively. Note that a single card can be equipped to emit either audible or ultrasonic transmissions as desired to send to a telephone, a computer, or other digital devices as needed. In another embodiment, the audible frequencies selected conform to the standard DTMF scheme.

4.1 CLIENT COMPUTER SYSTEM

Referring briefly to FIG. 1, in the client computer system 14, a special client remote access software in accordance with one embodiment of the present invention is installed and running. In addition, a standard microphone, speaker(s), and a web browser are utilized. Of course, a web browser is not absolutely essential so long as the computer system allows the user to access the Internet. This can be accomplished with a piece of communications software. At the web merchant or web portal side, a server is provided to handle the user's redemption needs. Thus, having downloaded the coupon from a TV 12 or radio 11, the user can take his card

to his computer 14, access the Internet 16, and redeem his coupon at the sponsoring web merchant's or web portal's website.

Referring now to FIG. 11, the client computer system will now be described. The client computer system includes a web browser (e.g., Microsoft Internet Explorer, Netscape Navigator) 115, a special client remote access software 114, at least one speaker 111, a microphone 112, and drivers 113 for the sound device(s) (e.g., speaker/microphone). The sound card and corresponding sound card software normally interfaces with the speaker and microphone. Most computers currently on sale include a sound system, usually a "Sound Blaster" sound card, connected to at least one microphone and at least one speaker.

Note that the sound devices that are necessary depend on the particular application of the electronic card. If the electronic card is one-way transmission only, only the microphone is needed in the computer system. If the electronic card is two-way, both the speaker and the microphone would be needed. If the electronic card is one-way receive only, then the speaker would be needed in the computer system.

In a preferred embodiment of the invention, client computer system 110 and electronic card 10 communicate using these standard computer components of client computer system 110, which are usually for human communication, not for computer communication. Some computers are provided with other types of sound systems, which also support the application of preferred embodiments of the invention, possibly with a variation in frequencies to account for different circuit or sampling characteristics. Typically, this sound system is designed for generating music and other audible sounds. In addition, many computers include an internal speaker and a modem speaker. Some computers use USB speakers which are connected directly to the USB (Universal Serial Bus).

In one preferred embodiment of the invention, a standard sound card, such as the popular "Sound-Blaster" is used to generate sonic and/or ultrasonic signals to (and to alternatively or additionally receive them from) an electronic card. The acoustic signal may be audible (in some applications) or inaudible (more preferable), for example having mainly ultrasonic or infrasonic frequencies. Preferably, frequencies of about 22 kHz and 24 kHz and 32 kHz are used, since a standard sound card provides these sampling rates (and/or their multiples, e.g., 44 kHz and 48kHz). Alternatively, lower frequencies, such as between 17 kHz and 21 kHz may be used. In other embodiments, the standard sound card receives sound waves from the electronic card 10 (see FIG. 1) for further processing.

In some preferred embodiments of the invention, a sound card is adapted to work in the near ultrasonic range, for example by increasing its sampling frequency. Generally, the microphone and loudspeaker used for a computer system can support low frequency ultrasound with sufficient fidelity without adaptation. However, in some embodiments of the invention, a special ultrasound-sensitive microphone or ultrasound-effective speaker may be used. In other cases, the sensitivity of a particular microphone and/or loudspeaker maybe determined by the user prior to or during communication with an electronic card.

To provide for software control of the speaker 111 and the microphone 112, the client computer system 110 includes drivers 113. Normally, the user can set playback volume and recording volume on the software control panel which are then set in hardware by the drivers.

A special client remote access software 114 is provided to interface with the speaker/microphone drivers 113 via communication line 116 and the web browser 115 (or communications application) via line 117. The special client remote access software 114 was written specifically for the various embodiments of the present invention. This software 114 is installed in the client computer system 110 and is normally loaded at all times because the user may use his electronic card 10 at any time. Of course, if the special client remote access software 114 is not loaded, the user simply opens the application whenever he is operating the card.

The special client remote access software 114 performs multiple tasks that are important to the various embodiments of the present invention. During the initial stages of the user's on-line purchase, the special client remote access software 114 processes the sound waves corresponding to the digital ID that have been emitted by the electronic card 10. After having been received by the microphone and processed by the sound card, the sound waves are processed further. The special client remote access software 114 checks the encrypted digital ID sound waves to make sure that the data is complete and corresponds to the appropriate user's electronic card 10. Thereafter, the received data is processed by special client remote access software 114 in different ways depending on the application.

4.2 INSTALLATION AND INITIALIZATION

As mentioned above, the special client remote access software 114 in the user's PC is needed to communicate with the electronic card and the web browser. At times, the special client remote access software 114 can access the Internet and communicate with web servers without the web browser. The installation of the special client remote access software 114 can be accomplished in many different ways. The installation may occur over the web as the software is downloaded from a web server and then subsequently installed in the user's PC. Alternatively, the software can be installed via CD-ROM or floppy disk. Furthermore, when the user buys a computer, the software may be bundled with the computer equipment so that installation is automatic.

In communicating with the web browser, the special client remote access software 114 uses Java applets. When the special software 114 needs to interact with a web page, the Java applet calls the appropriate ActiveX controls to perform basic functions associated with that web page. The deployment of ActiveX by the special software 114 is routine and is known to those ordinarily skilled in the art. In this manner, some aspects of the special client remote access software are found in various servers that can be downloaded to the local client as they are needed. The basic special client remote access software 114 however, is installed locally. Thus, as the user navigates from one webpage to another, different functions may be supported. As the user encounters these webpages, the user can download these different functions to extend the capabilities of his electronic card.

For example, assume that a user has encountered a shopping website. The shopping website requires some authentication to log in. The website indicates that it supports the electronic card. The user then downloads the authentication logic from this website's server. Once downloaded, the user can then press his electronic card to authenticate himself into the website and access his account. When he reaches the checkout line, he downloads the form fill logic from that website's server. When he presses the button on his electronic

card, the just recently downloaded form fill logic portion of the special client software recognizes the electronic card transmission as requesting a form fill. The special client software then fills out the form on that webpage to assist the user. Other functions can be supported in this manner. Thus, as the user navigates from one webpage to another, he can encounter webpages that support different electronic card functions. If desired, the user can download those functions to extend the usefulness of the electronic card at that website.

In other embodiments, the special client software does not need the web browser to communicate on the web. After all, the special client software can contain all functionality that is in the web browser in addition to the functions needed to communicate with the electronic card. In a further embodiment, the special client software is not needed as the web browser provides all the functions that the user will need. A Java applet downloaded via a Java VM can perform all the specialized electronic card-related tasks, while the web browser itself allows the user to communicate on the web.

Initialization primarily involves the sound system and its supporting equipment. Two main tasks are executed – (1) mixer settings, and (2) sound card memory allocation. When the special client software is launched or otherwise turned on, it initially stores the default mixer settings so that later, it can return the PC to the state before the special client software was activated. The special client software then checks and adjusts the mixer control settings so that the sound card is optimized to interact with the electronic card.

First, the recording setting must be on. If it is off, the special client software turns on the recording setting. In other embodiments, the special client software asks the user to turn on the recording setting.

The special client software then performs several tests, with and without the assistance of the user. These tests involve testing the speaker, the microphone, and the electronic card-PC communication, as detailed below. These tests need not be performed every time, though.

The special client software also checks the microphone. If the microphone is off, then the special client software enables the microphone to be turned on. Alternatively, the special client software may ask the user to turn on the microphone. The special client software may also ask the user to test the microphone by speaking into the microphone. Various threshold settings are stored – (1) silent mic, (2) non-receiving mic, and (3) receiving mic. Alternatively (or additionally), the special client software may ask the user to operate the electronic card. If the test fails, the special client software will ask the user to fix the electronic card by providing various tips, such as proper press of switch, proper distance of electronic card to microphone, proper orientation of the electronic card to the microphone, and the like.

Additionally, to avoid feedback problems, the special client software turns off the playback control. For those sound blasters with AGC, the special client software will turn on the AGC setting when appropriate, as well as other special settings (e.g., boost).

The special client software takes control of the volume control slider and moves it all the way up to maximum. In some cases, however, audio clipping may be a problem due to the presence of ambient noise. If so, the special client software may move down the volume control slider and then subsequently alert the user to retransmit the data from the electronic card. In one embodiment, a test may be performed with a sample audio file. During the initialization phase, the special client software asks the user to transmit a sample data. By

pressing the TX switch in the electronic card, a sample audio file is transmitted. Based on the reception quality of this sample audio file, the special client software adjusts the volume control setting that allows proper recording while minimizing the negative influence of ambient noise.

For the sound card memory allocation, the special client software sends a request to the sound card driver in the PC to allocate memory. The memory has to be substantial enough to hold the audio data. In a typical sound card, 8 MB are available in the buffer. Usually, not all of this memory is needed. However, in some applications, many seconds of audio need to be recorded. As an exemplary number for the amount of memory used, approximately 1 MB is needed to record 10 seconds of audio.

In one embodiment of the sound card, assume that the special client software needs about 1 MB of memory to record 9-10 total seconds of audio. The sound card driver divides the 1 MB of memory into 36 buffers, where each buffer holds approximately 250 ms of audio data. When any buffer is filled, the sound card driver sends the audio data in that buffer to the special client software.

For two-way embodiments, a test with a sample .wav file is done to determine whether the electronic card can receive data properly. The special client software includes a sample audio .wav file. After the memory is allocated by the sound card, the sound card driver sends a pointer to a buffer location. The special client software then sends the sample .wav file to the buffer location specified by the pointer. The sound card then plays the .wav file through its speaker(s) while the electronic card receives this audio sample. If the expected audio sample is received and properly decoded in the electronic card, then the electronic card generates an audible beep to indicate that the test was successful.

Typically, these initialization settings are made upon launch of the special client software. When the electronic card transmits the data to the PC, the special client software processes this data. After processing this data, one embodiment returns the PC back to the initialization state where it waits for additional data transmissions from the electronic card. Thus, the special client software is active (usually as a tray application on the desktop) and the sound card is optimized for electronic card-to-PC communications until the application is closed.

In another embodiment, however, the special client software restores the default mixer settings. As mentioned above, the special client software stored the mixer control settings prior to adjusting them for the electronic card. If the user needs to use the electronic card again, he enables the initialization routine to start over again for the mixer control settings and the sound card memory allocation.

4.3 BASE STATION TRANSMISSION SOFTWARE

The primary purpose of the base station transmission software is to generate the data stream shown in FIG. 5(B). The data portion of the data stream can be instructions, flags, and pure data for storage (e.g., coupons). For the most part, if sound is utilized, a conventional audio file (e.g., .wav file) is played by a software audio player as is known in the art.

In some cases, the data is transmitted from a computer system via the speakers. The special client software packages the data to be transmitted, whether the data is locally available or downloaded remotely from a website, and transmits them. The transmission involves the playing of the audio .wav file. Thus, the

packaging of the data to be transmitted can be as simple as locating the relevant audio file in memory and playing that audio file via the speakers.

In other cases, the data is transmitted from a TV or radio set. Today's television sets and radios are fairly passive and dumb devices; that is, they merely broadcast what they have received from the conventional TV/radio stations or the cable infrastructure. Accordingly, the transmission software is installed in the location where the coupon data is mixed with the programming. This may be the headend or even the network program source in the cable infrastructure. Once mixed, the coupon data (whether audible or ultrasonic) and the regular TV/radio program travel through the normal channels to the user's TV or radio set. Thereafter, if the TV or radio set is on, it transmits the data stream of FIG. 5(B) via acoustic waves, where the coupon data is found in the data portion of the data stream.

4.4 BASE STATION RECEPTION SOFTWARE

When any sound is emitted by some sound source, whether or not the sound source is the smart card of the present invention, the microphone on the computer (computer 14 of FIG. 1) may pick up that sound. If the sound complies with the data stream format of FIG. 5(A), the special client software 114 (FIG. 11) can process it and extract the data therein. If, however, the sound is unrecognizable (or is otherwise noise) to the special client software 114, it ignores it. Generally, the special client remote access software 114 in the PC receives a signal, determines whether the signal is proper, and if so, performs digital signal processing on the signal and decodes it. Based on the decoded signal, the special client software 114 can perform many functions such as open a web browser to a specific web page, fill out a form, redeem a coupon, and otherwise automate previously manual operations.

In one embodiment, the base station is a personal computer that is connected to the Internet. FIG. 13 shows a flow chart of one embodiment of the reception software portion of the special client software 114 (FIG. 11). In FIG. 13, the process begins at step 130. At step 131, the software initializes the sound device (e.g., "Sound Blaster" sound card) and optimizes the mixer settings. Here, the software allocates enough memory in the sound device to properly receive all the data. In one embodiment, it allocates 1 MB of memory, which allows for approximately 10 seconds of sound. It also checks to make sure the microphone is on (if it's off). The recording volume is initially set at the highest level. In some cases, however, if the recording volume is too high, signals will overflow the system and data may be lost. In other words, clipping may occur because of ambient noise. In this case, the software will readjust the recording volume slider to suitable levels. If the recording volume is too low, weak signals may not be detected. To avoid feedback, the playback mic control is turned off. In some sound devices, an automatic gain control (AGC) feature is provided. In this case, the software turns on the AGC.

After the initialization step, the PC is in a "waiting for signal" state at step 132. As mentioned before, in accordance with one embodiment of the present invention, the signal is in the form of a Frequency Shift Keying (FSK) signal. At step 133, the software performs the detection operation. The detection of the FSK signal involves two distinct operations – multi-rate processing and signal detection. In multi-rate processing, the signal from the A/D converter (from the sound device) is high pass filtered and downsampled while

preserving the range of frequencies in which the received signal is assumed to occupy. This stage is used to restrict the attention of the detector to a narrow band of frequencies in which the received signal may or may not be present.

The problem of detection is to determine whether a transmitted signal is present in a background noise environment. Assuming noise is gausian in nature, one technique is to correlate the received signal with the specific expected wave. The output of the correlator Z[n], can then be compared against a threshold to decide if signal is present. The test is

$$Z[n] = \sum_{m=0}^{\infty} h_{mf}[m]y[n-m] \underset{<H0}{\overset{>H1}{\gtrless}} \eta$$

y[n] is the received signal. $h_{mf}[n]$ is a matched filter (usually a sinusoid for FSK transmission). H1 is the alternate hypothesis (signal present), and H0 is the null hypothesis(no signal present). The test threshold η is a value determined to minimize the probability of false alarm, while maximizing the probability of detection. This maximization is determined directly from the distribution of the test statistic Z[n].

In practice, the frequencies and amplitudes of the FSK signals are not known a priori, with the result that a band of frequencies, corresponding to that band of frequencies defined by the range of error from the transmitting card, are scanned using Discrete Fourier Transform (DFT) banks and then subjected to Generalized Likelihood Ratio Tests (GLRTs), to establish the presence or absence of a signal given. A GLRT is used since the amplitude of the transmitted signal is unknown, and so is the estimated parameter in the test. The noise thresholds for the tests are generated from a delayed window of "noise only" data, where the decision "noise only" was made by the detector at an earlier time, or from the start-up default condition, where the noise statistics are estimated. Subsequent to statistical testing, the received signal is further established as valid if it contains the proper data format (see FIG. 5(A)) and spacing between frequencies f0 and f1.

Once the signal has been detected at step 133, step 134 decodes the signal. The decoding procedure considers each of the two FSK channels separately to draw conclusions about the transmitted data. Referring briefly to FIG. 14, the input detected signal is provided to two short term correlators – frequency f1 correlator 140 and frequency f0 correlator 141. Again, the notion of a test statistic is used, where the test statistics are generated by the two correlators. The hypothesis testing in this case is that between the alternate hypothesis (Signal present, power A0 in correlator 140 or A1 in correlator 141), and the null hypothesis (No signal present, power level E0 in correlator 140 or E1 for correlator 141). The testing between the two hypotheses in each channel can thus be understood to establish the received signal variance as being either A1 (or A0) over E1 (or E0) in correlator 140 (or 141) given a Gaussian distribution for each hypothesis and an equal probability that the received bit is a one or zero, that is, for correlator 140, the following test is used:

$$\frac{p\left(r/\sigma_{r/H_1}{}^2 = A1\right)}{p\left(r/\sigma_{r/H_0}{}^2 = E1\right)} \underset{<H_0}{\overset{>H_1}{\gtrless}} 1$$

This two-pronged approach for making bit decisions is necessary since the received FSK signal may be subject to echoes, a phenomenon that affects each channel differently. The advantage of making two decisions, one for each channel, as opposed to a single decision, based on a test statistic generated from testing the likelihood of one frequency (channel) over the other, is that when both channels disagree on the value of the received bit, one can use the ratios A1/E1 and A0/E0, as a means for favoring the decision of one channel over the other. That is, if one channel has a stronger echo, it is less reliable. It is also important to note that the quantities A0, A1, E0, and E1 are all time varying quantities, owing to the fact that card movement, even slight movement, can give rise to noticeable changes in echo and signal levels. As a result, these quantities must be tracked throughout the transmission. It should be clear that if the bit rate is Fb = 1/Tb, then the above procedure is performed exactly once every Tb seconds, where the optimal timing, that is, the point at which to sample in an interval Tb, is determined during synchronization and resynchronization.

The output of correlator 140 is provided to threshold 144, where the threshold is determined from the log-likelihood ratio test between zero mean Gaussian distributions having variances A1 or E1, under the alternate and null hypotheses, respectively. If the signal is greater than this threshold, then block 146 makes a decision that the signal is a logic "1" and updates A1 based on the the current output power from correlator 140, and using some averaging with the current value of A1. If the signal is less than this threshold, a "0" is established, and the value of E1 is updated based on the current output power from the correlator (140) and the current value of E1. Similarly, the output of correlator 141 is provided to threshold 145. If the signal is greater than the threshold determined from the likelihood ratio test that decides between the alternate hypothesis (variance = A0) and the null hypothesis (variance = E0), then block 146 makes a decision that the signal is a logic "0" and A0 is updated based on a weighted average between the current output from the f0 correlator (141) and the current value of A0. If the signal is not greater than this threshold, then a logic "1" is decided and E0 is updated. The signal is then provided to block 146 for the decision. Under most circumstances, we expect that the two LRTs (144 and 145) will make the same decision, agreeing that a "1" or "0" was received for a given symbol interval. In cases where the two disagree, then if this is due to echoes, we can establish the best decision based on that channel having less echoing, which is determined from the ratio E0/ A0 or E1/ A1. This final level of decision making is performed at step 146.

To summarize the decoding operation, each of the two channels is processed separately, with a threshold being both tested against and updated from the current observation. In the case where both channels make the same decision, a secondary test is provided which takes into account the signals when the channels are inactive.

Returning to FIG. 13, the decoded data is then stored and processed based on the application at step 135. The application may be simple form filling on a web page after the user purchases some merchandise. The application may be the automatic launching of the user's web browser and navigation to a particular home page. Also, the application may be the delivery of the data to a web site for processing at the server, such as when coupons are redeemed. The process ends at step 136. Normally, the special client software is always turned on in the background (i.e., application could be placed in the Windows "tray").

The detection operation will now be discussed in greater detail. One of the keys to implementing a recursive DFT rests on preserving the property of orthogonality between the frequencies in the DFT and ignoring the choice of phase, which itself is arbitrary. Phase is only significant in a relative sense; that is, phase exists between the frequency components in the received signal. If desired, this phase can be discerned in a recursive DFT scheme with a few additional operations. Accordingly, this allows for the extensions of this scheme to Phase Shift Keying (PSK) and Quarternary Phase Shift Keying (QPSK), as well as the generalizations of these procedures.

Referring now to FIG. 15, a portion of the digital signal processing scheme is shown. Several DFT banks 150 are provided to perform the DFT operation on the received signal y(t). The DFT banks are necessary because of the inherent inaccuracy (i.e., due to small clock error) of the smart card in generating the FSK signals. If one knew the FSK frequencies (e.g., f0 and f1), then the entire detection process would be one of correlating along f1 and f0 and searching for a particular pattern or bit stream on which to synchronize using some type of statistical test as a criterion for acceptance. Because of the lack of a precise knowledge of the transmitted frequencies, the data format of the smart card includes a preamble. Referring briefly to FIG. 5(A), the preamble includes the two frequencies f0 and f1, where these two transmission intervals are sufficiently long to estimate each of the two FSK frequencies precisely. The known bit pattern is then used for synchronization. The reception software in the computer identifies the correctness of the received frequencies by their spacing (f1-f0), durations, and energy relative to the ambient noise level.

Since the smart card's clock error is consistent, identifying one variable leads to the simple calculation of the other variables; that is, the variables f1, f0, and T (symbol duration) have one degree of freedom which is the specific clock error in the smart card.. Thus, assuming that the duration of each frequency is sufficiently long, and that the energy over the given interval exceeds the threshold specified by the GLRT, then the symbol interval T can be recovered from the F1 and F0 intervals, as depicted in FIG. 5(A). With the symbol interval in hand, synchronization can be performed by using the delay line 152 in FIG. 15 along each of the corresponding frequencies f1,f0, according to their respective indices in the DFT bank 150, and with the aid of the known bit stream FIG. 5(A).

After the highpass filtering and downsampling, the frequencies of interest are located in the narrow band of 0-2kHz. The bit rate for the signal in this system is 200 bps in one embodiment, which is a symbol period of 5 msec long (T_{symbol}=1/200 bps). The downsampled rate is approximately 5 kHz (4.9=44.1 kHz/9, where 44.1 kHz represents the sampling rate of the sound card in the PC and 9 represents the downsampling factor). At this downsampled rate, approximately 25 samples are taken in one period (5 msec) of the received signal.

For practical purposes, the 0-2kHz narrow band is divided into 13 (which is approximately 25/2) bands to assist the software in determining the actual frequency of the received signal. Accordingly, the DFT banks 150 include 13 separate banks, where each bank is focused on one of these narrow bands. In effect, each bank or bank channel determines how much of the received signal is directed along the frequency the bank channel is

associated with; that is, how much the given bank channel frequency (e.g., w_0) contributes to the received signal.

Because the bit rate for the system is 200 bps in one embodiment, the DFT window in the DFT banks is 5 msec long (T_{symbol}=1/200 bps). Referring briefly to FIG. 16, the DFT window 167 is 5 msec long. Within the DFT window 167 are several sampled points, such as samples 160, 161, 162, 163, and 164, although in FIG. 16, each DFT window is not associated with 25 sampled points for the sake of clarity in the illustration. The 25 points in DFT window 168 are used to generate the 13 DFT coefficients for the particular embodiment as specified by the 44.1kHz sampling rate, 200 bit per second transmission, and downsampling factor of 9. Since the signal being analyzed is real, the spectrum has conjugate symmetry, and it is therefore sufficient to analyze only half of the signal's total bandwidth. Having the DFT in window 167, we can proceed to compute the DFT in window 168 recursively in the following manner.

Fundamentally, recursively computing the DFT comprises the moving correlation between a given complex exponential $e^{jk\omega_0 n}$ with the received signal x[n]. This quantity is denoted by $\hat{a}_k[n]$ such that:

$$\hat{a}_k(n) = \frac{\sum_{m=n-N+1}^{n} e^{jk\omega_0 m} x[m]}{N}$$

Defining the intermediate variable $\hat{x}[n]$ such that $\hat{x}[n] = e^{jk\omega_0 n} x[n]$, the quantity $\hat{a}_k[n]$ is a moving average of the quantity $\hat{x}[n]$, and hence can be written in the form:

$$\hat{a}_k[n+1] = \hat{a}_k[n] + \frac{\hat{x}[n+1] - \hat{x}[n-N+1]}{N}$$

Note the change in lower bound from N to N+1, as in the lower bound on the sum defining ak[n], which is termed the sliding DFT coefficient. Note that the difference

$$\hat{x}[n+1] - \hat{x}[n-N+1] = x[n+1]e^{j\frac{2\pi k(n+1)}{N}} - x[n+1-N]e^{j\frac{2\pi k(n+1-N)}{N}}$$
$$= (x[n+1] - x[n+1-N])e^{j\frac{2\pi k(n+1)}{N}}$$

so that the DFT coefficient $a_k[n+1]$ is simply updated from $a_k[n]$ by generating the difference between the newest and oldest samples, and adding to the real part of $a_k[n]$ this difference times the cosine of 2π k/N.

Similarly, the imaginary part of $a_k[n]$ is updated by adding the product between the difference (x[n+1]-x[n+1-N]), scaled by the reciprocal of the window length N, and the sine of 2π k/N.

With this recursive formulation, the kth DFT coefficient $a_k[168]$ for DFT window 168 can be computed from the kth DFT coefficient $a_k[167]$ from DFT window 167 by determining the difference between sample 165 and sample 160, and updating the real part of $a_k[167]$ with this difference times the cosine of 2π k*168/N, and similarly updating the imaginary part of $a_k[167]$ by multiplying the difference between sample 165 and sample 160 with the sine of 2π k*168/N.

Another recursive form for DFT is given by expressing the DFT window as the impulse response

$$h_k[n] = \sum_{m=0}^{N-1} e^{j2\pi \frac{k(N-1-m)}{N}} \delta(n-m)$$

This representation has z-transform

$$H(z) = \sum_{m=0}^{N-1} e^{j2\pi \frac{k(N-1-m)}{N}} z^{-m}$$

$$= e^{-j2\pi \frac{k}{N}} \frac{1-z^{-N}}{1-e^{-j2\pi \frac{k}{N}} z^{-1}}$$

which yields the recursion formula

$$a_k[n] = e^{-j2\pi k/N}(a_k[n-1] + x[n] - x[n-N])$$

Note that this recursion formula requires twice as many operations as the first recursion.

Returning to FIG. 15, the output of the DFT banks 150 is a block 151 that calculates the magnitude of the received signals for each channel. These values are then provided to delay lines 152, which is slightly longer than the data stream by a factor of 3/2. The delay lines store the values output from the magnitude block 151.

Concurrently, an additional delay line 153 is provided. This delay line takes in input y(t) to make a calculation of the noise variance. The noise variance is actually calculated in the Auto-Regressive block 154. The delay through 153 of FIG. 15 is sufficiently long so that the variance estimated at the output of 153 in the AR block 154 is from a period of time considerably earlier than the data in the correlator bank 150 of FIG. 15 and the delay lines 152 of FIG. 15. This means that since the detector is currently searching for a signal, that

earlier period whose power is evaluated in 154 of FIG. 15 must be a period deemed 'noise only.' Hence, the statistics so computed are enough to specify the threshold η of the Neyman-Pearson test on Z[n], described earlier.

The bank channels having maximum energy are then found in the delay line 152, according to the F1-F0 format described in FIG. 5(A). Since the sequence F1-F0 is transmitted first, these signal are the oldest in the delay lines, or the furthest back in 152 in the direction of the arrows. These selected bank channels are then compared to the calculated noise threshold to decide whether they are signal or noise, and also to each other to make sure that the proper frequency separation is present. Once these tests are passed, the detector has now determined the two bank channels that correspond to f0 and f1, or certainly close enough for decoding purposes.

Once the f0 and f1 frequencies have been determined with the f0 and f1 signals, the detector can now focus on synchronization. For the synchronization bits, the detector is programmed to know the particular pattern. If the pattern is 01010101, then the detector starts at a column in the delay lines 152 of FIG. 15 (where the frequency index denotes a row in the delay line 152) that corresponds to the point immediately after the location of the frequency identification intervals, F0 and F1, and alternately sums the values from the two selected banks, corresponding to f0 and f1, in step sizes of T, corresponding to the estimated symbol interval as estimated from F0 and F1. For example, the detector starts with the first bit, "0", which is the first symbol received, and so is the oldest on the delay line. The detector takes the value from the selected bank channel assumed to correspond to f0. The detector then proceeds to the next bit, "1", with location offset from the point previously taken from f0 by T samples and in the direction of the most recent sample, or towards the DFT bank, and adds this value from the f1 bank to the previous value. The detector continues with this 01010101 pattern until it has summed, for each value in the bit stream, the corresponding channel magnitude, with each such element separated from the previous by symbol interval T. Since this sum is a function of the offset from zero time, where zero time denotes the point where the energy in the first synchronization bit exceeds that in the last frequency identification bit, as in FIG. 5(A), we construct a cost function C[m], where m denotes the offset in samples from the zero time, and we define this first sum as C[0]. We write

$$C[n] = \sum_{m=0}^{M} b[m] f1[D - n - mT] + (1 - b[m]) * f0[D - n - mT]$$

where b[n] is the known preamble sequence, D is the offset from the output of the Magnitude device 151 to the zero time in 152, f1 is the delay line associated with frequency f1, and similarly for f0. Note that the sum moves from the oldest recordings of the 151 ouput towards the newest, in agreement with our understanding that the first bit transmitted will be the oldest recorded.

The detector now evaluates the sum C[1], which determines the sum of the delayed f0 and f1 correlator outputs offset by 1 sample from the previous sum, with the offset in the direction of the most recent sample, or in the direction of the DFT banks (opposite the direction of the arrows in FIG. 15). As before, the cost function C[1] is generated by alternately summing the magnitudes stored in the delay lines 152 of FIG. 15, spaced apart

by T samples, with the choice of frequency index f0 or f1 in the delay line 152 given by the corresponding value of the bit in the known bit sequence "0101010101".The detector now evaluates C[2], C[3], etc.. until it has evaluated at least T points, which is sufficiently long to determine a synchronization point.. When all the elements of C[m] are then compared to each other, one of the points is the maximum; that is, when these sums are plotted, the plot forms an upside down V pattern. The sum corresponding to the peak of this upside down V pattern is the synchronization point. From this synchronization point, one can in turn evaluate A0, A1, E0, and E1, which are the powers in each channel for one or the other of the two frequencies transmitted. Knowing the synchronization point on the received synchronization pattern, these quantities are directly calculated by taking advantage of the known (synchronization) data sequence.

The final issue to address is resynchronization, which bears sharp resemblance to synchronization. Based on the timing synchronization point K established from the maximum of C[m], the decoder will sample every T samples at points K+nT until the decoder reaches the 'stop' bit framing a given received byte. Since the "start" and "stop" bits are known, these bits are used to resynchronize much in the same way as the known synchronization sequence assisted in establishing the synchronization point K. In this case, however, rather than having many bits, there are only two, but conceptually the process is the same. A cost function is constructed from a point corresponding to the middle of the coming "start" bit. In this way, knowing that we are probably not off by much in terms of synchronization loss, we can sum the magnitude of the delayed "stop" bit with the current "start" bit, generate a cost function C'[m], and use the maximum as the new synchronization point K'. In some applications, an AGC can be introduced to the DECODING stage at a point prior to the f0 and f1 correlators to ensure that the resynchronization cost C'[m] always has the correct maximum by correcting the received signal in the presence of fading or weak signals.

In another realization, one can replace the auto-regressive noise power estimator 154 of FIG. 15 with a bank of autoregressive (AR) estimators which separately track the power in each of the frequencies analyzed by the bank 150 of FIG. 15. In this case, the delay line 153 of FIG. 15 can be removed, and the input to the bank of AR power estimators can be placed at the end of 152 of FIG. 15, after the delay line length of 152 is extended from L to accommodate the time required for the preamble duration and the time for the AR buffers in the new frequency - power estimation unit to fill with noise.

Interference Suppression:

The utility of estimating the noise power as a function of frequency, which is called the periodogram estimate, is particularly useful in the case where the background noise environment is colored. Classically, detection in the presence of colored noise amounts to preceding the detection mechanism with a prewhitening filter. When detecting frequencies, however, a whitening filter would translate to an increased threshold for those frequencies where the noise power is higher, and a reduced threshold at those frequencies with little noise power. This is in fact exactly how the spectrogram is used – thresholds are set at a frequency by frequency basis, where out of band interference can then be ignored. The cumulative effect of the periodogram estimate is then simply to replace the previous estimate of the threshold, for a given frequency, with the corresponding periodogram noise estimate for that frequency.

The advantages of this digital signal processing scheme are primarily threefold:

(1) The received signal may have a low signal-to-noise ratio since the DFT bank used for detection is essentially a bank of narrowband filters, improving the SNR per channel as compared with simple energy tests on the received signal. This is particularly important since the acoustic signals that are detected have very low amplitudes.

(2) The detector is practical to implement because of the application of the moving average concept to the DFT banks.

(3) The accuracy of the detector is close to optimal. The detector is a true matched filter.

In another embodiment, n-ary phase shift keying (nPSK) technique is used to decode the signals instead of FSK. In this scheme, the delay lines or channels at the output of the DFT bank, select one of the channels based on magnitude. Having selected the best bank, estimate the phase shift by processing the I-phase component and the Q-phase component of this bank. The offset determines whether the transmitted data is a "1" or "0".

4.5 CONCURRENT OPERATION OF MULTIPLE RECORDING SOFTWARE

In some computer systems, the operating system does not allow more than one recording software to operate at any given time. One such group of operating systems is Windows 95/98/NT/2000. If Windows allocates resources in the sound card for a particular commercial recording software, the special client software 114 (in FIG. 11) in accordance of the present invention may not work properly. After all, the electronic card and the special client software need the sound card in the PC to capture the audio signals for electronic card-to-PC transmissions and to generate the audio signals for PC-to-electronic card transmissions.

Assuming that the commercial recording software was installed first, Windows dedicates resources for that software in the sound card. Any other recording software that is installed later may not be recognized by Windows. Of course, if the special client software 114 (in FIG. 11) in accordance with the present invention is installed first, then the electronic card-special client software will work properly. The later-installed commercial recording software may have some problems working properly.

Of course, the user could manually unlink the commercial recording software from Windows to make the special client software work properly, but this is a cumbersome and annoying task. Furthermore, if some bug in the first-installed commercial recording software is present, the sound card in the PC would be locked and the special client software 114 (in FIG. 11) cannot function.

In accordance with one embodiment of the present invention, a special driver would be written and placed between the current driver and the Windows Multimedia interface. Referring to FIG. 43, several applications 430, 431, 432 are installed in the computer station, which in this example is a PC with a Windows operating system. One of the applications is the special client software 114 that can communicate with the electronic card of the present invention.

In order to access the sound card 438, these applications use the Windows Multimedia interface 433. Normally, the Windows Multimedia interface 433 communicates directly to a driver 437 to access the sound card 438. In one embodiment of the present invention, a special driver 435 is written and is placed between the

Windows Multimedia interface 433 and the driver 437. The API 434 of the special driver 435 is a copy of the API 436 of the driver 437. This special driver 435 is installed instead of the current default driver 437. But the special driver 435 uses the default driver 437 for normal operation. The special driver 435 also changes some of the recording parameters for the special client software 114 to function properly. Note that some of the processing can be done in the driver level, where the invention's "driver" layer will perform the processing.

In operation, when an electronic card signal is detected by the sound card 438, the driver 437 presents the data to the special driver 435. Some byte of data in the electronic card transmission will be provided to let the special driver 435 know that this data is for the special client software 114 and not the other recording applications. Of course, some decoding logic would be provided in the special driver 435 to decode this byte in the electronic card transmission. Once decoded, the special driver 435 processes this data for the special client software 114, while preventing other applications (such as application 430) from taking control. In effect, the special driver 435 convinces Windows Multimedia interface 433 that the current recording channel is no longer valid. Then, the special client software 114 accesses Windows Multimedia interface 433 for its own needs. This way, the special client software takes control of the sound card 438 without crashing the other applications in the computer system.

In another embodiment, as shown in FIG. 44, the special client software 114 interfaces directly with the special driver 435 instead of indirectly through the Windows Multimedia interface. The special client software 114 "steals" the appropriate handles that are used by another application (e.g., application 431) so that the electronic card-special client software communication can take place via the sound card 438. As known to those ordinarily skilled in the art, Windows provides handles of Windows Multimedia interface 433 to the relevant application. The relevant application uses the handles to have Windows Multimedia interface 433 perform various tasks.

4.6 SERVER-BASED PROCESSING

In the above description of the base station, special client software is resident in the client to perform such tasks as digital signal processing, data processing, performing some web-related action, and communication with selected web servers. Typically, all the necessary functionality are found in the special client software. In some cases, however, the software needed to perform some functions is downloaded from a designated server on an as-needed basis. In other words, the special client software in conjunction with a particular supporting web server determines whether a particular functionality is available in the client. If so, then the user goes about his business to conduct any transaction or otherwise communicate with that web server. If not, the special client software downloads that functionality from that web server so that the user can employ this functionality with this web server.

In another embodiment, the server contains all the functionality described above for the base stations to process the acoustic signals and perform the designated action based on the data in the signals. The client contains only the necessary software to record sounds and deliver those recorded sounds to any designated server. The server would then playback the recorded sounds and digitally process the signals to extract the data therein (if any). Thus, instead of processing the signals and communicating the data to the web server, the

client merely records the sounds and delivers them to the server. The server itself performs the digital signal processing operation, data processing operation, and the requisite action.

In this embodiment, the client software contains two main features: (1) recording, and (2) communications. The first feature allows the user the record the acoustic signal that is emitted when the user presses the button on the electronic card. The second feature allows the recorded signal to be delivered to a default designated web server to process the signals for authentication. The default designated web server would be contacted if the user did not already launch his web browser or the web browser has accessed a web page that does not support the electronic card and its communications protocol in accordance with the present invention. If, however, the web browser has already been launched and the user has accessed a page that supports the communications protocol of the present invention, then the communications component of the client software would interface with the web browser to deliver the recorded sound to that particular web page's web server.

Typically, when the web browser accesses a web server (i.e., web page) that supports the communications protocol of the present invention, the web server would send a code (or embedded data in the header) along with the html data that only the client software can interpret. It functions like a flag. When this code is detected by the client software, the recorded audio file can be delivered to this web server. If the code is not detected (i.e., this web page does not support the communications protocol of the present invention), then client software sends the recorded audio file to the default server.

5.0 APPLICATIONS

The spectrum of applications covered by the various embodiments of the present invention is broad. Referring to FIG. 46, at the core of the various applications is the electronic card 460 itself, whether in one-way or two-way form. As a receiver of information, the electronic card 460 can receive all kinds of information from simple facts to coupons, discount offers, promotional offers, and incentive points. The reception of information occurs via some electronic device 461, such as a broadcast media (e.g., TV, radio) or a personal computer.

The received information can be in two forms – (1) embedded information, or (2) actual content for later pattern recognition. The embedded information can be some code that complies with the communications protocol of the present invention. Exemplary embedded information can be actual synthesized sounds that are generated as part of the broadcast program, code that was mixed in later at some point in the distribution chain of the broadcast program, and an audio file that is played on a website.

For the reception and processing of actual content, no communications protocol need to be followed since the electronic card is recording the actual sounds (whatever they may be) that emanate from the speakers of the TV, radio, or computer system. Later, the user can playback his recording where some pattern recognition server will attempt to match that sound clip with one of the soundtracks stored in its database. When a match is found, the server will identify the sound clip, provide links associated with the sound clip, or automatically redirect the user to a relevant website associated with that sound clip. This pattern recognition feature is particularly valuable when the user has limited or no access to the Internet at the moment that the user

hears the sound. By recording that sound at that moment, he can later get more information related to that sound clip.

Based on the type of information received (and saved), the electronic card 460 can be used to exploit this information. Thus, if the information received is a coupon, the electronic card 460 can be used to redeem this coupon either online on the web or at a conventional bricks-and-mortar store.

As a source of information, the electronic card 460 allows the user to perform various acts with the mere press of a single button. The button press can launch applications or functions as represented by reference numeral 462, authenticate the user into a website or server as represented by reference numeral 463, or perform other acts 464 within a service once the user has successfully accessed and been authenticated into a service.

For the launching action 462, the press of the button initiates such things as launching an application (e.g., web browser), accessing a particular website (e.g., buying club, travel service (airline, car, hotel), online account service, online banking, and proprietary service such as America Online), or accessing some service that requires telephone dial-in. In this launching action, no authentication is necessary since the user is merely accessing services that are publicly available but in a way that is more efficient and user-friendly.

For the authentication action 463, the press of the button on the electronic card 460 enables the user to securely log into various services S_1, S_2, ... , S_N, whether these services are accessed over the web or via a telephone number. Thus, instead of arduously entering ID and password information, the electronic card 460 simplifies the process by performing the login functions for the user without compromising the security concerns of these services. Exemplary services include an online trading service, a private intranet, a proprietary database, a remote desktop, a remote hard drive service, a web-based email service, or a music collection service. The list of services, whether commercial or personal, is long and can be anything that requires some authentication action to allow the user to access the contents therein. The authentication would be needed because the service contains personal or otherwise private information that need to be securely protected, or the service is commercially motivated to limit access to paying users.

Once the user has successfully been logged into a service (accessed and authenticated), the user can use the electronic card 460 to perform other actions with the press of a button. These actions can be as simple as filling out a purchase form at the checkout line to purchase some merchandise at an online store. For more sophisticated operations, the press of the button on the electronic card 460 may involve detecting the context of the user's current online experience and taking some action based on this context. Thus, this context-sensitive feature can intelligently detect what the user wants to do based on which web page his was viewing at the time he pressed the button. One example of this type of action is the e-wallet 464 which simplifies the user experience at various merchants' websites M_1, M_2, ... , M_N.

In another embodiment, the authentication action 463 follows immediately from the launching action 462. Thus, although FIG. 46 shows two arrows directly flowing out of electronic card 460 into launch 462 and authentication 463, this alternative embodiment would show only one arrow directly flowing out of the electronic card 460. This one arrow would point to launch 462, which would point to the authentication action 463.

Importantly, these applications require no infrastructure changes. Existing sound systems in personal computers work with the electronic card.

5.1 BROADCAST MEDIA

One embodiment of the present invention is the user of the electronic card to download (and later redeem) coupons via broadcast media (e.g., television, radio). For the moment, the manner in which the coupons, targeted sales offers, special discounts, sales information, and the like are delivered to the broadcast media devices such as televisions and radios will not be discussed. Hereinafter, the term "coupon" or "coupon data" will be used to refer to these various sales offers. Thus, the electronic card 10 can receive coupons from a radio/stereo system 11 via sound waves 19w; a television 12 via sound waves 19x; a personal computer 14 via sound waves 19y; and a conventional non-web store 13 via sound waves 19z. To receive these sound waves, the electronic card 10 contains a transducer for converting the received sound waves into electrical signals for digital signal processing. The electronic card 10 is placed near the speakers of these broadcast media devices, computer speakers (such as speakers 14a and 14b), and speakers at checkout counters in conventional stores. Although the speakers generate the actual sound waves, the source of the sound waves (and the data therein) is located at key locations in the television/radio infrastructure (e.g., headend of a cable service), web infrastructure (e.g., web site), and the conventional store office (e.g., network server in the back room of a department store).

Once the coupon data has been received and stored in the electronic card 10, it can be redeemed in any number of ways. In one embodiment, the user of the electronic card 10 can use a web browser (e.g., Microsoft Internet Explorer or Netscape Navigator) in his personal computer 14 to access the Internet 16 via his Internet Service Provider (ISP) 15. Once on the Internet, the user can access any web merchant's web site 17 or web portal 18. Having located and accessed the web merchant 17 or web portal 18 that is sponsoring the coupon that he just downloaded, the user would then go to the web page that contains the coupon redemption information. Such a web page can be the home web site of the web merchant, or it could be merely a button on the web page that says simply, "Click here to use your electronic card coupon." When the user clicks on the button, the server associated with the web page would send an audio file (e.g., .wav file) to the web browser. The web browser would interact with the sound card in the computer 14 to play the audio file. The electronic card would receive the sound waves generated from the speakers 14a, 14b of the computer 14, process them along with the already stored coupon data, compare them to make sure that the proper coupon data is stored in the electronic card 10, and if the coupon data is proper, the electronic card 10 would generate a password on its LCD. The user enters the password manually on the keyboard and submits it to the web site. Then, depending on the type of coupon that the user previously downloaded into his electronic card, the web site could apply the coupon to the user's purchase or award a merchandise for free. This is just one of the many ways in which the user could use or otherwise redeem his coupon in his electronic card 10. This and other ways of redemption are detailed below.

An alternative option is that the customer will not need to remember the merchant's web address. The web address will be stored as part of the coupon data. The user would simply access a central homepage, press

the button on his card, and the card will transmit the data (two-way card) and the browser will direct him automatically to the merchant's web page. In fact, the web address may even direct the user to the exact product with the discount already in place. To save space and communication time, instead of full webpage addresses, the coupon will contain a coupon ID which will be interpreted at the central homepage. A second option will be to use a tray application that always listens and does the job of the central homepage (selection of coupon and redirection). In addition, using the same pattern recognition method described below, the coupon could be a recorded part of the commercial which will then be associated and detected in the central web page.

If the user stored multiple coupons, the browser will ask him which one to use and he will make his choice either via clicking or via the keyboard/mouse. These and other embodiments will be described further below.

5.1.1 BROADCAST MEDIA INFRASTRUCTURE

One embodiment of the present invention allows coupons to be downloaded from the television/radio infrastructure to a user's electronic card 10 (see FIG. 1). The manner in which the coupon can be redeemed varies from application to application. First and foremost, a brief discussion of the television and radio infrastructure will be provided.

Cable television systems are well known. As shown in FIG. 23, these systems are usually comprised of a headend 170a with one or more trunk lines 172a-172c extending therefrom, where each trunk line has a plurality of feeder lines 173a-173c extending therefrom into subscriber areas. Each subscriber 174a-17 is attached to a feeder line via a line tap onto the feeder or service line.

If the distances between the headend and subscriber areas are substantial, intervening distribution hubs 171a-171c may be located along the trunk lines to replenish the strength and quality of the signal transmitted to the subscribers. Distribution hubs simply act as small headends and exist to ensure the quality of delivered signal in large CATV networks. Each distribution hub may, in turn, be coupled to a plurality of service sites by feeder lines. Each service site may have one or more service lines extending therefrom to couple a plurality of subscribers to the service site.

In this cable network, a transmission signal is provided by the headend 170a over the trunk lines 172a-172c to the distribution hubs 171a-171c or service hubs. This amplified signal is then provided to the feeder lines 173a-173c extending from the distribution hub or service hub to provide the signal to the service sites. Taps located at each subscriber site bring the transmission signal into a subscriber's site.

The transmission signal from the headend 170a may include entertainment signals and data signals. The entertainment signals may be received as broadcast signals received via satellite 179 from an originating location. This originating location may be another headend 170b. This originating headend 170b receives its signals from channel or program sources 175a-175c. These channel or program sources 175a-175c may be HBO (i.e., Time Warner), TBS, ESPN, ABC, NBC, CBS, PBS, or even the Food Network. It is also possible for the channel or program sources 175a-175c to have a direct link to headend 170a (instead of headend 170b) if these channel or program sources are located reasonably close so that a satellite link is not necessary.

At the headend 170a, the policies and business strategies dictate which of the many programs the headend 170a receives from the headend 170b will be rebroadcast to the subscribers and on which channels. Each subscriber area may receive a different set of channels and programs as determined by the headend 170a. Of course, the subscriber also controls which of the available channels he receives based on his subscribed service.

Each broadcast signal is placed on its own channel within the spectrum of the trunk, feeder and service lines used in the CATV system. The spectrum of the lines coupling the CATV system together is the range of frequencies supported by the communication conduits used for the lines. In a typical CATV system, this spectrum is divided into a transmission portion and a return portion. The return portion of the spectrum may be used to support data transmissions, telemetry, and/or control information from subscriber sites back to the headend. The data transmissions from subscribers typically include status information about the subscriber's equipment which may be used by components at the headend to ascertain the status of the cable system or subscriber equipment.

Referring now to FIG. 24, the conventional broadcast television and radio infrastructure is somewhat analogous. A user 185, among many users, has a TV antenna on the roof of his house. With the antenna and the TV inside his house, the user can receive broadcast TV signals from a number of TV station transmission towers 183a-183c, if these transmission towers are reasonably close and are transmitting at a suitable power. These transmission towers 183a-183c are associated with local TV stations 181a-181c.

Typically, each TV station is affiliated with one of the major networks – NBC, CBS, ABC, PBS, Fox, or WB. By being affiliated with one of the networks, the local TV stations can broadcast network programming during prime time (usually 8 PM to 11:00 PM), late night (11:30 PM to 1:30 AM), daytime (e.g., soap operas), and certain other designated time periods (e.g., weekend sporting events). In addition, these local TV stations can broadcast locally produced programming such as local news, local sporting events (e.g., high school or local college), and local events (e.g., downtown Christmas parade). Finally, these local TV stations can broadcast syndicated programming at various desired time slots. These syndicated programs can be reruns of popular TV shows (e.g., MASH, Cheers, Star Trek), currently produced game shows (e.g., Jeopardy, Wheel of Fortune), or the lengthy infomercials, among others.

Usually, the TV stations 181a-181c receive non-locally produced programming from a network or programming source, such as source 184. If the distance is great, a link with a satellite 186 is needed. Typically, each local TV station would have its own satellite dish and receiver to receive these non-locally produced programming from the source 184. In other cases, a distribution center 180 is provided with a satellite dish and receiver which then delivers the programming to the appropriate local TV station 181a-181c via lines 182a-182c. Typically, the distribution center 180 is associated with a particular network (e.g., NBC) to serve several nearby local TV stations who are also affiliated with the same network but which serve different local regions (with some overlap).

The infrastructure for radio stations is similarly structured as shown in FIG. 24. Thus, a radio station 181a has local programming as well as network programming and syndicated programming (e.g., Howard Stern

Show). The non-locally produced programming are received from the network or program source via satellite. The locally-produced programs originate from the radio station itself normally. The user 185 has a radio/stereo system with speakers and an antenna.

5.1.2 BROADCAST MEDIA COUPON TRANSMISSION

A coupon is a sales item that a merchant distributes to the mass public or a limited set of the mass public (i.e., targeted consumers) to promote his store (web or otherwise), product line, service line, or other business. The hope is that after redemption of the coupon, the consumer will like the product or his "visit" to the store just enough so that the consumer will buy that coupon or visit that store again. With this initial step, the merchant hopes to breed brand or store loyalty with this consumer. Usually, coupons are found in print media (e.g., newspapers, magazines) or on ad banners in certain web pages. But, as mentioned above, coupon distribution via the print media or the Internet is inefficient and ineffective.

Use of a special card that simply records time slices of sound for playback to a centralized pattern recognition server that correlates each slice to a coupon is discussed more fully below. But in circumstances where a more brief and reliable way of communicating coupons is desired, or in information environments that are too data rich for convenient implementation of a pattern recognition server, another method of communicating coupons to a card from an ordinary television, radio or sound device will now be discussed.

In accordance with one embodiment of the present invention, coupon data can be either in the audible frequency range or ultrasonic range. These data are mixed with normal programming so that when the user is watching TV or listening to the radio, he can collect coupons in a relatively simple manner. The television or the radio set itself is a passive device; that is, it receives electromagnetic signals, demodulates them, and presents the information in the signals to the user via the TV screen and speakers. Thus, the TV set or radio set itself does not generate any coupons; rather, it merely presents what it receives from the program/channel source.

Accordingly, the coupon data are mixed at a point somewhere along (and including) the communication path between the network/channel/program source and the user. Taking the exemplary cable infrastructure illustrated in FIG. 23, the coupon data can be generated with the program at the program source, such as program source 175a. In one example, the studio that makes a particular movie or TV show can "place" a coupon into the plot of the show. Much like product placement, the producers of the TV show could, for example, create the data stream (see FIG. 5(B)) by electronically synthesizing it. In this example, this synthesized data stream is audible. During the making of that TV show, an actor could announce on-air, "Please take out your XYZ card to receive a free gift or coupon. In just a few seconds, the coupon will be delivered to you." A second method will be to show a special visual mark at the corner of the screen at the beginning of the commercial and remove it when it is over. At this point, the audible data stream is played. This is recorded as part of the show. Of course, the context of the TV show is such that this announcement will not seem out of place or inappropriate. The TV show could be a home shopping network or a standard sitcom. When this TV show, which was recorded sometime in the past, is finally broadcast on TV, and the user watches it, he will be able to download the coupon at the proper time. So, when the scene where that actor makes that

coupon announcement is shown, the user merely points his electronic card to the TV speakers and receive the audible data stream for storage in his card. The user now has the coupon or gift in his electronic card. Of course, only those users with the electronic card can interact with the TV in this manner to receive this coupon. In this case, the coupon is provided within the show itself and therefore, no mixing of the data stream with the audio tracks is necessary.

In an alternative embodiment, this embedded audio data could be played repeatedly throughout the broadcast of this show so that the user need not time his recording precisely. Thus, whenever this show is on, the user could record a portion of the broadcast and since the embedded audio data is looped over and over again, the user is assured of capturing this data in his electronic card.

For the most part, however, the merchant of the coupon do not want to be indelibly linked to a TV show, radio show, or movie forever. In this case, the data stream containing the coupon data is mixed with the audio tracks at another point in the broadcast link. If the merchant has some agreement with a channel or network source, such as HBO or CBS, he can ensure that his coupon his placed with certain shows for a certain time period. If the merchant's agreement runs for one year, he may specify that every episode of CBS's "60 Minutes" for the coming year should air the merchant's coupon at some specified time. Although "60 Minutes" is produced like always, the CBS channel source that is responsible for distributing the show to its affiliates mixes the merchant's coupon data stream with the audio tracks of "60 Minutes". The CBS channel source also provides some visual indication of when the data stream will be played to alert the viewer to get his card out for the download. This show is then provided by CBS to the headend 170b (FIG. 23) which then delivers "60 Minutes" along with other programming to the appropriate headend 170a for regional distribution. When "60 Minutes" is finally broadcast on cable TV, the user merely takes out his card at the appropriate time (which is specified) and downloads the coupon.

Similarly, a merchant may buy certain 30 second or 1 minute commercial slots to be played during commercial breaks of a TV show. The merchant may record the data stream in his commercial so that when the commercial is finally played, the coupon data can be played and the user can download the coupon.

Similarly, the mixing of the coupon with the programming (or commercial) may occur at the headend 170b or 170a. Normally, the headend associated with the cable service has commercial slots of its own to sell. Some of the merchants buy these commercial slots and much like the above TV commercial, the merchant records the coupon data stream with the commercial so that when the commercial finally airs, the coupon data stream is emitted and the prepared user can download the coupon. The headend could also mix coupon data streams on its own with the audio portion of the programs that are aired. A headend that is responsible for a region can strike deals with local merchants who want to air their coupon data stream. In this manner, local merchants can distribute the coupon data to the subscribers in the region of interest at a price much lower than the national merchant who wants to advertise nationally. This is similar to paying for local advertisement time on local TV channels.

The same principles apply to the conventional TV/radio broadcast infrastructure. The coupon data stream can be recorded or mixed at the production studio (e.g., for shows and commercials), the network source

(e.g., CBS), and the local station (e.g., station KXYZ). Each entity in this broadcast link can strike its own deals with merchants who want to provide coupon data to users.

When the data stream is emitted by the speaker of the TV or radio, the user normally points his electronic card in the direction of the sound and presses the RX button to receive and download the data. The card then turns off after the data has been received. If more coupons are available, the user can activate his card and receive more coupons. The number of coupons stored in the card is limited by the storage space.

Referring to FIG. 5(B), the data stream includes a data portion. This data portion can be any length and can contain any information. In the coupon case, the data portion may include a merchant ID and a coupon number. The coupon redemption scheme relies on these two pieces of information to authorize the redemption.

In another embodiment of the present invention, the coupon data are transmitted to those subscribers with set top boxes. Set top boxes are normally used for interactive TV as well as certain premium cable services (e.g., AT&T Cable Service's Expanded Service with Digital Cable). For these cable services, these set top boxes also provide some electronic TV program guide functionality so that the user can simply select his channel using his on-screen program guide rather than entering the channel number directly. Of course, the user can still enter the channel number directly if so desired.

For this embodiment, the coupon data are transmitted during off-peak hours (e.g., early in the morning) once a day, or during the vertical blanking intervals (VBI). As the coupon data is transmitted, the set top box receives and records them for later playback as necessary. Thus, instead of the coupons being associated with a program, the coupons are now associated with a channel or the electronic TV program guide. The user can turn to a dedicated Ad channel where he can scan the listed coupons and select the ones he wishes to download. When he has selected a coupon for download, he presses a button on his set top box remote control (or his electronic card). The set top box then plays the audio file that contains the coupon data. The user would of course have his electronic card ready and pointed toward the speaker. The coupon data is now stored in his electronic card.

5.1.3 BROADCAST MEDIA COUPON REDEMPTION

Assuming that at least one coupon is stored in the user's electronic card, the user has several options to redeem his coupon:

(1) Password-based Internet Manual Redemption -- access the coupon sponsor's website and redeem manually via a password

(2) Internet Automatic Redemption -- access the coupon sponsor's website and redeem automatically

(3) Store Redemption -- physically visit a store and manually redeem at the checkout line/kiosk

These redemption schemes will now be discussed. In the preferred embodiment, the automatic form of redemption if favored over the manual redemption, although both are feasible.

5.1.3.1 Password-based Internet Manual Redemption

Password-based Internet Manual Redemption implies that the user must enter some key sequence with his computer keyboard to redeem his coupon. In one embodiment, the user's electronic card includes an LCD display. In this embodiment, the user accesses the website associated with the stored coupon. Eventually, he

navigates to the page where the coupon redemption function is provided. He may even see a button on the web page that says "Click here to redeem with your electronic card." When the user presses the button on the web page, the web page asks the user to press the RX switch on his electronic card. The web page plays an audio file which includes what is hereinafter referred to as "redemption data" and the electronic card receives this audio signal and processes it.

Based on a known algorithm that checks whether the coupon is valid or not (based on the merchant ID and coupon number), the electronic card displays a password. Simultaneously, the web page asks if the user received the signal properly. If not, the user can press that button on the web page again to initiate the playing of the audio file. If the user's electronic card received the audio signal properly and provided a password, the web page provides a section that allows the user to manually enter the password. The user then enters the password. The web site checks to make sure that this is a valid password and if so, authorizes the redemption. If the password is not valid, the website will deny the redemption request. The user then proceeds in the conventional manner to either continue shopping or go to the checkout line to claim his gift or otherwise apply his coupon to his purchase.

In this embodiment, the password is unique to this particular redemption because the counter value and the individual ID (refer to the discussion above with respect to FIGS. 5(A) and 5(B)) in the card have been incorporated in the password generation. Thus, merely giving a friend this same password will not enable this friend to "redeem" a coupon because that password is unique to the electronic card holder and that particular transaction. Another electronic card user who downloads a coupon will have a different password.

In another embodiment, the special client software 114 (FIG. 11) plays a more important role. When the user navigates to the web page where the coupon redemption function is provided, he may see a button on the web page that says "Click here to redeem with your electronic card." When the user presses the button on the web page, the web page asks the user to press the TX switch on his electronic card. When the user presses the button on the web page, the web site delivers the redemption data which is provided to the special client software. The user also activates the TX switch on his electronic card to transmit the coupon data to the PC. The PC processes the coupon data with the redemption data and generates a password. The password is displayed by the PC and the user can enter it manually with his keyboard into the web page. The web site checks the password and either authorizes or denies the redemption request.

In the above two examples, the user's electronic card may hold several coupons. The processor checks each coupon separately with the redemption data to generate the password. For those coupons that are not associated with a particular merchant's redemption data, they are ignored.

Note that these password or two-factor security schemes are, as a practical matter, less convenient to the user. So, these two-factor security schemes will be employed if security is paramount. If, however, convenience is paramount, such as for online shopping, these two-factor security schemes will not be employed. The user only needs the electronic card itself to conduct his online shopping.

5.1.3.2 Internet Automatic Redemption

Internet Automatic Redemption implies that the user need not enter any key strokes with his computer keyboard to redeem his coupon. Furthermore, the user's electronic card need not have an LCD display. In this embodiment, the user accesses the website associated with the stored coupon. Eventually, he navigates to the page where the coupon redemption function is provided. He may even see a form on a web page that requests, "Please enter the coupon redemption number." The user then presses the TX switch on his electronic card which transmits his counter value, individual ID, and the coupon data. If more than one coupons are stored in the electronic card, all coupons are transmitted to the PC.

The special client software 114 (see FIG. 11) receives the data and displays a dialog box with some choices and asks the user which coupon he would like to redeem. The user selects the choice that corresponds to the coupon he wishes to redeem. The special client software then fills out the web page form with the coupon redemption number (which may incorporate the individual ID, counter value, and coupon data) and sends the form back to the web site. The web site checks the coupon data as well as the user's individual data and counter value to ensure that this user is a valid card holder and eligible to receive this coupon. The counter value is used to ensure that this same downloaded coupon cannot be used again by some computer hacker who stole the coupon redemption data online. As described above, with each press of the electronic card, the counter value increments.

In another embodiment, when the user navigates to the web page where the coupon redemption function is provided, he may see a button on the web page that says "Click here to redeem with your electronic card." When the user presses the button on the web page, the web page asks the user to press the TX switch on his electronic card. When the user presses the button on the web page, the web site delivers the redemption data which is provided to the special client software. The user also activates the TX switch on his electronic card to transmit the coupon data to the PC. The PC processes the coupon data with the redemption data and generates a password. The password is not displayed and the software can provide this password to the web site automatically without the user ever knowing the password. The web site checks the password and either authorizes or denies the redemption request.

Again, the password is unique to this particular redemption because the counter value and the individual ID (refer to the discussion above with respect to FIGS. 5(A) and 5(B)) in the card have been incorporated in the password generation. Another electronic card user who downloads a coupon will have a different password.

5.1.3.3 Store Redemption

In this embodiment, the user takes his electronic card to a conventional non-web store. Of course, the store sponsored the coupon he downloaded or otherwise sells a product/service of the company that sponsored the coupon. He takes his electronic card to a kiosk, which is equipped with a PC. The user activates the kiosk to prepare it to receive the coupon data. He then activates the TX switch on the electronic card to transmit the coupon data, along with his individual ID and counter value. The kiosk receives the information and checks to make sure the coupon is valid. If the store is a national or otherwise chain-type store, this check may occur at a designated network server that links other related stores. If the store is purely a local store, the check may be

done locally at the kiosk or a network server that serves that particular store. If the check indicates that the coupon is valid, the kiosk may generate an actual paper coupon for the user to use at the checkout line.

Note that in another embodiment, the system uses pattern recognition as described more fully below. In this pattern recognition embodiment, the kiosk may "listen" for the recorded time slice of audio stored in the electronic card and perform pattern matching.

In another embodiment, the user may simply go to the checkout line at the store (with or without any merchandise, depending on the coupon). At the checkout line, the store has a computer that also functions as an electronic cash register. Equipped with a standard sound device, the cashier asks the user to press his TX switch on his electronic card. He does so and the coupon data along with his individual ID and counter value are transmitted to the store computer. This transmitted data is now checked. Again, like the kiosk case above, if the store is a national or otherwise chain-type store, this check may occur at a designated network server that links other related stores. If the store is purely a local store, the check may be done locally at the network server that serves that particular store. If the check indicates that the coupon is valid, the computer allows the user to redeem that coupon. If some merchandise is involved, the value of the coupon is applied to the purchase of that merchandise. If a free promotional item is offered, the item is given to the user without charge. Thus, based on the nature of the coupon, the action taken after the check will vary.

Another redemption scheme involves the use of the magnetic strip on the electronic card. A code would be written onto the magnetic strip portion of the electronic card as the user downloads coupons electronically off the web or some media device. The logic circuitry necessary to write this code onto the magnetic strip area exists in the form of magnetic strip writers. The various components to realize the magnetic strip writer are manufactured in miniature form to comply with the electronic card's form factor requirements. Appropriate software in the electronic card would detect that a coupon was downloaded and stored in the electronic card. This software would then instruct the magnetic strip writer circuitry to write the redemption code onto the magnetic strip area of the electronic card.

5.1.4 INTERACTIVE TV AUCTION

In this embodiment, the television set is an interactive TV set, typically with a set top box. When a live auction is broadcast on one of the channels, the user is allowed to bid on an item by pressing the TX switch of his electronic card. For example, assume that one of the channels is an auction channel, perhaps even called "The Auction Channel." The Auction Channel broadcasts traditional auctions with perhaps live participants. However, in addition to live participants, TV viewers equipped with the electronic card of the present invention are also allowed to bid on the item. Whenever the user presses the TX switch, the electronic card sends out his individual ID, counter value, group ID, among other data. The two-way set top box receives the user's data stream and passes this data stream along to the various distribution hubs and headends that make up this return path. Ultimately, the user's data stream makes its way to the server of the Auction Channel for the particular auction he is viewing.

When the Auction Channel's server receives the user's data stream, performs an authentication check (i.e., the user is a valid user) and the request is a valid request by checking the counter value, among other data.

When all the checks have cleared, the user's data stream is interpreted as a valid bid by the Auction Channel's server and also by the human auctioneer. This process can continue until the item has been awarded to the winning bidder.

Alternatively, the user's data stream may go to a dedicated authentication server that is independent of the Auction Channel's server. Once authenticated by this authentication server, the user can then use his conventional set top box remote control to bid on items for that particular auction.

5.1.5 CONTENT RECORDING FOR SEARCH/REDIRECTION

In another embodiment of the present invention, the electronic card can be used for recording an audio clip of the raw content broadcast over TV, radio, or heard by the cardholder. Once the audio clip has been recorded, a variety of redemption schemes allow the user of the electronic card to benefit from the recording. For the purposes of this patent specification, the term "redemption" is used to denote any type of action that the user takes to obtain something for recording that audio clip with his electronic card. Basically, the redemption schemes include: (1) finding information that is related to or associated with the audio clip more quickly and easily than conventional Internet searching techniques; and (2) receiving coupons, incentive points, or other sales offers as a reward for watching that TV program/advertisement or listening to a particular radio broadcast/advertisement. These redemption schemes can be implemented on-line over the Internet or at a conventional store. Details of these redemption schemes are provided below.

5.1.5.1 Electronic card Hardware

Referring to FIG. 1 again, the electronic card 10 is now basically a portable digital recorder of sound. Audio, for example, from TV and/or radio can be recorded as an audio clip. Typically, only 5 to 10 seconds of the audio clip need to be recorded for the redemption scheme to succeed. Thus, if a user missed the beginning of a broadcast, he need not worry since recording any portion of the entire audio soundtrack is sufficient for successful redemption. As for the quality of the recording, high fidelity level is not necessary and thus low component/fabrication costs and small form factor sizes can be achieved.

FIG. 20 shows one embodiment of the electronic card that provides the analog recording function. This FIG. shows a two-way card, in which the receiver portion 209a functions as a sound recorder and the transmitter portion 209b functions as a playback device. Power to the entire card is provided by a power supply 207, which in one embodiment is a Varta LPF-25 battery. The power supply 207 provides power to the microprocessor 205, the switch block 206, and the RAM 208 for battery back-up.

The digital core of the card is a microprocessor unit 205, which is coupled to a battery backed-up RAM 208. The RAM 208 needs to be battery backed-up to keep the recorded sounds in memory for as long as the user desires. In one embodiment, the microprocessor 205 manages the memory in the RAM 208 in a first-in first-out (FIFO) scheme. In this manner, the oldest recorded and stored audio clip is played first (during playback). If not enough memory space is available, the microprocessor 205 erases the oldest recorded audio clip first. Thus, as more and more audio clips are recorded and stored, more and more of the oldest stored audio clips will be replaced by the newer audio clips if memory space becomes an issue.

For the analog front end portion, a transducer 200 and a switch block 206 are provided. The transducer 200 can be either a single transmitter/receiver transducer or two separate transducers (i.e., one transducer functions as a microphone and the other transducer functions as a speaker). The switch block 206 provides power to the entire card. In one embodiment, the card contains two switches – a record switch and a transmit switch. These two switches are provided in the switch block 206. As described above, the switch block has silicon switches so that when the user releases the switch too soon, the rest of the circuitry in the card still has enough power to perform their respective functions. The recording feature will now be discussed. When the record switch is pressed in the switch block 206, power from the power supply 207 is provided to the transducer 200 as well as the rest of the circuitry in the card. Sound that is picked up by the transducer microphone is delivered to the receiver portion 209a of the card where it is amplified (amplifier 201), filtered (BPF 202), and gain controlled (AGC 203) prior to being digitized (A/D 204). The digitized sound is provided to microprocessor 205 which stores the digitized recording in RAM 208. Because each recorded audio clip takes up only 5-10 seconds, the RAM 208 must be large enough to support all the recordings that need to be stored. Typically, 5 seconds of sound take up approximately 500 KB of memory.

The playback feature will now be discussed. Having stored the sound in RAM 208, the recorded sound can be played by the user at any time. When the user presses the playback switch in the switch block 206, the recorded sound stored in RAM will be played through the transducer speaker of the card. Each press of the playback switch plays a single recorded audio clip in the order in which they were stored. Thus, the first press of the playback switch activates the playback of the oldest audio clip file. The second press of the playback switch activates the playback of the second oldest audio clip file. This process is circular so that after the newest audio clip file is played, the next audio clip file to be played corresponds to the oldest audio clip file. Of course, one ordinarily skilled in the art can devise other similar schemes to playback recorded audio. Multiple buttons can be implemented as well as a single button with multiple functions (or modes). Perhaps a delete button can be implemented so that the user can selectively delete the desired audio clip.

The circuitry in the transmitter portion 209b of the card is similar to that of FIGS. 2, 7, 8, 9, and 10. However, in this embodiment, the switch press activates a transmit routine that incorporates the audio clip file stored in RAM 208. A pointer is implemented that keeps track of which audio clip to play. After each press of the playback switch, the audio file being pointed to is played, and the pointer then moves to the next oldest audio file in RAM 208. In addition, the DES3 encryption scheme which includes the use of the group ID, individual ID, and counter values can also be used for authentication purposes. Thus, when the playback switch is pressed, an encrypted version of the audio clip file along with other authentication data is transmitted to the computer's microphone. The server receiving this data can authenticate the user and provide the pattern recognition search service for website redirection or coupon/incentive point collection, as described below.

5.1.5.2 Server Architecture

A server computer station 210 associated with the broadcast media interactive system in accordance with one embodiment of the present invention will now be discussed with respect to FIG. 21. At the core of the server 210 is a web server 215b which interfaces with a database server 212, a messaging server 215a, an

authentication server 213, and the Internet 16. The web server 215b is further coupled to communications lines 219f (e.g., via a modem or network router connected to server 210) and the Internet 16.

In one embodiment, the web server 215b performs many tasks related to the management of the accounts, merchandises, coupons, incentive points, and soundtracks, music sales, sales of other services or merchandise associated with the recorded sound clips, or other information services relevant to the card issuer. From executing code for any number of different applications, managing resources, handling web requests, managing files and records, creating files and records, deleting files and records, delegating tasks, and handling exceptions, the web server 215b provides the main processing for the server 210. As noted above, this functionality, in other embodiments, could be distributed across multiple hardware servers.

The web server 215b also works with a messaging server 215a via line 219d (e.g., the system bus or a network connection to another hardware server) and a database server 212 via line 219b. The messaging server 215a works with the web server 215b via line 219d and is also connected to the Internet via communication lines 219e. The messaging server 215a provides various messaging functionality in various communications media such as telephone, email, instant messaging, active desktop application, and web browser notices. For example, email notices such as product news, discount updates, and customer service access are provided via communications line 219e. News of upcoming sales offers that may interest the potential customer are delivered frequently. Also, any questions that a user may have may be directed to customer service through the messaging server 215a, which will direct the email to the appropriate personnel within the customer service department. As noted above, various forms of instant messaging as are well known in the art could replace some or all of the functionality of messaging server 215a.

Note that communications lines 219e and 219f are standard interfaces to the Internet (e.g., an Ethernet or other network interface to a router and CSU/DSU, modem, etc.) or across machines which are typically Ethernet-connected at the "back end" of the network.

In another embodiment, the web server 215b and messaging server 215a are integrated in an Internet server 215. The interface to the Internet 16 is provided by primary communications line 219f (line 219e is not implemented). Thus, all web traffic passes through this Internet server 215 via communications line 219f. The messaging server 215a communicates with the web server 215b and the back end of the system (e.g., database server 212).

The database server 212 performs many tasks related to the creation, deletion, and management of various files and records managed by the server 210. The database server 212 supports the web server 215b in accomplishing its tasks of running the redemption portion of the broadcast media interactive system. The database server includes a management tools and web page information unit 212a and a pattern recognition search engine unit 212b. The management tools and web page information unit 212a provides exactly that – tools for the web page administrator to update, modify, and troubleshoot his web site. The web page information is also provided herein so that the web server 215b accesses the web page information from this unit 212a. Thus, when a user logs into the web page associated with server 210, the look and feel of this web page is stored in the unit 212a. However, the web server does not access the unit 212a for each access of this

web page; rather, the web server 215b accesses the web information in the unit 212a only periodically to update its contents. The pattern recognition search engine 212b will be discussed in greater detail below. Generally, however, the pattern recognition search engine 212b performs pattern recognition matching functionality between a user-submitted audio clip and the soundtrack files in the soundtrack database 211d.

The database server 212 serves a database of content to be operated or accessed in conjunction with card operation. For example, that database server 212 can serve an incentive points database 211a, a coupon database 211b, a merchandise database 211c, a soundtrack database 211d, and an account database 211e. These databases 211a-211e are coupled to a communications line 219a and to the database server 212.

These databases on communications line 219a comprise the "back end" of the system. Note that the common bus-like illustration of the communications line 140 is merely conceptual. The databases may not actually be on a common bus. These databases may be widely dispersed geographically or integrated into one database. Also, some of the databases may be on a common bus while others may be located remotely and accessed via the Internet.

The incentive points database 211a contains various incentive points banner ads and programs. Additionally, the prerequisites for earning these incentive points are also stored herein. Similarly, the coupon database 211b contains various coupon information that is either disseminated via the messaging server 215a or awarded to certain users when certain requirements are satisfied. Also, the merchandise database 211c contains various merchandise information that can be purchased by users or awarded based on satisfying certain requirements. These databases 211a-211c can also contain links to specific web pages associated with the incentive point, coupon, or merchandise so that the user can be properly redirected to that website. In another embodiment, these databases do not contain ads, programs, coupons or information; rather, these databases contain only links where the user can be properly redirected for more detailed information. The website associated with the link has the programs and coupons that are awarded to users. If necessary, these websites communicate with the account database 211e to keep credits, debits, and points information.

The soundtrack database 211d contains soundtrack files for those TV programs, TV ads, radio programs, and radio ads of companies that are participating in this broadcast interactive system. This soundtrack database could also just be a collection of music from a given genre that is available for sale. That is useful for implementations in which cardholders know that they can operate their card to identify that sort of music. For example, a "top 40" card or a "country & western" card might be considered. The various incentive points, coupons, and merchandise are awarded in conjunction with some matching function performed by the pattern recognition search engine 212b against the files in the soundtrack database 211d. Alternatively, the matching function results in the user being redirected to the website that is associated with the matching soundtrack file.

For example, assume that a requirement for winning a certain number of incentive points or a particular coupon or a particular merchandise is providing proof that the user watched a particular ad that appeared in conjunction with a certain TV show (e.g., ABC Corporation's ad in an "X-Files" episode). One form of proof that the server 210 will accept is the audio clip recorded with the electronic card 10 (FIG. 1). The

user records an audio clip from that advertisement (perhaps the jingle portion of the ad). The user then accesses the website associated with this server 210 with his browser and plays back the recording. The pattern recognition search engine 212b compares the user's audio clip to those stored in the soundtrack database. If a match is found between the user's submitted audio file and a soundtrack file in the soundtrack database 211d as determined by the pattern recognition search engine 212b, then the incentive points, coupons, and/or merchandise are awarded to the user who submitted that audio file.

Analogously, the successful match may result in the user being redirected to a particular web page where he can get more information on the product/service that was advertised in that TV ad. For example, if a user recorded an audio clip from a commercial featuring XYZ Corporation's coffeemaker, the pattern recognition search engine would then match the user-submitted audio clip with the appropriate soundtrack file associated with XYZ's coffeemaker. The match results in the user being redirected to the website associated with the XYZ coffeemaker.

In another example, the user may record a sound clip from some music that he heard over the radio. Although the user is unsure of the music's identity, he knows that he "likes" it. He accesses some central music website where he plays his sound clip. The pattern recognition software identifies the music and provides for the user the various CDs and other music forms (e.g., MP3) that are available for purchase. Thus, without knowing the title or artist of the music that he just heard on the radio, the user is able to identify and purchase that piece of music by merely recording a sound clip from that music and playing it back to a central website. This is especially useful because in most cases, the radio station rarely identifies the title (or even the artist) of a piece of music prior to actually playing that piece of music over the air. Usually, this identification occurs after the music is played. Sometimes, the radio disc jockey identifies this music along with several other songs that have also aired, which complicates the identification process for the user. Not only does the user have to match the identification with the actual song he heard, but he may have to wait for quite some time before the radio disc jockey makes the on-air identification. With this embodiment of the present invention, the user merely records the a clip of the song and play it back to a central music website. The music website will identify the music immediately and also suggest CDs that contain that song to purchase.

The memory 214 provides support for the database server 212 and the authentication server 213 so that these servers can serve all the user requests coming in. For example, hundreds if not thousands of users may be accessing this server 210 to submit audio clips. These audio clips are temporarily stored in the memory 214 until they are served by the database server 212, the authentication server 213, or both. The pattern recognition search process also requires some memory space to perform the match functions.

The account database 211e contains information about each user's account. Normally, only a user with an account (i.e., member) get the benefit of this broadcast media interactive system with points, coupons, and merchandise. The account information includes account balance (points or otherwise), expiration date for each point or group of points, redemption information, credit card information, billing information, billing address, and whether the account is authorized for using points for credit. Although this embodiment illustrated in FIG.

2 shows the account database 211e integrated with the rest of the server 210, another embodiment may have the account database located in a third party's server and maintained by the third party.

These databases 211a-211e contain appropriate linking fields so that an entry in one database can be associated with a related entry in another database. For example, when a user earns incentive points from the incentive points database 211a, that user's account in the account database 211e is appropriately updated.

In another embodiment, the incentive points database 211a, the coupon database 211b, and the merchandise database 211c are integrated into one database. The soundtrack database 211d and the account database 211e, however, are kept separate. In still another embodiment, these databases are distributed across one or more machines. These machines are coupled via communications line 219a to the database server 212. These databases comprise the "back end" of the system which the Internet server 215 access.

The authentication server 213 provides security functionality so that only those users with a proper account can access the features provided by the server 210. In particular, the data stream of the electronic card, which includes the group ID, individual ID, counter value, and raw data, can be encrypted. These fields can be checked against the account database to ensure that the proper user (individual ID, counter value) associated with a proper participating merchant (group ID) is accessing the system. Of course, the audio clip (i.e., raw data) is used only when the user has been authenticated. The authentication server also ensures that only those users with the properly sponsored electronic card (which performs the encryption and frequency translation (e.g., to ultrasound)) can access the server. Thus, anyone with a standard tape recorder cannot merely record an audio clip of a TV commercial, access the website associated with server 210, playback the audio clip, and obtain the desired service (e.g., redirection) or item (incentive points, coupons, merchandise).

In another embodiment, the authentication server is not implemented so that, for example, any user with a tape recorder could record the relevant audio clip, access the web site associated with server 210, playback the recording, and obtain the desired service or item, so long as the user is a member (i.e., has an account in the account database 211e) or opens a new account. This aspect, however, might be less than desirable because of the lack of convenience that the electronic card would otherwise provide. Still, the basic audio recording and playback functionality required by the system could be so provided.

The pattern recognition search engine (212b in FIG. 21) will now be discussed. In particular, the pattern recognition search functionality in the pattern recognition search engine will be described. Referring now to FIG. 22, the 5-10 second audio clip that was submitted by the user is represented by reference numeral 220. This audio clip is sampled at sampling block 221. In one embodiment, the sampling rate is 2,000 samples per second. The sampled audio clip is presented to a normalization block 222. The normalized audio clip is then presented to filtering block 223 to remove undesired frequency components.

A time slice block 224 receives the filtered audio clip. This time slice block divides the audio clip into time slices, where each time slice is approximately 20-50 msec in duration. Each audio file in the soundtrack database 211d (in FIG. 21) has also been divided into time slices. The search for a match between the user-submitted audio clip and one or more audio files in the soundtrack database 211d (in FIG. 21) involves comparing time slices of the user-submitted audio clip and time slices of the audio files in the soundtrack

database. The length of each time slice in the pattern recognition search engine 211d (in FIG. 21) should be short enough to make the match process time-invariant. In other words, the incoming audio clip submitted by the user is a 5-10 second clip from any portion of the soundtrack that aired on TV or radio. One user may start recording as soon as the soundtrack began, while another user starts recording 4.2 seconds into the soundtrack. No two users may record the same section of the broadcast soundtrack. To compensate for this time variance, the match process must make the time slices short enough so as the make the search engine time invariant. On the other hand, each time slice must not be so short that the match process would be too computationally intensive requiring a very fast processor. Analogously, if the time slice is too long, the pattern recognition search engine may not find any match whatsoever.

For each time slice, a feature calculation block 225 performs feature calculations. The feature calculation block 225 attempts to extract some usable feature for each time slice. Typically, the feature calculation block 225 performs some time domain to frequency domain transformation process. In one embodiment, the feature calculation block 225 performs a Fourier Transform on the data in each time slice. In another embodiment, the feature calculation block 225 performs linear predictive coding (LPC) on the data in each time slice. In still another embodiment, the feature calculation block 225 performs a power spectral density on the data in each time slice. However, the present invention is not limited to such time-to-frequency domain transformations. Other transformations as known to those ordinarily skilled in the art of pattern recognition search technology can be applied.

Based on the feature calculation for each time slice, a comparator block 226 attempts to find a match between each time slice from the audio clip submitted by the user and the time slices in the soundtrack database 211d (in FIG. 21). In one embodiment, a time slice associated with the user's audio clip is compared with each time slice in the soundtrack database. The calculated features in each time slice are compared to each other. The audio file in the soundtrack database that provides the closest match for this initial time slice results in the search engine producing a hypothesis where that audio file in the soundtrack database is considered a match. This hypothesis will be tested in block 227 as more time slices associated with the user's audio clip are compared to the soundtrack database. The check hypothesis block 227 creates a table or a list of soundtrack files that have successfully matched the time slices in comparator block 226. When the number of matches for a particular soundtrack file exceeds some "high confidence" threshold, then the particular soundtrack file is considered a match with high confidence. Alternatively, if a particular soundtrack file exceeds some "medium confidence" threshold (which is much less than the "high confidence" threshold) of matches and no more time slices are available for further comparisons, then that particular soundtrack file is considered a match with medium confidence. Similarly, if a particular soundtrack file exceeds some "low confidence" threshold (which is much less than the "medium confidence" threshold) of matches and no more time slices are available for further comparisons, then that particular soundtrack file is considered a match with low confidence.

Also, if a particular soundtrack file does not exceed the "low confidence" threshold and no more time slices are available for further comparisons, then the pattern recognition search engine will determine that no

match exists. Alternatively, the pattern recognition search engine may determine that a match with negligible confidence exists for this latter case.

5.1.5.3 System Operation

In this section, the recording of content will be described first, followed by the various redemption schemes. In general, a user need to merely press the record button on his electronic card when a TV commercial, TV program, infomercial, radio commercial, or radio program is being aired. However, to get any benefit out of this broadcast media interactive system, the broadcast content must have a corresponding soundtrack file in the soundtrack database 211d (in FIG. 21). Normally, the soundtrack can include the entire audio from the content, whether it's an hour-long drama, a two-hour long TV movie, a half-hour sitcom, or a thirty-second commercial.

The operation of the server in FIG. 21 can be done centrally or in distributive fashion. In the central operation scheme, only one website or entity would own and operate the server of FIG. 21. Accordingly, all users must come to this entity's website to request pattern recognition search services to obtain the coupons, incentive points, sales information or to be otherwise redirected to the proper website where the user can receive coupons, points, and sales information. Usually, the owner of the server of FIG. 21 negotiated some type of arrangement with a merchant (XYZ Corporation for ads, commercials, infomercials), TV network (e.g., ABC, CBS, NBC, Fox), cable service provider (e.g., AT&T Cable Services), satellite service (e.g., Direct TV), local TV station, local radio station, and the like. This arrangement includes placing the soundtrack of the program or the commercial in the soundtrack database for pattern recognition searching purposes. Without such an arrangement, the user can record any content he pleases but he will not be able to redeem it for any value in return.

In the distributed scheme, any web merchant, network, cable provider, local station (TV, radio, or otherwise), and the like can own and maintain its own server of FIG. 21. In this case, users would have to go to each web entity's website for service. If a user just recorded an audio clip of a commercial on CBS, he may have to go to the website of either CBS or the company associated with that commercial. In this distributed scheme, multi-entity arrangements may not be necessary.

For example, assume that CBS wants to increase viewership of certain TV programs. To utilize the various embodiments of the present invention, the electronic cards must be distributed to users so that they will use them when watching TV programs. CBS and/or other entities may provide for card distribution in any number of methods.

One method includes distributing these cards in the same package as another product. For example, in a joint venture with TV Guide Magazine, CBS and TV Guide distribute these electronic cards as a securely placed insert in the upcoming issues of TV Guide (with or without any additional price increase in the TV Guide). As another example, CBS and a certain XYZ Corporation agree to distribute these electronic cards in XYZ's compact discs (CD) in a joint venture to co-market CBS and XYZ Corporation's CD division. When a user purchases an XYZ CD, the CD package includes a free electronic card.

In another distribution scheme, CBS may limit distribution of these cards to some entity with a large membership base. For example, in a joint venture with AOL, CBS and AOL agree to distribute these electronic cards to AOL members only. AOL members would receive these cards in the mail. Similarly, VISA card holders may receive these electronic cards in the mail as a result of some arrangement between CBS and VISA.

In another distribution scheme, the major credit card organizations (i.e., VISA, Mastercard, American Express) arrange for its member issuing banks to distribute these cards to all new and existing card holders. In this arrangement, CBS has no involvement in the distribution, but rather benefits from having some other organization handle the distribution of the cards.

Whatever the card distribution scheme, assume for the purpose of discussion that these electronic cards are now in the hands of users. CBS would of course market the use of these electronic cards via print (e.g., newspapers, magazines) and electronic media (e.g., TV commercials, radio broadcasts, Internet newsgroups, CBS's website). CBS would also have some arrangement with the server of FIG. 21 to carry soundtracks of its programs and commercials in the soundtrack database 211d (in FIG. 21). Now, to increase viewership, CBS would market certain programs heavily. It mentions that by recording an audio clip of a CBS program (or relevant portion of a CBS program, such as the opening credits) or a commercial that appeared within a program's time slot, the user could redeem the recording to earn coupons to various merchandise, earn incentive points such as mileage with a popular airline, win free merchandise, or otherwise obtain some benefit. In this case, the broadcast media interactive system benefits both the sponsoring entity (e.g., CBS, TV Guide, XYZ Corporation) by increasing viewership or product purchase, as well as benefiting the user.

Redemption schemes will now be discussed. Basically, the redemption schemes include: (1) finding information that is related to or associated with the audio clip more quickly and easily than conventional Internet searching techniques; and (2) receiving coupons, incentive points, or other sales offers as a reward for watching that TV program/advertisement or listening to a particular radio broadcast/advertisement. These redemption schemes can be implemented on-line over the Internet or at a conventional store.

In the first type of redemption scheme, the user would take his electronic card, which contains the audio clip of a TV program or commercial, to his computer and access the Internet. The user initially recorded this audio clip because he was interested in a particular TV program (if his audio clip was some portion of the TV program), or some product or company (if his audio clip was of some portion of a TV commercial or radio commercial). The user wants more information about that program, an actor/actress of that program, the network itself (e.g., CBS) carrying that program, the product that was showcased in that commercial, or the company that makes/distributes that product in that commercial. However, the use of a conventional search engine might be too complicated, inefficient, or both when he tries to find the relevant information on the web. The electronic card facilitates his searching efforts.

When he accesses the website associated with the server of FIG. 21, the website then instructs the user to play the recording to his PC microphone. He plays the recording. When a match occurs between the user's audio clip and a file in the soundtrack database 211d (in FIG. 21), the server then redirects him to the relevant web page. Assume that the user was interested in a particular product in a TV commercial, the server redirects

him to the website of the company that makes or sells that particular product. In may cases, the user is directed to the particular web page that has the detailed information about that product to simplify the process for the user. The user need not be directed to a company website where he then has to wade through the tens or hundreds of pages of products that the company makes or sells. Rather, he is directed to the very page that has all the information that the user desires on that particular product. From here, the user can access information about the company that makes or sells that product, if desired.

Assume that the user is interested in finding more information about a particular actor who appeared in a television program. While watching that program, the user would record an audio clip of a portion of that program. He would then playback this recording in the manner described above as instructed by the website. The website associated with the server of FIG. 21 would then perform a pattern recognition search of the submitted audio clip. If a match occurs, the website would then redirect him to a web page that corresponds to the TV show he was watching. From this website, the user can then find links to the actors in this program, including the actor he is interested in, and access the linked web pages to obtain more information about that actor. If desired, the user can also obtain more information about the network that broadcast that TV show, the studio that made that TV program, or a whole host of other information related to that TV program.

Similarly, assume that the user recorded an audio clip of a TV commercial. In that commercial, the merchant advertised certain coupons or mileage points by going to his website and registering. The user takes the recorded audio clip, plays it to the server via his microphone across the Internet, and waits for pattern match. The server then informs the user that a match occurred (or no match), and redirects him to the merchant's webpage. Here, the user can register to earn his coupons or mileage points. In this case, the user's account balance is modified to reflect the earning of the mileage points. This account can be at either the website that the user was redirected to or the website of FIG. 21, where the account database 211e is maintained. This example is also related to the second redemption scheme. However, in this example, both the redirection and the earning of coupons or points occur together.

As another example of this second redemption scheme, the user takes his recorded audio clip in his electronic card to the website associated with the server of FIG. 21. When he plays back the recorded audio clip, the server performs the pattern match search and generates some match result. If a successful match results, the user with the proper account in the account database 211e earns the advertised incentive points, mileage points, or coupons. These earnings are reflected in the account database 211e associated with that user. The user can then redeem these coupons at any participating merchant and follow rules associated with their redemption, such as using the coupons prior to the expiration date.

As mentioned briefly above, the user can also take his electronic card to a conventional non-web store for redemption. Of course, the store sponsored the coupon that he saw (and recorded) on TV or radio or otherwise sells a product/service of another company that sponsored the coupon. Sometime after recording the audio clip with his electronic card, the user takes his electronic card to a kiosk, which is equipped with a computing station or terminal. The user activates the kiosk to prepare it to receive the coupon data. He then activates the playback switch on the electronic card to play the recorded audio clip. The kiosk receives the

information and delivers the audio clip to a server or computing system that contains the pattern recognition search engine and the soundtrack database. If the store is a national or otherwise chain-type store, this search function may occur at a designated network server that links other related stores. If the store is purely a local store, the search may be done locally at the kiosk or a network server that serves that particular store. If the search indicates that the coupon is valid (i.e., audio clip matches a soundtrack file), the kiosk may generate an actual paper coupon for the user to use at the checkout line.

In a variation of this embodiment, the user may also simply go to the checkout line at an actual conventional store (with or without any merchandise, depending on the coupon). At the checkout line, the store has a computer that also functions as an electronic cash register. Equipped with a standard sound device, the cashier asks the user to press his playback switch on his electronic card. He does so and the audio clip is transmitted to the store computer. This transmitted audio clip is now checked with the soundtrack files in the soundtrack database. Again, like the kiosk case above, if the store is a national or otherwise chain-type store, this check may occur at a designated network server that links other related stores. If the store is purely a local store, the check may be done locally at the a network server that serves that particular store. If the check indicates that the coupon is valid, the computer allows the user to redeem that coupon. If some merchandise is involved, the value of the coupon is applied to the purchase of that merchandise. If a free promotional item is offered, the item is given to the user without charge. Thus, based on the nature of the coupon, the action taken after the check will vary.

Similarly, the user may go to a kiosk or customer service station. When he plays the recorded audio clip, the kiosk or customer service station informs him the location of the merchandise associated with the recorded audio clip. The user can then find his item in that store with relative ease.

5.1.6 BOOKMARKS FOR BROADCAST MEDIA

In a variation of the content recording embodiment, the audio clip can be used to keep a "virtual bookmark" in the electronic card with respect to the broadcast content. Later, when he access the Internet, he can playback his recording at a central website. Once the pattern recognition functionality in that website finds a match, it directs him to the website associated with that recorded content.

Typically, when a user is watching television or listening to the radio, he may be interested in particular content that just aired. However, he has no easy momentary access to the Internet to look up that content. In some instances, even if he has easy momentary access to the Internet, he does not want to look for more information relevant to that content because he wants to continue watching/listening to the broadcast that is airing. In these cases, the electronic card can be used to record an audio clip of the broadcast. By doing so, he has stored a virtual bookmark to a web address.

Later, at his convenience, he can access the web and go to a central website. This central website has a pattern recognition functionality. When the user plays back the recorded audio clip, the pattern recognition software attempts to find a match. When it finds a match, this match is associated with a table that contains web addresses. At this point, this central website can redirect him automatically to this web address or simply display the web address for the user. This web address has more detailed information on the product/service

that was the subject of the broadcast he just recorded. If the broadcast was a commercial, the recording would allow the user to later be redirected to the webpage of the merchant associated with that commercial or even directly to the webpage of the product/service being advertised. If the broadcast was a TV program, the recording would allow the use to later be redirected to the webpage of the network or production company that produced that program, or even to a fan webpage of that particular TV program.

Multiple recordings can be stored in the electronic card so that in effect, the user is storing multiple "virtual bookmarks." They are analogous to bookmarks because web bookmarks on browsers allow the user to conveniently and quickly access a particular desired webpage without any searching. Similarly, the "virtual bookmarks" in the electronic cards allow the user to conveniently and quickly access a particular webpage without any searching effort by the user.

In another embodiment, the "virtual bookmark" can be used to make a realtime purchase on a home shopping network channel. When the user sees an item on the home shopping network channel that he wants to purchase, he records an audio clip while that item is on display on TV. The user would take this audio clip to his computer, access the home shopping network website, and playback the recording. When the pattern recognition software in the server detects a match, the user is given the option to purchase that item. Alternatively, the user could go to a central website where the pattern recognition feature redirects him to the home shopping network website based on the successful pattern match. Thereafter, the user navigates to the webpage containing the item or the redirection automatically takes the user to the webpage of that item.

5.2 SMART E-WALLET SYSTEM

In accordance with one embodiment of the present invention, a smart e-wallet application is provided which allows the user to use the electronic card in conjunction with a web browser to make on-line shopping faster and more convenient. Essentially, the smart e-wallet system according to one embodiment of the present invention allows the user to automatically launch a browser, send the user ID and password to the e-wallet server, and emulate the "fill" and "submit" buttons when the user is in a website's checkout line with the simple press of the switch in the electronic card. More details are provided below.

5.2.1 INSTALLATION

The smart e-wallet system comprises the e-wallet client software, the electronic card, software associated with the electronic card (DSP, sound card drivers, etc.) and an e-wallet server. The installation of the e-wallet client software and the electronic card software can be accomplished using standard methods. In one embodiment, the user would already have an electronic card that is sponsored by a merchant, portal, or some other entity that has an interest in distributing the electronic cards. The software installation process includes downloading the electronic card software from the website associated with the electronic card company and also downloading the e-wallet client software from the website associated with the e-wallet company. These two separate processes will now be described.

Referring to FIG. 29, a log server 296 and a registration server 295 are provided. In one embodiment, the log server 296 is operated by and associated with the electronic card company and the registration server 295 is operated by and associated with the e-wallet company. Alternatively, the log server 296 is operated by

and associated with an e-wallet company and the registration server 295 is operated by and associated with a typical web merchant. In other embodiments, both the log server 296 and the registration server 295 are operated and associated with a single company, whether electronic card, e-wallet, or web merchant/portal.

Typically, the servers are NT-based systems that use the IIS platform to handle Internet requests and feature a SQL server by Microsoft to manage and store the collected data. The log server 296 primarily handles user registration of the electronic card, installation of the software associated with the electronic card, and collects MIS data for later use and analysis.

As part of the registration and software installation process, the log server stores and updates a list of users and their corresponding electronic card IDs by name. Note that while the server knows each electronic card ID, it does not know or have access to the electronic card's secret key (i.e., MyEWallet password) which is generated by the hash function, as described further below in the security section of the patent specification. The log server also prepares the installation software and personal data file for each user. Finally, the log server stores and retrieves each user's usage characteristics.

To start the installation process, the user accesses a website that is associated with an e-wallet company, such as the website supported by registration server 295 in FIG. 29. The user may also be asked to provide other personal details including:

(1) full name (first, middle, last)
(2) email address
(3) electronic card number (or user ID)
(4) optional e-wallet profile name
(5) address 1
(6) address 2 (optional)
(7) city
(8) state/province
(9) zip/postal code
(10) home telephone number
(11) work telephone number
(12) interests/hobbies
(13) shopping preference
(14) household size
(15) household income
(16) Question for password
(17) Secret answer for password question

These are just representative information that the registration process requires. Some information may not be requested at all. In another embodiment, the user need not manually enter these information; rather, the information is stored in the electronic card itself and the mere activation of the card will provide this information to the server.

Since this registration server 295 is associated with the e-wallet company only, the registration server 295 takes the user to the log server 296, or the server operated by the company associated with the electronic card. After all, the e-wallet company provides e-wallet service and software to many different types of people, regardless of whether or not they have the electronic card of the present invention. The company associated with the log server 296 provides the service/software for the electronic card. Alternatively, the user may have gone directly to the website associated with the electronic card company first. However, as described above, if the user happens to go to the website associated with the e-wallet service first, that website will redirect the user to the website associated with the electronic card company.

The log server 296 delivers a registration web page that requires the user to enter the electronic card number. A dialog box can pop up to inform the user of the terms and conditions of the e-wallet/electronic card program. When the user agrees, the log server 296 delivers the software download page to the user. The user then downloads the software associated with the electronic card which can include the data file for personal information. An application file also includes a one-time code which is similar to the electronic card's transmission of the Series in the data stream. This one-time code is unique to each user and is used later in the smart e-wallet application for security purposes, as described further below. The user then subsequently installs the software using standard techniques, such as using an installation wizard program. The install wizard also tells the user how to install the microphone and test the microphone, sound card, and the electronic card. At this point, only the software associated with the electronic card is installed. This software is similar to software 114 of FIG. 11.

Finally, the installed software sends the user to the website associated with the e-wallet system. Here, the user name and password are entered by the installed software and the e-wallet client software is downloaded. The e-wallet client software can then be installed using its own techniques. The user is then notified that the installation of the smart e-wallet application has been successfully completed. The entire installation process takes only a few minutes (with a 33.6K baud modem).

Of course, the separate e-wallet company-sponsored registration server and the electronic card company-sponsored log server need not be two separate servers. Either, or both, companies can agree to operate a single server that provides registration for e-wallet and registration for the electronic card.

Alternatively, the user may purchase a disk or CD-based software package, which he then installs in the conventional manner. Also, the software could be bundled together with other pieces of unrelated software when the user purchases a computer from a store or directly from a manufacturer. Once installed, the user can proceed to the website associated with the e-wallet and/or electronic card and register.

The smart e-wallet system allows for multiple installations in multiple personal computers. Thus, a user could use the smart e-wallet system from the home and the office with a single electronic card. The installation procedure is as described above. However, a security mechanism is provided to ensure that the subsequent installations are legitimate. In the process of installing the software for the first time, the log server/registration server will provide the user three unique information options (i.e., question and answer). The user must provide a response to one of these options. In subsequent installations, the registration server/log

server will prompt the user with the same question. If the user provides a correct response, the server will allow the new installation to proceed.

5.2.2 OPERATION

An e-wallet is a convenient application that allows the user to shop and purchase items on the web with relative ease. Because the user had registered with the proper personal information such as name, address, phone number, credit card number, expiration date, and the like, the user's shopping experience is a painless and positive one. Indeed, this information may have already been entered by the card's provider. When the user is about to purchase some item at a website, he goes to the checkout line. Instead of filling out a form like he would normally do, he invokes the e-wallet application which contains all of his personal information. The e-wallet application would either fill out the form automatically for the user or deliver equivalent information to the website so that the sales transaction can be finalized.

Referring now to FIG. 29, the smart e-wallet application (which includes the e-wallet client software and the electronic card software) is a single tray application which is represented as an icon in the System Tray by the Windows OS if the application is active. Typically, the smart e-wallet application opens automatically on start-up. Of course, the user can turn off (i.e., close) the e-wallet application at any time after it has been opened by, for example, right clicking the tray icon and selecting "Exit." The icon will then promptly disappear from the system tray. Conversely, the user can manually open the e-wallet application from the Program Menu, or if a short cut has been provided on the desktop.

If the user has successfully registered with the e-wallet system (e.g., registration server 295 in FIG. 29), the user can use the electronic card 10 to gain instant access to a designated e-wallet "home" website and perform easy and secure purchases from that site. For the purpose of this patent specification, this designated "home" site is called MyEWallet.

First and foremost, the computer station 14 is powered up and running. Secondly, the sound system is also running properly and active. When the user clicks on the electronic card, the electronic card transmits a data stream which should be detected by the client software. The electronic card software portion of the smart e-wallet application checks for a valid transmission (i.e., user password). It the transmission is invalid, the user receives a security warning. If the transmission is valid, the smart e-wallet application performs any number of functions that is context-sensitive. For the most part, the smart e-wallet application checks the launch status (i.e., open or closed) of the web browser and the URL of the web page accessed. FIG. 30 shows a flowchart of this context-sensitive process.

The process starts at step 300. Step 301 checks to determine if the web browser is closed or opened. FIG. 29 shows a portion 290 of the computer screen that displays the web browser. If the web browser 291 (in FIG. 29) is closed, the smart e-wallet application launches the PC's default browser at step 302, accesses the MyEWallet website at step 303, and logs the user into the website (steps 306, 307). If the user is properly registered, the web page opened will be the user's personalized web page. The e-wallet interface 292 (in FIG. 29) will appear with the user ID and password automatically filled in by the smart e-wallet application as shown in step 306. Thereafter, the user ID and password are delivered to the MyEWallet website at step 307. If

proper, the user has now been logged into the MyEWallet website. The user can browser and shop as he pleases as indicated at step 308. At this point, the user's e-wallet which contains his personal information can be used to fill out a form or otherwise deliver these information to the website to finalize any sales transaction. Note that the smart e-wallet application fills in the user ID and password and submits them automatically to the MyEWallet server to log in. Thus, the mere press of the switch in the electronic card automates an otherwise manual process.

Returning to step 301, if the web browser is open, the smart e-wallet application checks the URL of the current web page at step 304. If the current URL is not MyEWallet, the smart e-wallet application opens another window at step 305, accesses the MyEWallet web page at step 303, and logs in the user as described above. As in the first case above, the smart e-wallet application fills in (step 306) and submits (step 307) the user ID and password automatically. At this point, the user proceeds with his web browsing and shopping in this second window. The previously opened first window is not associated with the smart e-wallet system so any tasks performed in this first window will not benefit from any automated tasks already performed by the smart e-wallet system. In another embodiment, the smart e-wallet system will access the MyEWallet web page and log in the user in the first window, without opening up another window. Thus, in this alternative embodiment, step 305 is eliminated.

Returning to step 304, if the browser is already opened to the MyEWallet URL but the user did not log in yet, the smart e-wallet application proceeds to fill in the user ID and password in the e-wallet interface 292 (in FIG. 29) at step 306, followed by submission of the user ID and password to the MyEWallet server at step 307. If proper, the user is logged into the MyEWallet system and can now take advantage of the e-wallet system.

Once the user is logged into the MyEWallet server, the next click of the electronic card performs other tasks. If the application is in the "fill" stage, the smart e-wallet application will fill out the form on the current web page, just as if the user had clicked on the "fill" button with the mouse. If the form is completely filled out, the web page would now be in the submit stage. The next press of the electronic card emulates the press of the "submit" button.

The user can, of course, fill out the form himself. If any portion of the form is filled out, the smart e-wallet application detects that the web page is in the "submit" stage. If the browser is already opened to the MyEWallet URL and the application is in the "submit" stage, the smart e-wallet application will submit the completed form on the current .html page to the appropriate server, just as if the user had clicked on the "submit" button with the mouse.

During these user transactions with web merchants and portals, the smart e-wallet application sends usage information to the log server 296. Specifically, whenever the electronic card is activated, the log server 296 gathers the following information:

(1) electronic card serial number (or individual ID)

(2) group ID (i.e., sponsoring web merchant or portal)

(3) server date and time

(4) PC date and time

(5) Counter value (or card click number)

(6) Action performed by card (e.g., open browser, login to wallet, press "fill" button)

(7) URL of the website visited by the user

These data can be used later to monitor user on-line behavior so that targeted marketing and advertising schemes can be employed. Additionally, if the user has some technical or other problems with the system, the appropriate customer service representative can assist the user more effectively with these stored historical data.

5.2.3 SECURITY

Generally, the e-wallet application in the client computer station performs two checks – (1) card signal is valid based on signal structure, and (2) card transaction is valid based on the counter value. These checks must be performed in realtime whenever a sound is detected by the sound system of the PC. In one embodiment, the client computer station checks both card signal transmission validity and card transaction validity. In another embodiment, the client computer station performs card signal transmission validity and a remote server performs card transaction validity.

The sound system, and in particular the microphone, is active in the computer station. Accordingly, any signal or noise can be picked up by the microphone. Noise or other random sounds should not trigger the operation of the e-wallet client application. To trigger the operation of this e-wallet system, a proper signal from the electronic card has to be detected.

As described above in the data format section of this patent specification, the electronic card transmits f0, f1, sync byte, known byte, the data, and the CRC, along with start and stop bits at every byte interval. The data portion consists of the individual ID and the Series (which is generated by applying DES3 encryption on the key, group ID, and counter value). The transmitted signal that is generated by the card has a unique structure, which the client software in the PC can use to detect a valid signal.

The e-wallet client software also has a table that was generated from a DES3 operation on the card signal so that the client can perform a pseudo decryption function. This table has the following fields – card signal, counter value, and user password. Also, the e-wallet application keeps track of the last counter value that was transmitted by the electronic card (and detected by the e-wallet application) as an additional check, as explained further below. In one embodiment, the table includes 3,000 possible card signals that could be detected by the e-wallet client software. Based on the various possible card signals, the table provides corresponding counter values and user passwords.

When a signal (or noise) is detected, the e-wallet application first determines if the signal is a valid electronic card transmission. If it is not a valid signal, the signal is ignored and no further processing is necessary. If, however, the signal is valid, the e-wallet application determines whether the card transaction is valid. The e-wallet application determines card transaction validity based on the counter value in the table based derived from the card signal structure. If the derived counter value in the table is greater than the counter value that was previously stored by the e-wallet system, then the card transaction is considered valid. Why?

The electronic card increments the counter value in the card each time the card switch is pressed. Thus, if the current counter value of my card is 24, this implies that I had pressed the card 23 previous times. This counter value of 23 is currently stored in the PC. When the user presses the electronic card, the counter value of 24 is transmitted to the PC and the card increments its internal counter value to 25. This 24th press of the electronic card is a valid transaction because the transmitted counter value 24 is greater than the stored counter value of 23.

If, however, an interceptor recorded the electronic card transmission while the user pressed the electronic card when the 24 counter value was transmitted, he may attempt to use this recording to break into the user's account. At this point, the PC's counter value is now 24 because the user had just transmitted the counter value of 24. If the interceptor attempts to log into the user's MyEWallet account by playing back the sound recording to the microphone, the sound recording would transmit a signal that included the counter value of 24. The PC's counter value is 24. Since the interceptor's signal's counter value of 24 is not greater than the PC's counter value of 24, the card transaction is considered invalid.

Once the card transaction is considered valid, the smart e-wallet application performs a two-factor on-the-fly authentication operation to generate a MyEWallet password. As mentioned above, the electronic card transmits a data stream which, for the most part, is constant except for the counter value. Accordingly, each transmission of the data stream in the electronic card contains a one-time code and the individual ID (or card serial number). Also, a one-time code is also generated by the server that provided the software download during the smart e-wallet application and provided to the client computer station. This one-time code is stored in the hard disk during the software installation and is different for each user. Upon determination of a valid transmission and a valid transaction, the smart e-wallet application takes the detected one-time code from the electronic card and the hard disk-stored one-time code and hashes them together to generate a MyEWallet password. In another embodiment, a simple XOR operation could be performed on the card's one-time code and the hard disk-stored one-time code to generate the MyEWallet password.

Multiple benefits are provided by this on-the-fly authentication scheme:

(1) Only the electronic card in accordance with the present invention can be used to log into the MyEWallet server and access the user's account. No other card can achieve successful authentication.

(2) Since the hashing function generates the MyEWallet password from both the electronic card's transmission and the one-time codes on the hard disk, the password does not "exist" in either location; that is, the MyEWallet password is neither in the electronic card nor the client computer station's hard disk. A hacker/virus will not be able to retrieve the electronic card's secret ID (or password) from examining the user's computer hard disk since the secret ID (and password) are not stored there. The secret ID and password are not stored in the application's .exe file. Similarly, even if someone stole the card, the MyEWallet password cannot be determined since the MyEWallet password is generated anew from the information from the electronic card and information from the computer station.

(3) Because of the use of the always incrementing counter value, the mere recording by an interceptor of one or more of the electronic card's transmission and the subsequent playback of that recording will not enable the interceptor to gain access to the smart e-wallet system. As described above, the smart e-wallet system only accepts card transactions with a counter value that is higher than the counter value stored in the smart e-wallet system.

(4) Because the one-time code transmitted from the electronic card is unique for every transaction, the user need not remember the password since the smart e-wallet system generates the password for each transaction.

In another embodiment of the present invention, the counter value is tracked by the log server. By doing so, a particular security problem associated with PC-based tracking of the counter value is eliminated. To elaborate on the problem, assume that the smart e-wallet application is installed and running in two PCs – one at home and the other at the office. One day, the home PC's counter value is 15 and the office PC's counter value is 14. The user uses the office PC to purchase various items on the web. As a result, the counter value in the office PC is now at 18. During the transaction where the counter value 17 was transmitted to the office PC, an eavesdropper recorded this card transmission. He could then take the recording to the user's home and if he somehow accessed the user's home PC, he could log into the smart e-wallet system and access the user's account. Why? The recorded transmission includes the counter value of 17. The home PC checks for a valid transaction by comparing the received counter value with the last counter value in the computer, which is 15 in this example. Since the received counter value (i.e., 17) is greater than the last counter value (i.e., 15) in the computer, the smart e-wallet system considers the transaction to be valid.

In contrast, a server-based solution to the tracking of counter value would eliminate this problem altogether. Because the server tracks the counter value, any recording of transmissions and subsequent playback would not enable the interceptor to access the MyEWallet account. The counter value in the recording would not be greater than the counter value in the server, regardless of which computer (office or home) is used. Similarly, this problem would not be an issue at all even if the PC kept track of the counter value if the user used only one computer for all transactions.

As mentioned before, the primary purpose of the authentication server is to authenticate users. To this end, the authentication server maintains a database of the following that information associated with each user: DES3 keys; counter values; electronic card individual ID (or card serial number); electronic card group ID; and other secure personal information such as user name, password, credit card number, credit card expiration date, and the like. When a user wants to log into the smart e-wallet system, the user presses the switch on the electronic card. This transmitted data is included in the request that is delivered to the server over the Internet. When this request is received, the server checks the individual ID (serial number) of the card transmission. Remember, the individual ID is not encrypted. The server then decrypts the data using DES3, checks to make sure that the individual ID is associated with the group ID, and then checks the counter value. Refer to FIG. 32 and the corresponding discussion below.

5.3 WEB TRANSACTIONS AND AUTHENTICATION

The use of the electronic card in accordance with one embodiment of the present invention provides many benefits for on-line web transactions. One problem with the current method of conducting sales transactions over the web is that merchants and banks are concerned about card presence issues. In other words, because the merchants and banks cannot get your signature on the sales transaction slip like conventional store purchases, the risk of repudiation of that sales transaction falls on the merchant. How do the merchants know that you are who you say you are and are using your card as opposed to someone else's card? If a sales transaction is repudiated, the merchant does not get paid; the credit card issuing bank loses some customer satisfaction; the acquirer bank loses some transaction cost for processing this repudiated transaction as well as experiencing some annoyance; and the relationship between the acquirer bank and the merchant can potentially deteriorate.

Generally speaking, the credit card fraud rules dictate that when a transaction is "card present," the risk of fraud falls on the issuer. In a conventional store purchase, the merchant processes the customer's credit card by checking with the issuer before completing the sales transaction. When the credit card is cleared, the merchant finalizes the sales transaction. This is done in realtime. On the other hand, when the transaction is "card not present," the risk of fraud falls on the merchant. Usually, these transactions are the telephone or Internet orders where the reliability of the credit card actually being present is low.

By using the electronic card of the present invention, the card presence issues are significantly reduced. With the appropriate client side and server side software, the only transactions accepted by the participating merchants, acquirer banks, and issuer banks are those involving the electronic card. The issuer bank (or even the credit card organizations) can require the merchant to only accept the electronic card of the present invention or else the risk of fraud falls on the merchant. Customers will no longer be able to merely type in the credit card number because these participating institutions will want some greater assurance that the credit card is present during the sales transaction.

For example, assume that a company JKL, Inc. is a web portal. JKL has been able to successfully sign on numerous merchants onto its website. In addition JKL has provided the electronic card of the present invention to all of its members. They instruct the member to use the electronic card for all sales transactions conducted on their portal or with merchants associated with the portal. With such an arrangement, the acquirer bank for merchant XYZ Company agreed to pay the merchant XYZ Company the full amount of all sales transactions conducted with the electronic card. This acquirer bank believes that the use of the electronic card minimizes card presence issues and the transaction is trustworthy. Similarly, the user of the electronic card is secure in knowing that his credit card number is not being broadcast throughout the web where it could be potentially intercepted and used elsewhere. He knows that purchases made with merchants associated with the JKL web portal are bona fide legitimate purchases that he made himself (or an authorized agent).

Similarly, a web merchant such as XYZ Company has a website. It provides the electronic card to all of its members. The company requires use of the electronic card to conduct sales of its items. It sets up this policy to protect its members from unscrupulous credit card thieves and to ensure that its acquirer bank will guarantee payment for all sales transactions. The risk of repudiation is low for the merchant.

The following sections provide details into the credit card infrastructure that the electronic card of the present invention supports, some on-line authentication applications, some off-line authentication applications, and other web-related applications.

5.3.1 CREDIT CARD INFRASTRUCTURE

Referring now to FIG. 31, a simplified diagram shows the relationship among the various players for credit card transactions. The customer 314 normally obtains a credit card from his issuer bank 313 (e.g., CitiBank). He may have obtained the credit card by filling out an application or the issuer bank pre-approved the credit card and sent it to the customer. Regardless, the customer 314 has an account with the issuer bank 313. For all his transactions with the credit card, the customer 314 receives periodic statements of his activities from the issuer bank 313.

The customer 314 purchases merchandise or some service from a merchant 311 whether web-based or conventional store-based. If cash is used, no credit card-related issues are raised. However, if the customer uses a credit card, the various parties shown in FIG. 31 are involved at some point or another. With the credit card, the customer 314 can purchase goods and services from the merchant 311. Sometimes, this sales transaction can be legitimate or illegitimate (e.g., stolen credit card). But for the most part, this sales transaction is usually finalized.

In order to be paid for a given sales transaction involving a credit card, the merchant 311 sets up an account with an acquirer bank 312. The merchant can select any number of acquirer banks to conduct its business. The acquirer bank 312 will honor the credit card-based sales transaction and pay the merchant 311 so long as the merchant 311 complies with the rules governing their business relationship. For example, the acquirer bank 312 may require that a signature of the customer 314 be provided on the sales slip. For web transactions, the acquirer bank 312 may require certain security signing authorities be used to decrease the risk of repudiation. The particular deal between the merchant 311 and the acquirer bank 312 can vary but usually involves a small flat fee per credit card sales transaction or a small percentage (with a cap on the actual dollar amount) per transaction. In any case, the acquirer bank 312 also makes some money out of the sales transaction between the customer 314 and the merchant 313.

Of course, the acquirer bank 312 ultimately gets paid by the customer's issuer bank 31, who in turn require corresponding payment from the customer, usually by check or money order. The issuer bank 313 also makes some money from the interest from customers 314 who do not pay the full amount of the credit card balance by the due date.

Governing the behavior of the issuer bank 313 and the acquirer bank is the government (not shown) and the appropriate credit card organizations 310, such as VISA and MasterCard. Of course, the government regulates the banking industry heavily to protect consumers and the banks themselves. The credit card organizations 310 control everything from the credit card itself (e.g., physical specifications, electrical specifications, logo placement, photo placement, embossing) to credit card readers and the communications protocol for on-line verification. Accordingly, the credit card organizations 310 place additional restrictions on the issuer bank 313 and the acquirer bank 312.

At times, a particular sales transaction can be disputed by the customer 314 because: (1) the sales transaction is legitimate but the customer cannot remember the transaction; (2) the sales transaction is not legitimate and of course, the customer cannot remember the transaction; (3) the sales transaction is legitimate, the customer remembers the transaction, and the customer still wants to dispute the transaction out of criminal intent; or (4) the sales transaction is legitimate, the customer remembers the transaction, and the customer disputes the transaction price. To resolve the dispute, the customer 314 can call the issuer bank 313. For low priced items, the issuer bank 313 typically credits the customer's account regardless of whether the dispute or the sales transaction is legitimate or not. In other instances, however, the issuer bank may resort to actual proof that the customer's signature is provided on the sales receipt. For web purchases, no signature is available to serve as such a proof. Any number of people with the credit card number could have initiated and completed that sales transaction over the web.

The electronic card of the present invention alleviates these card presence issues. Various card distribution models are possible within the framework of this credit card infrastructure. The electronic card can be distributed or otherwise sponsored by any of the following players: (1) merchant, (2) issuer bank, and (3) credit card organization.

First, a merchant, whether web merchant, web portal, or some other company with a web presence, can distribute the cards to its members and potential members. If this company does not get involved in the distribution of the electronic cards, it can sponsor the electronic cards instead. Thus, members can use the electronic card to purchase goods and services over the web at any website associated with this electronic card. Of course, if multiple merchants are sponsoring this electronic card, the member customer can use the electronic card at any website associated with these sponsoring merchants to make a purchase.

Similarly, an Internet Service Provider (ISP) can sponsor or distribute these electronic cards to its subscribers. In one embodiment, the ISP indicates to its subscribers the participating merchants that accept the electronic card as a means of payment. Initially, this list of participating merchants may be fairly limited but as more and more subscribers use the electronic card, more and more merchants will accept the electronic card as the payment means instead of (or in addition to) the conventional credit card.

In another embodiment, the ISP could set up the authentication server with the smart e-wallet system. The subscriber initially logs into the authentication server at the ISP and once authenticated, the subscriber can browse the web as usual and shop on-line. When the subscriber encounters a purchase form as a result of selecting a merchandise and going to the checkout line, the subscriber can use the form fill function of the smart e-wallet to complete the sales transaction. Refer to the smart e-wallet system description above.

Second, the electronic card could be distributed by the issuer banks 313 themselves. So, as customers 314 apply for credit cards, they receive these electronic cards instead. However, these electronic cards could be used like the conventional credit cards because the electronic cards comply with standard credit card form factor requirements. To the average customer, these electronic cards are no different from the standard conventional credit cards with the magnetic strip, logo and embossed name, credit card number, and expiration date.

Third, and related to the second point above, the electronic card could be sponsored by or otherwise supported by the credit card organizations (e.g., VISA, MasterCard, American Express). Thus, all issuer banks must provide electronic cards that comply with the requirements specified in this patent specification when distributing new or replacement credit cards to their respective member account holder customers.

In another embodiment, the issuer bank can bundle an online service membership with the credit card account. So, when a customer applies for a credit card, the issuer bank sends the customer the electronic card (which can also function as a conventional credit card with the magnetic swipe) and an automatic online service membership. The first use of the electronic card (when the user has accessed the online service company's website) could affiliate the user with the account. With this bundling, the online service provider could keep track of various user-related usage data. The online service provider could then send membership (and cardholder) usage data to the card issuer bank.

The principle advantages of this bundling scheme to banks is that they increase the frequency and depth of interaction with their cardholders. The effect is to heighten the cardholders' awareness of the issuers brand and services. This could lead to interesting opportunities, such as maintaining more detailed databases on use habits to help make more tailored offers of additional services to the cardholder. The increased presence of the card in users' everyday experiences could also lead to increased transaction volumes.

Moreover, the fact that users activate their cards more regularly than they would use a simple payment card leads directly to applications not otherwise possible. Issuers of cards under the present invention, by virtue of network servers used to authenticate the cards, can be made aware of when cards are being activated. Since the cards are being used in the context of Internet sessions, issuers may assume that cardholders will be present near their computers for some limited period following card activation. During that period of time, issuers can use the opportunity of a cardholder's presence to exchange useful messages with the cardholder. Exemplary messages include notifying cardholders of upcoming bill due dates, notifying cardholders of past due dates, and notifying cardholders of special promotional offers or discounts. Ideally, the cardholder would also provide a mechanism for the user to respond immediately. Because the issuer knows that the user has a card presence, the issuer can even use that opportunity to conduct higher risk transactions than they normally would in a card-not-present atmosphere. Because of the presence of the card, the issuer might, for example, allow balance transfers, withdrawals or bill payments to be paid online.

Another embodiment for increasing interaction between issuers and cardholders integrates the cards with "push" technology, such as is known in the art, for sending a priori messages to Internet users. At any point during an Internet session (whether or not a card has been activated but preferably after), alerts that call for card activation can be pushed out to the cardholder over the Internet. Exemplary alerts of this kind include notification of successful or unsuccessful bids for auctions or 'reverse auctions' (e.g. eBay, Priceline), as well as stock trading alerts. Through integration of "push" technology to the electronic card's client software, alerts can be conveniently delivered to the cardholder. As is known in the art, "push" technology can deliver such information as messages, content and patches to client software, without direct client request.

In one embodiment, a cardholder is pushed an alert, indicating that her bid to a reverse auction was not accepted. The user could then be prompted to activate their electronic card to authenticate their re-entry to the bidding system in one step. This scenario saves time in the re-bid process, and can reduce both customer drop-off rates in re-bidding, as well as re-bid repudiation. This scenario provides advantage over the current system of unauthenticated, email alerts. In another embodiment, the user is pushed an alert indicating their successful bid. The user could then be prompted to activate their electronic card in order to print a record of their successful bid.

In another embodiment, the integration of the card with push technology provides users with the opportunity to pay bills securely. The client software could be configured by the user or service provider to receive bill payment alerts from merchants, utilities or financial services. For example, bill payment and presentment services could push payment alerts to customers, to remind them to pay their telephone and electrical utilities bills. In a similar fashion, online financial service companies could remind users to make mortgage or margin payments, or to contact customer service regarding returned checks.

The user authentication functionality of the card enables secure payment of such bills in direct response to these prompts by operating a card.

5.3.2 ON-LINE AUTHENTICATION

In accordance with one embodiment of the present invention, the on-line authentication works in a manner similar to that of the smart e-wallet system described above. Generally, the electronic card interactive system can involve some checks locally at the client PC or remotely at the authenticating server.

For the local check, when the user presses the switch in his electronic card, the PC processes the signal and checks for electronic card transmission validity. If the structure of the signal detected by the PC's microphone and sound system is similar to that of the electronic card's signal, then the signal is presumed to be valid. Thereafter, the PC checks for electronic card transaction validity. Here, the PC merely checks whether the counter value in the signal transmitted by the electronic card is greater than the counter value last stored by the PC. If the transmitted counter value is indeed greater than the counter value stored in the PC, then the card transaction is presumed to be valid. In another embodiment, the counter check will occur at the authentication server, instead of at the local client PC. So far, the checks have only been made locally at the client PC. The remotely located authentication server will also perform checks of its own.

To perform the remote check, an authentication server includes a database, decryption facilities, and authentication logic. Refer to FIG. 32. The authentication process begins at step 320. The database includes the user names, DES3 keys, and other secure information (e.g., password, credit card number, expiration date, group ID, counter value, individual ID). Once the electronic card transmission passes the local client checks, the data from the electronic card transmission is delivered to the authentication server as an authentication request at step 321.

The data stream in the electronic card's transmission, which is included in the authentication request, includes an encrypted portion and an unencrypted portion. The encrypted portion includes the DES3 key, group ID, and counter value. The unencrypted portion includes the individual ID. The authentication server takes the

unencrypted individual ID and checks if a corresponding user is associated with that individual ID at step 322. If so, the authentication server decrypts the encrypted portion of the data stream at step 323. If not, the authentication server returns a security error message or a message otherwise indicating that access is denied at step 327 before ending at step 328.

At step 324, the authentication server checks if the group ID in the decrypted portion of the authentication request corresponds to the individual ID just verified. If that check is passed, the authentication server checks if the counter value in the authentication request is greater than the stored counter value at step 325. If not, access is denied at step 327. If the counter value in the authentication request is greater, then the authentication has been successful. The new counter value is then stored in the database associated with this user. This counter value check at the authentication server is in contrast to another embodiment where the counter value check occurs at the local client PC, as described above. Once the user has been authenticated, the authentication server returns a confirmation that indicates that authentication has been successful at step 326. This authentication process ends at step 328.

Once authenticated, the user is free to shop, purchase, and otherwise browse on the web. For e-wallet applications, the smart e-wallet application facilitates the form filling function in finalizing sales transactions. Smart e-wallet applications are provided above in the smart e-wallet system section. For other applications, the authentication process merely allows a user to access and other wise complete the sales transaction after pressing the TX switch on the electronic card. For example, once a user has shopped and selected an item to purchase from a website, the website delivers a purchase form to fill out. The user does so. However, instead of the credit card number, the user is asked to take out his electronic card and press the button. The user does so. When both the user's PC and the remote authentication server has authenticated the card transmission, the website will either return a web page that states "Thank you for your order. Your order number is 1234ABC" where the return confirmation message from the authentication server also finalized the sales (by emulating the "submit" button on the web page). Alternatively, a message is displayed indicating that the authentication process has been successful. The user then proceeds to submit the form manually and complete the sales transaction in the conventional manner.

This authentication model can be implemented in several different ways. The authentication server can be located or otherwise maintained and operated by several entities: (1) third party (e.g., private security based company, bank, or credit card organization), (2) merchant or web portal, or (3) ISP. These implementation strategies will now be discussed.

For the merchants, a convenient implementation strategy would involve some third party such as the hypothetical company RST Corporation which dedicates one or more authentication servers for various merchants. The third party could also be a bank (normally the issuer bank) or the credit card organization. Thus, the disruption to the merchants' web system would be minimized. Customers merely access RST's website to shop. When these customers have selected some merchandise to purchase, they merely take them to the checkout line on the website. Although the sales procedure varies from merchant to merchant, invariably

the customers get to a web page where they have to provide some personal details such as name, shipping address, and credit card number.

At this point, the customer is asked to take out his electronic card and press the button. When he does so, his PC handles the local authentication as described above. When he passes the local authentication checks, an authentication request is delivered to the IP address associated with the third party's authentication server location. Here, the third party's authentication server handles the authentication of this user. If authentication fails; access is denied and the merchant's server is notified in real-time of this condition. The merchant would then refuse this particular user's purchase request because, for various reasons, this user's account is delinquent, the account does not exist, the transaction is not valid because the counter value is not valid (perhaps the user was using a recording of another person's card transmission), the group ID is not valid, or the serial number (individual ID) is not valid. Alternatively, the merchant would assist the user in setting up an account.

If, however, the authentication server returns a confirmation to the merchant's server in real-time, the merchant's server would then allow the user to manually continue with the purchase process since the merchant deems this user to be present and in good standing. Alternatively, the confirmation from the authentication server to the merchant's server may also trigger the automatic completion of the sales transaction. The authentication request associated with the user pressing the switch on his electronic card essentially emulates the "submit" button that would normally be present in these sales forms.

This implementation strategy represents an advantage over the current on-line transactions because the merchants would receive transaction confirmation from a trusted source. This trusted source is the third party which not only confirms card presence during the sales transaction, but also checks various aspects of the account – from account delinquency to non-existence of the account. The frequent contact between the third party and the merchant and the added fraud-protection over conventional "card-not-present" transactions strengthen the relationship between the third party and the web merchant. If the third party is the issuer bank, the relationship between the web merchant and the bank would improve. For example, a credit card issuer of electronic cards under the present invention could offer to assume the risk of those "card-not-present" transactions only to merchants participating in the issuer's e-wallet, or e-commerce portal service. The effect would be raising the interaction with cardholders and transaction volume, without taking on real fraud risk, since the present invention provides adequate assurance that a transaction is, in actual fact, card-present.

For the second implementation strategy, the merchant and/or web portals themselves operate the authentication server independent of any third party. In this case, the database it maintains only keeps track of its own members. However, this implementation strategy may be less attractive to merchants who are more concerned with improving and maintaining their own content, instead of maintaining and operating an authentication server. However, it is a viable strategy for those merchants with the resources to support this separate server.

For the third implementation strategy, an ISP maintains and operates the authentication server. If only a few ISPs participate in this venture, only those subscribers in a region serviced by that ISP can benefit from the electronic card interactive system. To gain universal acceptance, many ISPs located throughout the world

must participate in this venture because web merchants are located across the web. However, it is possible to have the ISP authenticate the user when the user launches the browser. Upon accessing the ISP, the user will be asked to press the electronic card switch for authentication. Alternatively, the user will be asked to press the electronic card switch to launch the browser followed by other functionality in a manner similar to the smart e-wallet system described above. Thereafter, the smart e-wallet application will fill out any form for the user when he is about to purchase an item from a web merchant.

Ideally, the payment card associations (Visa, Mastercard, American Express, Discover, etc.) would agree that transactions effected by cards under the present invention were actually considered "card present," and honored to the same extent as any other card-present transactions. But also note that under any of these schemes for online authentication, those payment card associations need not make any change to their own transaction processing systems in order for merchants under the current invention to enjoy the benefit of card-present transactions. In the prior art, the payment card associations' systems are equipped to identify in real time whether a transaction is card-present (in store) or card-not-present (via phone or Internet.) Under the current invention, a merchant could be provided with evidence for its records that a transaction was effected not by manual entry of a card number, but by an actual transmission from a physical card. If a cardholder does not report a card lost or stolen, and then later attempts to repudiate the transaction, the merchant would have in his records good evidence that the transaction was genuine.

5.3.3 OFF-LINE AUTHENTICATION

In accordance with another embodiment of the present invention, off-line authentication works in a manner similar to that of the smart e-wallet system and the on-line authentication described above. The difference with the off-line authentication is that confirmation is not provided to the merchant in real-time.

In one embodiment, the confirmation would be sent to the merchants via email or through some other non-real-time means. In this way, the merchant and the customer could deal with each other in the conventional manner without waiting for the third party authentication server to complete the authentication check. But, before the merchant ships the merchandise or provides the service to the customer, the merchant would check to make sure the confirmation has been received. If the confirmation has been received, that sales transaction has been approved by the authenticating third party. If the confirmation has not been received, the merchant would hold shipment of the merchandise or otherwise refuse to provide the requested service. The third party could also keep the confirmation (or lack of confirmation) report for each sales transaction for future reference without affecting shipment or providing the service.

Like the real-time confirmation example described above, this embodiment represents an advantage over the current on-line transactions because the merchants would receive transaction confirmation from a trusted source, albeit in non-real-time fashion. This trusted source is the third party which not only confirms card presence during the sales transaction, but also checks various aspects of the account – from account delinquency to non-existence of the account. The frequent contact between the third party and the merchant and the added fraud-protection over conventional "card-not-present" transactions strengthen the relationship

between the third party and the web merchant. If the third party is the issuer bank, the relationship between the web merchant and the bank would improve. No major changes are required for the merchant's web site and the web server for the non-real-time authentication.

In another embodiment, the authentication server can assist those merchants who, for various reasons, do not want to make any changes to his system. The merchant may not even want to do the simple act of turning on the authentication flag in his server. Perhaps the merchant does not even want to perform any authentication. How do you provide authentication services to these merchants?

In this embodiment, the authentication server would place the confirmation number in a form field that is normally not used in most, if not all, of the purchase forms that websites require customers to fill out to place an order. In this embodiment, the ADDRESS LINE #2 would be used. This field is hardly, if ever, used by customers. In other webpages, a NOTES field is provided. The sequence of operations are as follows:

When the customer has selected an item to purchase on the web, he goes to the checkout line and encounters a form. He must fill out this form to place the order with the web merchant. In most of these forms is a field that is typically called "ADDRESS LINE #2." With the smart e-wallet application or other special client software that is designed for use with the electronic card, the customer takes out his electronic card and presses the button. The electronic card then transmits its data to the PC via the PC microphone. The client software delivers this data to a third party authentication server which performs the authentication in a manner described above. The authentication server then sends a transaction confirmation number back to the customer's PC client software, which fills in the ADDRESS LINE #2 field with this transaction confirmation number in the merchant's purchase order form page.

In one embodiment, the transaction confirmation number is merely a randomly generated number. In another embodiment, the transaction confirmation number is actually a digital signature of the order number and a public key. A digital signature is used to authenticate the identity of the sender (i.e., the third party authentication server) or the signer of the document. The use of the digital signature ensures that the signed document cannot be easily repudiated, cannot be imitated by someone else, and can be easily time-stamped.

A special merchant software can process all the purchase forms and associate customers with successful or unsuccessful authentication results. Thus, after completing the sales transaction, the third party authentication server places the transaction confirmation number on the purchase order form via the special client software located in the customer's PC. When the customer finalizes the sales, the purchase order form is submitted to the merchant. At the end of the day, the merchant has electronic versions of all the purchase order forms that have been filled out by customers as they purchased the merchant's products or services.

The special merchant software would process all the purchase order forms and decipher the transaction confirmation number provided on the ADDRESS LINE #2 field off-line. The special merchant software would then generate a report that indicates the success or failure of the authentication for each customer. The nature of the transaction confirmation number would provide this indication. The merchant can use this report to hold the shipment of the item purchased. Of course, the merchant would check with the customer to inquire why the

authentication failed and may even assist the customer in repairing the situation if the situation is reparable (e.g., insufficient credit limit, expired electronic card).

This embodiment of using the ADDRESS LINE #2 field represents an advantage over current on-line transactions because it provides merchants a transaction confirmation number from a trusted source. This transaction confirmation number indicates that the customer had the electronic card associated with a particular customer's credit card account present when he made the web purchase. Merchants can use this transaction confirmation number to validate the customer in real-time, if necessary, or any time thereafter. This information provides the proof necessary to counter later repudiations. This method prevents such fraud techniques as credit card number generators or stolen credit card numbers since the actual credit card number is not delivered over the Internet. Also, no changes are required in the merchant's web page or server.

In accordance with another embodiment of the present invention, some additional information is provided in the credit-card field in conjunction with the standard credit card number for authentication purposes. For example, a one-way card with an e-wallet software is provided. Whenever the user makes a purchase, he presses the button on the electronic card. With the button press, the card calculates the next number in a series, and sends it to the PC. The PC turns on the e-wallet engine and fills the address and credit card fields. However, instead of filling the regular credit card number, it fills a special code.

An exemplary code is designed as follows: 4 constant digits to designate the card number as a special kind, 6 digits for the card ID, and 6 digits of the card-sponsoring company's ID, and 6 digits from the pseudo-random series generated by the card (based on the counter value).

The merchant receives the card number and sends it through some channel to the acquirer bank as is typically done today. When the acquirer bank sees the special 4 first digits, he queries the server to checks whether the last 6 digits are valid according to the counter value. If two identical codes are received (same counter value), then a theft or some fraud has occurred, or if the code received is too old, then there was an attempt for theft. The server is located at the issuer bank and instead of listening for one credit number per user as is normally done, it listens for a unique credit card number per transaction.

5.3.4 PASSWORD GENERATOR

For this application, the electronic card and the PC client software are used to generate an ever-changing password to the user to access a web page. The electronic card contains a display for presenting the password to the user. The user then manually enters the newly generated password with the keyboard to enter the web page.

In this embodiment, the password generator includes the electronic card with a display, the special client software, the web browser, and the server that performs the authentication. Typically, the user browses the web and attempts to access a web page that he may or may not have an account with. If he has an account with this web page, he also has the electronic card provided to him by this merchant or some other sponsoring company that work. For various reasons, the access is limited to those users with open accounts and the electronic card. When the user requests access to this web page, the web page informs him that access is limited to members in good standing.

The web page asks the user to start the authentication process and when done, to enter the newly generated password before submitting the authentication form back to the website. The user enters his name (or ID) and perhaps a password. The server associated with this web page then sends an encrypted number to the user's PC via the web browser. This number is also accessible by the special client software. In another embodiment, the number is not encrypted. The special client software in the PC sends this number to the user via the PC speakers. This number can be based on the counter value or a randomly generated number. The counter value can be accessible by the server because the account database includes the counter value for this particular user.

The electronic card detects the encrypted number, decrypts it with its private key, and generates a password. This password is then presented on the electronic card's display. Concurrently, the web site server has also generated a password since the password-generating functionality is analogous in both the electronic card and the server. At this point, the user enters the password with the computer keyboard into the authentication form on the web page and submits it. When the server receives this password, it compares this received password to the password it generated internally. If a match exists, the user is allowed to access the web page. If a match does not exist, the user is denied access to the web page.

This approach provides several advantages over the conventional password-related approaches. Because the password is different for each transaction, the system is more secure. The user need not remember the password and even if one password was stolen somehow, that thief could not use it for another transaction. Also, the password does not exist in the electronic card, the PC, and the authenticating server for a long period of time. The password exists in the electronic card and the server for a short period of time. In the electronic card, the password is saved in RAM so when the electronic card powers down, the password is forever gone. In the server, the password exists for a short time (e.g., 5 minutes) that is just long enough for the user to log in successfully. Thereafter, the server discards the password immediately. In this configuration, the PC need not have a microphone since the user is not using the electronic card to directly transmit any data to the PC (or server). On a related note, the special client software does not need any special digital signal processing section to process any received signals since the electronic card will not be transmitting any signals to the PC.

5.3.5 CHALLENGE-RESPONSE

In another embodiment of the present invention, the merchant and user can employ challenge-response techniques to verify to each other's trustworthiness. Usually, one of the parties verifies that the other is indeed the party it claims to be for a given transaction. In some cases, however, both parties may want to verify each other for a given transaction.

In either case, digital certificates can be used. As known to those skilled in the art, a digital certificate is similar to an electronic "credit card" that establishes the certificate user's credentials when doing business or other transactions on the web. It is normally issued by a certification authority. The digital certificate contains the user's name, serial number, expiration dates, a copy of the certificate holder's public key, and the digital signature of the certificate-issuing authority so that the recipient of the digital certificate can verify that the certificate is indeed authentic and real. Some digital certificates conform to the X.509 standard.

FIG. 33 shows the sequence of steps of actions taken by the electronic card and the merchant in the case where the customer wants to verify the merchant. Initially, the merchant sends a digital certificate over the web to the customer. The digital certificate contains the date of expiration, name of merchant, signature of the certification authority (e.g., Verisign), and the merchant's public key. The customer's PC receives the digital certificate and in turn, transmits the digital certificate to the customer's electronic card. The electronic card contains standard logic and programming to perform a check to make sure the digital certificate is valid. In one embodiment, the electronic card checks to make sure that the digital certificate is signed by the certification authority and contains no errors. By verifying that the digital certificate is properly signed by the certification authority, the customer is making sure that no one is faking the information in the certificate.

At this point, the customer has the public key of the merchant. The customer can verify the merchant by sending a challenge and then testing the response to the challenge. The electronic card generates a random number. The customer transmits the random number to the PC. The PC then sends the random number to the merchant. The merchant signs the random number with the merchant's private key and sends the signed random number back to the customer's PC. The PC receives the signed random number and sends it to the electronic card. The electronic card checks the signed random number with the merchant's public key, which it obtained earlier. If the proper random number is recovered, then the merchant is presumed to indeed be the merchant it claims to be. The customer can now trust the merchant. Alternatively, instead of the customer sending a random number, the customer can send a digital certificate, which contains the ID and a public key. This certificate is sent by way of the certification authority.

Note that in this example, the party on the other side of the transaction knows the public key that matches the private key. The certification authority ensures that this public key belongs the merchant when the digital certificate has been delivered to the customer. To indicate a successful verification, the electronic card contains logic to sound an audible alert such as a ringing bell. If the verification is not successful, the electronic card can sound a different audible alert such as a buzzer.

In an alternative embodiment, the electronic card is not involved in this process. Rather, the PC performs all the steps that the electronic card is programmed to perform as shown in FIG. 33.

FIG. 34 shows the sequence of steps of actions taken by the electronic card and the merchant in the case where the merchant wants to verify the customer. For this case where the merchant needs to check the customer's identity to determine whether it can trust the merchant, a similar procedure is provided in the opposite direction. The customer's electronic card sends the card ID number (i.e., individual ID or serial number), the customer's public key, and a digital certificate. The PC receives this transmission and sends the card ID, the customer's public key, and the digital certificate to the merchant.

When the merchant receives the card ID, the customer's public key, and the digital certificate, it checks to make sure that it is a good signature from the certification authority. This provides the merchant with the assurance that no one is faking the card ID and public key.

The merchant then sends a random number to the PC, which retransmits it to the electronic card. The electronic card signs the random number with its private key and sends the signed random number back to the

PC. The PC then sends the signed random number back to the merchant. The merchant receives the signed random number and checks it with the customer's public key. If the check is proper, the merchant can be assured that it is dealing with the electronic card that it purports to be. The merchant can trust the electronic card.

FIG. 35 shows the sequence of steps of actions taken by the electronic card and the merchant in the case where they want to verify each other. In this embodiment, both the customer and the merchant check each other substantially concurrently. The electronic card sends a first set of data including the digital certificate, the card ID, the customer's public key, and a challenge (e.g., random number) to the PC. The PC retransmits the first set of data over the web to the merchant.

The merchant receives this first set of data and signs the challenge with the merchant's private key. The merchant then sends a second set of data which includes its own challenge, the response to the customer's challenge, and the digital certificate which contains the merchant's public key (among other data as described above). The customer's PC receives this second set of data and retransmits it to the electronic card.

The electronic card checks the digital certificate to make sure it was signed by the proper certification authority and the response to the customer's challenge (i.e., the random number originally sent by the customer and subsequently signed by the merchant with the merchant's private key). The customer checks the response with the public key that was just sent by the merchant as part of the digital certificate. If the response is proper, then the customer can trust the merchant. The electronic card then signs the merchant's challenge with the customer's private key and sends the response back to the merchant. In an alternative embodiment, the electronic card is not involved in this step of the process. In other words, the PC checks the merchant's digital certificate and the response to the customer's challenge with the merchant's public key.

The merchant then receives the customer's response to its challenge. The merchant checks the response with the customer's public key that was delivered initially. If the check is proper, the merchant can trust the customer.

In another embodiment, the electronic card can send back the response via conventional telephone systems. Thus, the merchant sends a challenge via the Internet to the customer's PC. The electronic card receives the challenge via the PC. The electronic card calculates the digital signature to sign the challenge and sends the response back via the conventional land-line telephone or cellular telephone system. In this embodiment, the acoustic signal is in the audible range. The merchant receives the response and checks it to make sure it is valid.

In another application, the use of the electronic card in chat rooms or message boards can prove invaluable in proving the authenticity of the user. Thus, the user would use the electronic card to log into the message board or chat room. The server would, of course, verify the identity of the user based on the electronic card and employing the techniques described above.

5.3.6 CRYPTO SERVICE PROVIDER (CSP)

As mentioned numerous times in this patent specification, the electronic card in accordance with one embodiment of the present invention should be compliant with the existing infrastructure. For Windows-based

systems, all web browsers and servers support client authentication by using Public Key Infrastructure (PKI), as known to those skilled in the art. Other exemplary merchant servers that support CSP include Apache, IIS, and Netscape Server. To use this authentication method, merchants need only turn on the "user authentication" flag within their server software, which requires selecting a button in a set-up menu.

Essentially, PKI allows users to send documents with digital certificates to prove that the user is indeed the user. The client authentication involves the use of cryptographic API (or crypto API), which provides an API between the various applications that are running in the user's client computer system (such as Microsoft Internet Explorer, Outlook Express, Word, etc.) and the cryptographic service provider (CSP) module.

As known to those ordinarily skilled in the art, CSP is a block of code distributed in Dynamic Link Library form that allows programs that are aware of it to connect and use its resources. Generally, CSP resources are essentially the hashing and encryption algorithms that it contains. Physically, each Crypto Service Provider (CSP) is a dynamic-link-library (DLL) with an associated cryptographic signature authorizing it for use by the Crypto API. One of the jobs of the CSP is to protect private key information from being exposed. Each CSP provides a different implementation of the Crypto API. Some provide stronger cryptographic algorithms than others. In addition to Microsoft, a number of third party developers have also released their own versions of Crypto Service Providers, each with its own unique set of ciphers, data formats and protocols. Indeed, two different providers may in fact include the same cipher algorithm but it would be incompatible due to different padding schemes, different key lengths, and different default modes.

Practically speaking, the CSP interacts with the user (and the user's applications in his client computer station) to allow the user to perform various security related tasks such as choose disk, give fingerprint (or voice print or biometric data), and the like. Because all web browsers and servers support it, the merchants who want a web presence are also required to support it. Thus, the CSP does not represent any change to the existing infrastructure.

In general, the CSP essentially enables the servers to ask the users to send digital certificates. The CSP in the client sends an unsigned digital certificate. The server which supports CSP receives the digital certificate and sends a random number back to the client to have it digitally signed. The client receives this random number and signs it with its private key and sends the signed random number back to the server. The server receives this signed random number and checks it with the client's public key for final authentication.

One drawback to this conventional approach is that the private key is held in the customer's client computer station. Thus, some hacker could theoretically break into that client computer station and steal private key. In accordance with another embodiment of the present invention, the private key is held in a third party CSP server. Referring now to FIG. 36, the electronic card sends its data (i.e., individual ID, group ID, etc.) to the PC. Similarly, the web merchant sends a random number (i.e., challenge) to the PC across the web.

The PC, through the CSP module, sends a digital certificate (which includes the customer's public key) and the electronic card data to a third party CSP server. This third party CSP server functions as a digital certificate signing facility and holder of private keys of all its members. This CSP server signs the digital certificate, signs the random number with the customer's private key, and then sends them back to the PC. The

CSP server also checks the data sent from the electronic card for "card presence" issues, which includes checking counter values and other parameters as described above in the On-Line Authentication section of the patent specification. The PC then delivers the signed digital certificate and random number to the web merchant who checks the signature with the customer's public key.

In an alternative embodiment, the digital certificate with the customer's public key could be sent directly to the merchant first. Thereafter, the electronic card sends the data and the merchant sends the challenge to the PC.

This scheme provides strong customer authentication without installing new server software. Cardholder privacy is also preserved because transaction information is not sent in real time to an Internet authentication server. With minor configuration changes to the existing software, merchants can confirm that a given electronic card was present in a particular transaction.

5.4 PLUG-IN APPLICATIONS

In accordance with another embodiment of the present invention, the special client software 114 (in FIG. 11) and works with one or more plug-ins in an integrated fashion. In one embodiment, the plug-ins are all subservient to the master special client software 114 (in FIG. 11). Thus, in addition to communicating with the electronic card, the special client software also manages the plug-ins. In another embodiment, the plug-ins are dominant over the special client software and can potentially perform more advanced and powerful functionality.

As known to those ordinarily skilled in the art, plug-ins or plug-in applications are supplementary programs to the user's web browser which assist the web browser to provide dynamic content that the web browser alone could not provide, such as playing sound or video. These so-called helper applications run as a separate application and require that a second window be opened. Plug-ins are easily installed and used with the web browser. A plug-in application is recognized automatically by the browser and its function is integrated into the main HTML file that is being presented. Exemplary popular plug-ins are Adobe's Acrobat, a document presentation and navigation program that lets user's view documents just as they look in the print medium; RealNetworks' RealVideo or RealAudio streaming media players, and Macromedia's Shockwave for Director, an interactive animation and sound player. Hundreds of plug-ins are available for download/install on the web or install via CD-ROM.

5.4.1 PLUG-IN SUBSERVIENT

In this embodiment, the special client software 114 (in FIG. 11) functions as the master or manager of the various plug-ins that are associated with the electronic card. These plug-ins are bidirectionally coupled to the special client software via the API layer. The special client software generally functions as described above – DSP for communicating with the electronic card, initialization, interaction with the web browser, interaction with the PC's sound system, etc. Additionally, the special client software basically provides the front end interface to the user and manages/launches the plug-ins when needed.

The plug-ins are generally sponsored by and/or written by various service providers, web merchants, or any company for that matter. By definition, these plug-ins are other software applications in the PC that are

called into service whenever the web browser, or in this case, the special client software needs them. Because these plug-ins are merely subservient support applications, their functions are controlled or otherwise limited by the special client software.

As the manager of the plug-ins, the main special client software keeps track of the group ID. As described above, the group ID is essentially the identifying number or code that represents the sponsoring entity, whether it is an individual, a company, or some other organization. For example, XYZ Corporation may sponsor a set of the electronic cards in accordance with the present invention to promote their website and product lines. They distributed the electronic cards to members and potential members so that they could use them to purchase products, request sales information, earn incentive points, obtain coupons and other discounts, and otherwise receive updated news about the company. Thus, XYZ Corporation is assigned a unique group ID that are provided in their electronic cards. Electronic cards sponsored by other companies will have their own respective companies' group ID. Theoretically, a user could have many different electronic cards just like some users have many different credit cards.

So, when the electronic card associated with a particular web merchant transmits some data to the PC, the special client software performs the DSP functionality to recover the data and checks the group ID. Based on the group ID, the special client software looks for the appropriate plug-in and enables its functionality. If the plug-in is outdated, the special client software will access a newer version of the plug-in over the web, download it, and install it. This may be done with or without the assistance of the user.

The special client software is equipped with additional functionality, because it is more than just a switch that routes the electronic card data to the proper plug-in based on the group ID. Assume that the special client software is sponsored by a particular bank, let's say the user's Visa issuing bank. This special client software associated can update and keep user passwords and IDs, check the user's credit card if it is delinquent, keep track of the number of times the user accesses the web, assist the user in navigating to the bank's home web page, assist the user in updating plug-ins, provide special offers to member users, scan other financial or other software in the PC and offer updates, retrieve email for the user, and numerous other functions related to the user's web experience with his bank. If a plug-in is necessary to view/hear content in a certain way, then the subservient plug-ins will be appropriately launched and enabled.

The kinds of functionality that can be supported by the plug-ins are limitless. Returning to the above example where the special client software is sponsored by the user's bank, the special client software may deliver the user to the bank's home page where, based on the content and various functionality programmed in that home page, the various plug-ins provide support, such as interactive buttons, sound effects, playing video, playing animation, and the like that are embedded on that web page. For example, a plug-in that provides the user with an interactive calculator to automatically calculate various aspects of his account may be provided. Furthermore, the user may be able to play a real-time video from the security camera at this bank with another plug-in. Another plug-in allows the user to send an email or message to various bank personnel to address questions concerning his account. If the user wanted to view one of his checks that did not clear, a document viewer plug-in is provided to assist the user in viewing that check.

Continuing with this example, another plug-in provides a message to the user via email whenever his account balance has reached certain thresholds (i.e., low threshold that incurs a charge) so that the user can take appropriate action. If the balance is too low, the user can quickly make a deposit or some other adjustments to his account so that he will not incur that penalty charge. Similarly, the user can have a plug-in that sends the user an email whenever anyone withdraws or deposits a certain threshold amount of money. These email or messaging plug-ins operate by automatically contacting the bank's web server, accessing the user's account, checking the account activity since that last time the plug-in logged in, and notifying the user of the activity (if any). The plug-in could send an email to the user's email address, or alternatively, display a message on the user's PC desktop in a manner similar to an active desktop.

In another embodiment, the plug-in associated with XYZ Corporation allows users to log into XYZ's website. In other words, the user takes out his XYZ Corporation electronic card and presses the TX switch. The electronic card transmits the data which includes the group ID and the microphone in the PC receives it. The data eventually makes its way to the sound card and then the special client software.

Based on the group ID, the special client software looks for the XYZ plug-in in the PC. If the plug-in is not available in the PC, the special client software accesses XYZ's website to download and install the latest plug-in. In the alternative, the special client software asks the user to download and install the XYZ plug-in. If the plug-in is detected, the special client software launches the plug-in, which then launches the web browser (if it has not been launched already). If the web browser has been launched, the plug-in navigates to XYZ's home web page. In another embodiment, if the web browser is already launched, the plug-in opens another window to navigate to XYZ's home web page.

At this point, the user is free to navigate anywhere on XYZ's website, or anywhere else for that matter. Note that the plug-in enabled the user to automatically log into the electronic card sponsor's (i.e., XYZ Corporation) website by the mere press of the switch on the electronic card. The master special client software steered the data to the plug-in associated with the group ID.

Another exemplary plug-in allows the user to log into a special members-only web page of the sponsoring web merchant/portal to obtain coupons, discounts, special offers, and other promotional items. Thus, if RST Corporation sponsored a particular electronic card and distributed the electronic cards to its members, the user of that electronic card could also log into a particular web page with the press of a button in the electronic card. On this web page are various promotional offers, discounts, and the like, which are available only to members of RST Corporation's website. The plug-in not only allowed member users to log into this special site but provided functionality that are optimized to view/hear certain information on this web page. Various interactive functionality on this web page are also made possible with the plug-in.

Another exemplary plug-in interacts with an electronic card that functions as a "voucher" or credit-limited card. The electronic card is then generic to multiple or many different web merchants. As users try to purchase merchandise with web merchant(s) that support this "voucher" electronic card, the plug-in checks the purchase to make sure that the user does not exceed his credit limit. Appropriate logic is provided in the plug-in to interact with the web browser to obtain the purchase price of an item so that the proper credit limit check can

be performed by the plug-in. If multiple web merchants support this electronic card, this generic plug-in can have different credit limits for each web merchant. If a credit limit is exceeded for a particular purchase, the user is notified with some dialog box and the purchase is otherwise cancelled. Thus, as the user navigates the web and attempts to make purchases, the plug-in checks each purchase to make sure the user is not exceeding the credit limit in his "voucher" electronic card.

If the electronic card is a multi-vendor card, the special client software determines which web page the user navigates to first in this subservient plug-in embodiment. If, however, the plug-in is dominant as described below, the plug-in itself determines which web page to navigate to first. This may create some conflict between or among competing dominant plug-ins.

5.4.2 PLUG-IN DOMINANT

In this embodiment, the plug-in is dominant over the special client software. In fact, the special client software merely provides the DSP functionality and checks the group ID to deliver the electronic card-transmitted data to the appropriate plug-in corresponding to the group ID. Beyond this, the special client software relies on the plug-ins for additional support.

In one embodiment, the dominant plug-in can be an application that is placed in the tray with an icon and is running concurrently. The dominant plug-in serves as the front end interface to the user. With this front end, the merchant associated with this plug-in can place advertisement, promotions, special offers, and other items that promote this web merchant's business. By being dominant over the special client software, the web merchant sponsoring the plug-in can write more code for the plug-in to provide more functionality. Indeed, the plug-in could be designed to operate with not only the electronic card described herein but other technologies as well, such as bar code readers.

Generally, the user takes out his XYZ Company's electronic card and presses the button. This data transmission results in the special client software detecting the group ID and enabling the XYZ plug-in to be launched. The XYZ plug-in now takes over, instead of the subservient plug-in embodiments where the plug-ins serve a more supporting supplementary role to the special client software.

Once again, the plug-in can provide various functionality such as messaging service associated with XYZ's website, delinquency information of the user's credit card, and provide ads and other sales information. Essentially, the exemplary functionality described above for the subservient plug-in are applicable for the dominant plug-in except that the front end is designed around the dominant plug-in. The special client software merely assists the dominant plug-in perform its tasks, i.e., by routing the electronic card transmitted data to the proper plug-in based on the group ID.

For both the plug-in dominant and plug-in subservient embodiments, the invention increases and enhances customer loyalty through electronic medium. By merely pressing the electronic card button, the web browser would open to a particular web page, whether it is the home web page of the company sponsoring the electronic card or the special client software. By going to this web page over and over again with the simple act of pressing the button on the electronic card, the user becomes more and more exposed to that web page's messages/ads/promotions. To increase the user's loyalty to this web page, the merchant sponsoring the

electronic card can offer incentive points to users for every visit to their web page using the electronic card. The plug-in can appropriately inform the web page whether the user accessed the web page through normal web browsing means or through the electronic card. Thus, even if the use had bookmarked various websites in the web browser, the loyalty program sponsored by this web merchant to promote the use of their electronic card will increase customer loyalty.

Additionally, the plug-in can navigate the user to the user's personalized web page on the web merchant's website or a particular community/interest group message board whenever the user uses the electronic card. In this way, targeted advertising, sales offers, discounts, and other coupons can be tailored to the user's specific interests/needs based on his past purchase decisions or the past purchase decisions of those group of people who are like the user (based on some statistical profiling scheme). Specific functionality needed by website can be provided by the plug-ins (e.g., playing sports game instant replay video/animation file for other community members to see).

5.5 POINTS/CASH PURCHASING MECHANISM

One embodiment of the present invention provides for a remote purchasing mechanism that involves the interaction of a consumer, a card issuer, and a web-based merchant. At the consumer end, an electronic card (or electronic card) and a client computer system are used. In the client computer system, a special client remote access software in accordance with one embodiment of the present invention is installed and running. In addition, a standard microphone, speaker(s), and a web browser are utilized. At the card issuer end, a card issuer server is provided to handle the consumer's account and authentication needs. At the merchant end, a merchant server or a server hosting the merchant's website is provided.

As a starting point for discussing one embodiment of the present invention, refer to FIG. 45. A consumer, who also has a membership with a card issuer 452 (to be explained further below), is equipped with a client computer system 451. The client computer system 451 has, among other things, a web browser which the consumer uses the surf the web and make purchases at various web-based stores. The web surfacing occurs on channel 457 with respect to this particular merchant server 453, which provides the product that the consumer wishes to purchase. When the consumer encounters a product that he wishes to purchase, he ultimately goes to the electronic checkout line of that particular web-based store. Normally, the web-based store, via merchant server 453, requires him to complete a form which asks for his name, shipping address, billing address, credit card number, expiration date of his credit card, and other personal information. Instead of manually filling out the form as usual, the consumer can use the secure purchasing mechanism in accordance with one embodiment of the present invention.

At the outset, the consumer is equipped with an electronic card 450 (or electronic card 450). The client computer system is a standard personal computer with a monitor operating on a Windows-based or Apple-based operating system. The electronic card 450 interacts with the client computer system 451 via medium 454. This interaction occurs to transfer the consumer's digital identification (ID) from the electronic card 450 to the client computer system to effectuate some transaction that is of interest to the consumer. The digital ID may be encrypted first in the electronic card and then transmitted to the client computer system 451.

After receiving the encrypted digital ID from the electronic card 450, the client computer system 451 opens another channel 455 to the card issuer server 452 which resides on the Internet and delivers the encrypted digital ID. The client computer system 451 may also send the URL of the merchant server in the same request or in a subsequent request. It accomplishes this using standard Internet accessing schemes by sending a request to the Internet with the uniform resource locator (URL) associated with the card issuer server 452. The card issuer server 452 is typically maintained and operated by a company that provides membership to Internet users and keeps member accounts of various selected currency. Thus, one card issuer may elect to provide frequent flyer miles to its members and allow its members to conduct sales transactions using the frequent flyer miles. Another card issuer may elect to provide incentive points to its members. Still another card issuer may elect to provide jelly beans as a form of currency to its members. Moreover, a card issuer may issue all these forms of currency. Whatever the currency, the card issuer company establishes and maintains an account database of its members. This account database includes name, shipping address, billing address, credit card number, expiration date, and digital ID. Of course, other information on the account holder may also be provided as necessary. The digital ID in the account is associated with the digital ID of the member/consumer that is programmed into the electronic card 450.

In addition to allowing the consumer to select the currency of his choice (that is also accepted by the card issuer), the card issuer also allows the consumer to allocate the amounts in that currency (and other currency) in any way that he desires for the purchase at hand. For example, assume that a book on a book merchant website costs $25. The consumer wants to buy that book but he wants to pay half in cash and the other half in accumulated incentive points at the current exchange rate. The card issuer server sends the credit card information to the merchant and subtracts (or credits) the appropriate number of incentive points from (or to) his account based on that day's exchange rate.

Having received the encrypted digital ID from the client computer system 451, the card issuer server 452 decrypts the digital ID, authenticates it, and references the account database to ensure that the digital ID corresponds to a valid member. In accordance with one embodiment, the card issuer server then opens up another channel 456 in the Internet and sends the credit card information of the member to the merchant server 453. The merchant server 453 processes the credit card information to finalize the sale and sends back a confirmation web page (which indicates that the sale is complete and typically provides a sales confirmation number) to the card issuer server 452. The card issuer server 452 then forwards the confirmation web page back to the client computer system 451. Alternatively, the merchant server 453 sends the confirmation page directly back to the consumer at the client computer system 451 via channel 457 without going through the card issuer server 452.

In another embodiment, the card issuer server 452 sends a confirmation back to client computer system 451 via channel 455 indicating that the digital ID is valid. The confirmation data may also include instructions and member profile data to the client computer system 451 to fill out the merchant's purchasing form. In another embodiment, the member profile data is stored in the electronic card itself so that no additional member profile data need to be sent back to the client computer system from the card issuer server. Having been

instructed to complete the form, the client computer system 451 completes the merchant's form in the web browser in automated fashion. The consumer then sends the completed form directly to the merchant server via channel 457. The sale is finalized in the conventional manner. In this case, the card issuer server 452 merely authenticates the consumer and delivers the confirmation back to the client computer system 451.

When the confirmation and instructions data are sent back to the client computer system, the special client remote access software in the client computer system opens up a second window (in addition to the window associated with the web browser). This second window provides the indication to the user of the confirmation. This second window also provides the user with the opportunity to select the desired currency for the sales transaction and specify the allocation (e.g., 40% cash and 60% incentive points for that particular purchase). When the user specifies the currency and the allocation, the information is sent back to the card issuer server, which processes the information by affecting the appropriate accounts. In one embodiment, the card issuer server then sends the credit card information to the merchant server. In another embodiment, the card issuer server sends the credit card information concurrently with the confirmation and instruction data, and the user and card issuer server negotiate for the currency and allocation later.

Note that with this secure purchasing mechanism, the card issuer can increase membership by appealing to the many Internet users who want to use alternate forms of currency to buy goods and services over the web. Additionally, because no special software is needed at the merchant server end, members can use their desired form of currency with any web merchant, unlike the past where consumers were limited to buying/redeeming points at the select few sponsoring merchants. With increased membership and usage, the purchasing mechanism of the present invention will improve and promote name branding of the card issuer's card or card issuer's service.

For the user, a purchase can be made with any web merchant with any desired form of currency (so long as the card issuer supports it). Additionally, because the data transfer from his electronic card to the PC to the merchant (via the card issuer) and back to the user is encrypted throughout the process, additional security is provided.

The special client remote access software performs multiple tasks that are important to the various embodiments of the present invention. During the initial stages of the user's on-line purchase, the special client remote access software processes the sound waves corresponding to the digital ID that have been emitted by the electronic card 10. After having been received by the microphone and processed by the sound card, the sound waves are processed further. The special client remote access software checks the encrypted digital ID sound waves to make sure that the data is complete and corresponds to the appropriate user's electronic card 450. After the check is completed, the special client remote access software opens another Internet channel to send a request to the card issuer server 452. The special client remote access software also sends the digital ID to the card issuer server 452.

During the next stage of the sales transaction, the card issuer server 452 sends back either: (1) a confirmation that the digital ID has been authenticated or no confirmation, or (2) a forwarded web page from the merchant server that indicates that the sale has been finalized with the proper confirmation number. In the

first case, the confirmation (or no confirmation) from the card issuer server includes instructions and data for the special client remote access software to complete the form that the merchant server requires for consummating the purchase. The special client remote access software then completes the form displayed in the web browser window without any intervention by the user. After automatically filling out the form, the special client remote access software is not involved any further in the transaction. The user interacts with the merchant server directly with his web browser to finalize the transaction.

In the second case, the card issuer sends the credit card and other relevant information to the merchant server. Thereafter, the merchant server finalizes the sales transaction with the information provided by the card issuer server and sends back the web page that contains the confirmation number of the order (and also some indication that the sale has been consummated such as "Thank you for your order. Your confirmation number is xyzabc123.").

In another embodiment, the electronic card is not needed. In other words, the user merely enters some digital ID with his keyboard. This digital ID is then encrypted and sent to the card issuer server, which processes this information as described above.

In summary, the various components of the system interact with each other to facilitate the purchasing process. The electronic card interacts with the special client remote access software via the client computer system's microphone to transfer a digital ID. The special client remote access software is capable of interacting with the speaker/microphone drivers in the client computer system for transferring the digital ID of the consumer, the web browser for transferring form data, and the card issuer server for authentication and other purchasing tasks. The card issuer server interacts with the special client remote access software for authentication and effectuating other purchasing tasks and the merchant server for delivering payment information. The merchant server interacts with the client web browser for standard web access and the card issuer server for transferring payment information.

The benefits to the card issuer are primarily two-fold. First, because non-conventional currency are permitted to be used by its members, membership in the card issuer company will grow and be very active in sales transactions. Second, the widespread use of the electronic card as a member of the card issuer company will promote name branding of the card itself.

The benefits to the consumer are also primarily two-fold. First, because data is encrypted throughout the entire link of the sales chain (from electronic card to PC to merchant and back), the purchasing mechanism is more secure than today's conventional method. Second, the user can use any desired form of currency (and in any amounts depending on how he allocates the cost) to make a purchase on the web with any web merchant, not just the few sponsoring merchants as he was accustomed to in the past.

5.6 BAR CODE READER

In another embodiment of the present invention, a portable bar code reader is used to scan bar codes to provide an effective link to the bar code's corresponding website for faster service. A couple of examples will be provided to clarify this embodiment.

Assume that a user purchased a merchandise from the store. This merchandise offers a $5 rebate if the

proof of purchase is returned to the manufacturer. In this embodiment, the user utilizes a portable bar code reader to scan the bar code of this merchandise instead to store the bar code in the reader.

The bar code reader can then be taken to the user's PC. After launching the web browser, the user takes out the bar code reader and presses the TX switch. The bar code reader then emits the sound which contains the data corresponding to the bar code. The structure and format of this sound signal is analogous to the sound signal described above in this patent specification. Part of the data in the bar code is the URL of manufacturer's website. The URL may correspond to the customer support web page, the technical support web page, or any other web page associated with the manufacturer of the merchandise.

When the special client software detects and properly decodes this signal, it provides the URL information along with any other data in the bar code (e.g., product serial number, model number) to the web browser which promptly navigates the user to the web page specified by the URL. Once at this web page, the user can then apply for the rebate by providing the name and shipping address. The manufacturer can then send a check in the amount of $5 for the rebate. Alternatively, the user can set up an account on this website so that his account can be credited.

As another example, the URL in the bar code can direct the user to a particular web site to get more information about that product, the manufacturer's other product lines, and other related sales information. The user may also earn coupons and other discounts for simply navigating to these web pages. The bar code represents a convenient way for the user to access the relevant web sites.

5.7 CARD-TO-CARD INFORMATION EXCHANGE

In another embodiment of the present invention, the electronic card is two-way card where the receiver is operational and waiting for signals when the power is on. In this embodiment, the electronic card contains user profile information. This user profile information includes name, company, title, email address, telephone number, and special interests (e.g., computer hardware, video graphics, software game developer). The electronic cards essentially communicate with each other to: (1) exchange information for storage, and (2) match two users (i.e., customer and vendor, or vendor and vendor) with similar interests.

In the first scenario, the action taken by the electronic cards is analogous to the exchange of business cards. To avoid collisions, though, the transmissions should occur at different time periods. As one user nears another user, the first user can press the TX switch to send the information to the second user. Then, the second user would press the TX switch to send his information to the first user. An audible alert (i.e., beep) would indicate when the transmission is complete (or the data storage is complete). This embodiment implies a manual operation.

Another embodiment is pseudo-automatic. When the first user nears a second user, the two users would each press the TX switch to transmit their respective contact information to the other. Instead of transmitting immediately, the two electronic cards would each determine some random time period. At the expiration of that time period, the electronic card would then transmit the information. Although both users may have pressed the TX switch substantially at the same time, the generation and use of the random time period ensures that, more often than not, the two electronic cards would each transmit information at different

time periods. Also, circuitry in the electronic card can be provided such that when one of the electronic card detects a valid electronic card signal from the other electronic card, and this electronic card's randomly generated transmission time period has not expired yet, this electronic card will not transmit the signal as long as it is receiving a valid electronic card signal. Even if the randomly generated transmission time period has expired, this electronic card will not transmit until all of the other electronic card's signal has been received and processed. Then, this electronic card will transmit its own information.

In both cases, an acknowledgment signal may also be implemented. In the first case, the electronic card will retransmit until the other electronic card sent an acknowledgment. Then, the second electronic card would transmit (and retransmit) until the acknowledgment signal was received by the first electronic card. In the second case, each electronic card generates a random time period. At the expiration of that time period, the electronic card will transmit the data to the other electronic card. Thus, using the randomly generated time periods for the transmissions, each card will continue to retransmit after each the expiration of each newly generated random time period until an acknowledgment from the other card is received and processed.

In the second scenario, the electronic card can be used as a means to match entities together – whether buyer-seller, vendor-developer, or employer-potential employee at a job fair. Thus, in one example, a potential buyer goes to a convention. At each booth, the vendor has a reader that can receive and process signals that are transmitted by the electronic card. When the user of the electronic card nears the booth, he presses the TX switch on the electronic card and the reader at the booth receives and processes the signal. If the company at this booth sells a product or is otherwise in a field that is related to the electronic card user's field or special interest, then the reader would indicate a match. The reader would send a match acknowledgment signal or a no-match acknowledgment signal to the electronic card. The electronic card would provide an audible alert that corresponds to the match or no-match acknowledgment signal, e.g., beep for match and buzz for no-match.

In all the scenarios above, the user can take his electronic card to his PC and later download the data therein. Either pressing another button or the same button in download mode (e.g., press twice in rapid succession) will cause the electronic card to transmit the data to the PC. The special client software could then process the data and store them in some usable format. Thereafter, the user could transfer the stored data in whatever application (e.g., Palm Pilot organizer) he desires.

5.8 WEBPAGE-DEPENDENT ACTIVATION

With thousands and thousands of webpages on the web, not every website will support the communications protocol of the present invention; that is, not all webpages are designed to listen for the electronic card transmission to perform some function or play an audio file that contains some data in a format that the electronic card of the present invention can understand. However, some websites support the communications protocol.

The user, however, is unaware of which website supports the communications protocol of the present invention as he navigates from one website to another. Two solutions to this problem are offered – (1) webpage provides indication, and (2) client station provides indication.

In the first solution, the website itself will indicate that it supports the communications protocol and

thus, the user will be able to take advantage of the electronic card's many benefits. A simple brand logo of either the card's sponsor or the card's manufacturer can be this indication. In other cases, a more lengthy explanation will be provided on the website – something of the form "This website supports the XYZ acoustic card. Please do not press the button on your XYZ acoustic card unless prompted to do so. We will provide some feedback to indicate that your transaction with the XYZ acoustic card has been successful." This instruction may be coupled with eye-pleasing graphics and other animation to make it clear to the user that the timing of the button press is important. Thus, as the user surfs the web, he will be alerted to those websites that support the communications protocol of the present invention.

In the second client station-based solution, the client station via the special client software will provide the indication to the user. In this embodiment, the special client software is installed in the client computer station. It is resident locally and is part of the System Tray set of applications. Normally, it is "asleep" in that it provides no apparent functionality to the user. However, it is operational and communicates with the web browser or whatever application is used to access the web. The special client software is installed in the client and "wakes up" whenever it detects a webpage that supports the communications protocol of the electronic card. This is accomplished by providing a code in the accessed webpage.

As discussed above, some websites support the communications protocol and others do not. This websites that support the communications protocol can embed a special code that is also known to the manufacturer of the electronic card. When the user accesses a website that has this embedded code, the special client software "wakes up" and alerts the user that this website supports the communications protocol of his electronic card. This alert can be a flashing icon on the Icon Tool Bar of the user's Windows desktop, a flashing or pulsating icon of the electronic card on the upper right corner of the screen, or some other visual or auditory cue. This tells the user that he can use his electronic card to conduct whatever transaction he has in mind on that site.

This special code can be provided as part of the header text. The code can also be used in conjunction with some logo or graphic on the webpage that indicates the exact type of electronic card supported. For example, the user has two electronic cards – XYZ Corporation's shopping card and a EZTrade Company's online trading card. At a particular website, the website indicates via some graphic that only the XYZ electronic card is supported.

In addition, different codes can be used in different webpages (or even in the same webpage) depending on the particular function that it supports. Perhaps a one particular webpage will fill out a form for the user when the user presses the button on the electronic card, while another webpage will authenticate the user to access his account. These context- and function-sensitive codes can be detected by the special client software so that the user's press of that single button on his electronic card will accomplish different things.

In a preferred embodiment, a single card can be used to interact with a large number of different web services. This makes a single card more useful to a cardholder. It also gives rise to an opportunity for card issuers to share in the revenues obtained by the service provider that makes the card-present authentication available. For example, assume that an online stock trading service finds this card-present authentication under

the present invention attractive enough that they will pay two cents to the authentication service provider every time a card is used to log in. As a way to encourage card use or adoption, the service provider could pass one of those two cents through to the issuer of the card used to effect that authentication. Ultimately, such revenue sharing could contribute to a "network effect" growing the demand for electronic cards, since all issuers and participating web services would be financially encouraged to keep their cards and services open to authenticating universally, and not just to their own services. Users under such a regime would benefit from the ability to use any card under the present invention to authenticate to any card-ready online (or telephone-based) service.

5.9 ELECTRONIC LOYALTY

Despite the advantage of money as a universally accepted means of payment, some consumers may not be willing to buy certain goods with money. Just as gamblers part with their money more freely when converted into "chips," consumers may be more willing to part with an alternative form of currency. "Points" are an example of a popular alternative currency used by many incentive award programs, as described below.

What are incentive award programs and how did they come about? Merchants have long realized that due to marketing costs, the first sale made to a customer is far more expensive (and thus less profitable) than ensuing sales. In order to maximize profits, most merchants work to build long-time relationships with customers, yielding ongoing sales with higher and higher profits. While many merchants would be willing to offer lower prices to entice particular customers to stick with them and not switch to competitors, this is often impractical and always expensive. Charging different customers different prices is difficult at many levels and even if it could be accomplished, giving the incremental profit back to the consumer defeats the merchant's goal in the first place. For this reason, incentive award programs were developed.

What is an incentive award program? Incentive award programs come in two varieties – loyalty incentives and attention marketing. Loyalty incentive programs award "purchase points" to those consumers who take certain purchasing actions. A classic loyalty incentive program provides a benefit to consumers who stick with or are loyal to a merchant and not switch to competitors, while "punishing" those who switch from brand to brand. Typically, an incentive is an incremental benefit that is worthless until enough points have been earned to redeem for a discount or a gift. Attention marketing programs reward consumers with "attention points" for paying attention to a marketing message.

The loyalty incentive program will be discussed first. A highly successful form of loyalty incentive award program with which many people are familiar is the airline mileage program, although non-mileage-based programs also are widespread. Mileage programs currently are conducted by almost every commercial airline. Travelers can earn mileage or mileage points by purchasing an airline ticket and actually taking the trip. The exact number of miles earned by the traveler is usually calculated by some formula based on the distance of the trip. After accumulating a certain number of miles or mileage points, the traveler can redeem his miles for a free or discounted airline ticket or some other award (e.g., coffee maker, free upgrades) that he can select from a catalog. The price-shopping, airline-switching fickle traveler would arguably not benefit (or not benefit sooner) than the traveler who is loyal to one airline.

Similar incentive award programs also have begun to flourish in an online environment over the Internet. Buyers can earn points online, for example, by purchasing goods from an online merchant, clicking on advertisements, filling out registrations and surveys, and performing various other activities of interest to merchants, advertisers and other companies. Users accumulate "points" into an "account" from which they can redeem their points for certain goods or services.

Even those consumers who are not regular online users or even familiar with the Internet may well be familiar with a variation of the point system. Many merchants award discounted or free merchandise to loyal and frequent customers. For example, by ordering a regular meal at a restaurant on ten different occasions (recorded on a stamped card), the customer may get 50% off the eleventh meal (or even get the eleventh meal free). Similarly, another merchant might give a loyal customer a free drink with his meal after every seventh or tenth visit. Another merchant might give $10 off the next purchase for a first-time customer. These variations on the loyalty incentive point system are just that – variations. Even though an actual physical card may be stamped after each visit to a restaurant or a gift certificate is handed out, these stamps and gift certificates are analogous to points, albeit in non-electronic form.

The tremendous power of loyalty incentives is this: the more points that a consumer has earned, the more the consumer wants points. Each incremental point is more and more valuable to the consumer because high point levels are associated with more exclusive (and valuable) benefits. So, the merchant benefits from the increased returns. The best customers are the least likely to switch to a competitor.

Although most point systems are still merchant-specific, more and more merchants are forming relationships with one another so that points are more universally accepted across different merchants, and thus more desirable to consumers. For example, purchasing goods from one merchant can result in earning points with another merchant. A consumer's use of his credit card might earn the consumer miles with Jones Airlines. Similarly, points earned through one merchant may be redeemable with another designated merchant. Thus, the consumer is no longer restricted to one merchant's catalog at redemption time.

But this is deceptive. Typically, points earned at an online store are usually not redeemable at a conventional bricks-and-mortar store, and voce-versa. Thus, the thousands of points earned at XYZ.com is worthless at the local department store. If a universal points database existed that allowed consumers to accumulate points and store points, much like a bank, as well as redeem them almost anywhere, consumers might be more motivated to participate in incentive award programs with greater frequency.

Thus, incentive award systems have demonstrated the viability of altering consumers' behavior if consumers perceive the points to be of value. Yet, the fixed-merchant nature and the inability to earn/redeem points between online and offline stores in existing incentive award systems often have limited the perceived value of points.

In accordance with one embodiment of the present invention, the Uniform Points System uses payment units, which can be in the form of actual points (and credit points) or cash (and credit). Uniform Points can be either purchase points or attention points. These points are part of a rewards system that rewards users who use the electronic card of the present invention. Although Uniform Points can be viewed as a separate form of

currency to purchase products, Uniform Points are better viewed as a means of building a mutually beneficial relationship between merchants and buyers. Thus, as users earn more and more Uniform Points, the users are rewarded with gifts and redeemable merchandise, while merchants are rewarded with more sales-generating traffic on their websites.

Although any form of payment unit can be used in the Uniform Points System of the present invention (including a mixture of cash and points), the patent specification will describe the embodiments with respect to points. However, one skilled in the art will recognize that the implementation details will be similar if money or alternative forms of currency were used instead of points.

How do users earn points? Participating merchants award Uniform Points to consumers, and allow for their redemption, in numerous ways. More importantly, these participating merchants have made these Uniform Points so universal that Uniform Points earned through one merchant can be redeemed with another merchant, and vice versa. Additionally, Uniform Points can also be converted into miles for many frequent flyer programs, and vice versa.

These Uniform Points can be earned in any number of ways, such as by registration, by purchase of product/service, and by viewing advertisements. The consumer is not necessarily required to visit any one website to earn points; rather, Uniform Points can be earned through any website or conventional bricks-and-mortar store that awards Uniform Points (i.e., those merchants with some relationship to Yahoo). Uniform Points can also be earned in other ways. Consumers can earn points from select merchants by:

(1) switching long distance carriers,
(2) updating user registration information periodically (to track changing interests)
(3) trying out a new service with an already existing membership,
(4) signing up for a new credit card,
(5) entering a merchant-sponsored sweepstakes,
(6) signing up for a trial membership to any merchant-sponsored club,
(7) playing online games such as poker, blackjack, and slots,
(8) answering questions for an online poll,
(9) trying a new product with no obligations,
(10) requesting a free quote on a vehicle,
(11) visiting a website (although some registration may be involved),
(12) writing and submitting product reviews (e.g., books, music, video),
(13) downloading software from a website,
(14) signing up a friend to some club membership,
(15) serving an online community by answering user questions,
(16) Points could be awarded as a multiplier (i.e., "Click here to double your points"),
(17) Points could be awarded offline as well (e.g., for using a shopping card at a supermarket), and
(18) purchasing a threshold amount of goods from multiple merchants.

This list is merely representative of the ways in which points can be earned. This list is not meant to be a comprehensive list. As mentioned above, these Uniform Points are universally accepted among the participating merchants. Thus, points earned through one merchant can be redeemed through another merchant. So, when a consumer earns 50 points through a music merchant by purchasing some compact discs, that consumer can redeem those earned 50 points with a pet supply merchant to purchase dog food. Of course, the music merchant may have one set of rules on how to earn these points and the pet supply merchant may have a different set of rules on how and when to redeem points and what thresholds are required for redemption. So long as these rules are observed, the consumer can use points like cash and apply them across different merchants.

Referring now to FIG. 47, the Uniform Points System will now be described. The central database 475 keeps track of points, gift certificates, and cardholder information. Points are as described above. Gift certificates are items that have a specific cash value that can be used at the gift certificate-sponsoring merchant's store, whether online or offline. Thus, a $20 gift certificate from XYZ Corporation is typically redeemable only at the XYZ store. The central database 475 can be considered a points/use database which keeps track of any online and offline card use, whether the card is used as a loyalty card (for earning and redeeming incentive points), a gift certificate, or an ATM card. Each registered user is associated with his own account for each of these uses. Usually, the central database 475 is periodically synchronized with each participating merchant's own account database, such as that associated with merchant account server 472 and 474. In other embodiments, the central account database 475 keeps the only copy of the account information so that the merchant's server 472 or 474 would have to access the central database to access any particular user's account information.

If the electronic card is used as a wireless acoustic card as described in this patent specification, the press of the button on the electronic card 470A triggers the transmission of a data stream. This data stream can be as simple as the card-specific digital ID. The user's PC 471 detects this data transmission and relays this card-specific digital ID (among other data described above) to the specific merchant's account and authentication server 472. Of course, the user may have automatically launched into (via the activation of the electronic card) or manually navigated to this merchant's website. The merchant's website would support the communications protocol of the present invention.

After performing whatever authentication tasks are needed, the server 472 accesses the account therein of the authenticated user. Based on the action taken by the user, the user's account is adjusted. For example, the user may have 50,000 points in his account and by the mere press of the electronic card button, he spent 20,000 points on a brand new color TV set. With this action, the central database subtracts the 20,000 points from this user's account. In another example, the user has an electronic card that represents a $20 gift certificate. The user accesses the merchant's website and uses $17 of this $20-valued gift certificate to purchase a CD. The central database adjusts this user's gift certificate account to reflect this purchase so that only $3 is now remaining. As a gift certificate, the electronic card of the present invention replaces the current paper gift certificates that merchants hand out.

Alternatively, the user could actually walk into a conventional bricks-and-mortar store and use the electronic card 470B. Because the current electronic card 470B has the traditional magnetic stripe on them, this electronic card could be used with any conventional magnetic stripe card reader 473. The authentication is performed via the merchant's account server 474 and the user's account is accessed via the central account database 475. This central account database 475 is the same database used for the non-magnetic stripe embodiment described above.

Thus, the versatile electronic card 470A/470B with the acoustic electronics and the conventional magnetic stripe makes it more attractive and convenient for the user to shop online and offline. On top of that, the central account database 475 increases the user's offline purchasing power through online purchasing actions, and vice versa. A user can shop online and earn incentive points. Because of the universally used central account database 475, these incentive points that were earned online can now be redeemed offline at any participating bricks-and-mortar store. The central account database 475 keeps track of any earned/redeemed points.

5.10 ADDITIONAL SYNERGIES WITH VOICE

The present invention's preferred communication method (data modulated on sound) gives rise to a number of convenient synergies when implemented with known voice technologies such as voice recognition and voice verification, Voice over Internet Protocol (VoIP). Generally, one of the goals of the present invention is to provide convenient, portable, physical authentication means for the Internet, in a known form factor used in the offline world, that does not require any infrastructure change unlike the traditional smart cards. The recent proliferation of voice applications for the Internet, such as voice recognition, and voice navigation for Internet browsers assures that sound infrastructure (microphones and speakers) are rapidly penetrating into all Internet platforms. The microphones being installed for those other purposes, generally speaking, are well suited for the card communications techniques described herein.

Generally, the strength of a security system is measured, in part, by the number and diversity of the security "factors" being required. Three such genres of security factors are commonly known as "something you know" (e.g. a password); "something you have" (e.g. a card, such as the reader-free electronic card described herein); and "something you are" (e.g. biometric measures such as voice.) For example, a password by itself may not provide complete security, because a holder may inadvertently disclose it, or the password can be guessed. A reader-free electronic card in accordance with the present invention can be lost or stolen. But when, as in accordance with various aspects of the present invention, a password is used as one factor, and the authenticated presence of a reader-free electronic card is used as another, security is enhanced.

For some applications, however, including high security transactions like extremely large financial transactions, there is no security factor equal in value to assuring that the correct person is present. Voice authentication as a biometric security factor is known in the art of computer security. Typically, these schemes will require the authenticating user to read arbitrary text, and then compare these vocal patterns to the authentic user's own speech patterns to verify conformity. One limitation of biometric security schemes, and voice authentication is no exception, is the requirement of special equipment to receive the biometric data (e.g.

fingerprint or iris readers, or microphones and sound systems for voice authentication). There are abundant known techniques for deploying voice authentication on a single computer, or over a network by sending voice sounds to and receiving authentication codes from, a network server.

But the fact that any issuer of the acoustic reader-free electronic cards of the present invention can be sure that each and every base station includes a microphone solves this barrier to introducing voice authentication as a security factor. Thus, one embodiment of the present invention enables the proprietor of a security system to deploy a regime including the "something you have" factor in the form of a card or other physical token practicing the acoustic data transmission techniques discussed above, plus any combination of a password or other "something you know" factor, plus biometric verification by voice authentication.

Lack of perceived security and a lack of user trust remain the principal deterrents to people adopting habits of shopping and doing commerce online. Because the base station described above includes a microphone and sound system, increased personal relationship and trust can be established under the present invention by requiring presence of a reader-free electronic card, and adding the personal attention of speaking with live people using VoIP techniques.

Major banks are moving to increase adoption of their online account services. Online banking represents a significant cost savings over in person banking at branches, and even telephone banking. But customers may hesitate to conduct banking activities online because over the Internet, no particular customer service representative can interact with shoppers directly. But known VoIP systems enable voice-based conversations with the other persons visiting a particular website, or with customer service representatives manning that site.

Under the present invention, when combined with online banking or other secure online services, an acoustic electronic card can be activated to enable various functionality within the sound infrastructure. The customer learns to trust the Internet and his transactions therein because of the guaranteed "card presence" transactions that are accepted by online merchants/financial institutions. Furthermore, conversations can be recorded for resolving non-repudiation issues for online banking and other conversations with merchants. The user can also choose his desired customer service representative. In the non-financial Internet world, one embodiment of the present invention allows authentication and limited audience chat plus voice chat in a message board or chat room.

6.0 NON-ACOUSTIC EMBODIMENTS

Instead of acoustics, another embodiment of the present invention uses radio frequency (RF) and magnetic field transmission/reception techniques to couple the electronic card and the client computer station.

For RF, data from the PC to the electronic card is transmitted using VHF or UHF frequencies. These high frequencies can be achieved by software manipulation at the PC. The CPU of the PC uses its data-address bus as the transmission antennas and modulating signals on the bus. The electronic card receives and decodes these signals with standard RF decoding circuitry. Alternatively, the PC can employ On-Off RF modulation by halting and restarting the CPU. The electronic card receives and decodes these signals with standard RF decoding circuitry.

For magnetic field, the PC speakers transmit the data from the PC to the electronic card. However, instead of picking off the audio signal, the electronic card picks up the magnetic field created by the speakers and their wires which are present when the audio is played. The pick-up element in the electronic card is a loop antenna.

6.1 RADIO FREQUENCY (RF)

Instead of acoustic signals, the client computer station (e.g., personal computer) can generate RF signals to the electronic card. With appropriate RF decoding circuitry, the electronic card can receive and decode the RF signals to process the data therein. Again, no additional hardware would be necessary in the PC to generate the RF signals.

The unique RF transmission technique in the PC involves using the address-data bus as the transmission antenna and the CPU as the oscillator. The PC currently generates electromagnetic signals because the electronic circuitry in the PC applies voltage to the various buses causing current to run along the wires. The electromagnetic signal is RF in nature because the PC's microprocessor speed is typically in the RF range (tens to hundreds of MHz). The microprocessor's speed is typically 100-450 MHz, although more and more new PCs are being sold with microprocessors in the gigahertz range.

As known to those ordinarily skilled in the art, the main frequency component of an RF signal is at the base carrier frequency. For a microprocessor at 100 MHz, a lot of the signal's power is present at 100 MHz. Signal power is also present at other frequencies which are whole number multiples of the main base frequency. Thus, some signal power is present at 50 MHz (multiple of 2), 33.33 MHz (multiple of 3), 25 MHz (multiple of 4), 20 MHz (multiple of 5), and so on. However, the higher the multiple, the less likely that the RF signal will have a frequency component at that corresponding frequency. Thus, at a multiple of 100, the chance that some frequency component would exist at 1 MHz is low. In some embodiments, appropriate division is performed to obtain the FSK frequencies from the higher RF frequencies.

The first step is to select the frequency of the RF transmission. In the FSK scheme utilized in this invention, the two frequencies are approximately 1 kHz apart. So, for example, one frequency can be 10.7 MHz while the other frequency is 10.699 MHz. The period of these frequencies would also have to be determined. Thus, for the frequency 10.7 MHz, the period is 93.4579 ns.

The next step is to determine how much time an instruction takes. Based on this instruction time and the frequencies selected above, the number of instructions needed for the whole period for each frequency can be determined. If frequency 10.7 MHz is selected for one of the RF frequencies, the number of instructions to fill up the above-calculated 93.4579 ns period would also be needed.

The PC's CPU itself will modulate the address-data bus for the desired frequency. In the above example, since 10.7 MHz was selected as one of the frequencies for transmission, the CPU will apply a logic "1" to the bus for half the period and apply a logic "0" for the other half of the period. The length of these logic "1" and "0" values that are applied to the bus can be controlled by the number of instructions that are delivered to the microprocessor since the time duration of each instruction is known. Accordingly, an RF frequency component will exist at 10.7 MHz in the above example. For longer periods (for lower frequencies), more

instructions are delivered to the microprocessor. For shorter periods (for higher frequencies), less instructions are delivered to the microprocessor.

At the electronic card, appropriate RF decoding circuitry can be employed to receive and decode the RF signals. Referring to FIG. 37, a high level view of the RF decoding circuitry in the electronic card is provided. In this design, off-the-shelf RF IC's are used. The transducer 370 receives RF signals and converts them to workable voltage levels. The pre-amplifier and bandpass filter 371 amplify and clean up the signals for further processing. In particular, the pre-amplifier portion of the unit 371 is a high input impedance amplifier. The bandpass filter portion of the unit 371 filters the signal in order to attenuate speech (or noise) signals. The RF signal is presented to the FM intermediate frequency (IF) unit 372. A quadrature network unit 374 is provided for frequency decoding using quadrature demodulation. Finally, the microprocessor unit 373 in the electronic card accepts the digital demodulated FSK signal, or in the alternative, an analog voltage that is correlated to the input frequency.

FIG. 38 shows an alternative embodiment. The transducer 380 receives RF signals and converts them to workable voltage levels. The RF signal is presented to the FM intermediate frequency (IF) unit 381 for filtering. The bandpass filter 382 cleans up the signals for further processing. The filtered RF signal is presented to the FM intermediate frequency (IF) unit 383 for further filtering. A quadrature network unit 385 is provided for frequency decoding using quadrature demodulation. Finally, the microprocessor unit 384 in the electronic card accepts the digital demodulated FSK signal, or in the alternative, an analog voltage that is correlated to the input frequency.

In the electronic card to PC transmission, the microphone in the PC can be used as the receiving antenna. However, the frequencies selected for the RF signal should be in the frequency range supported by the sound card in the PC. If the RF signal is in the 10 mV range, the sound card in the PC can detect it and process it as audio signals even though the transmission was via RF.

This embodiment provides several advantages. By using RF signals, the DSP software is much simpler in the electronic card. RF signals are much stronger and easier to process than acoustic signals. Lots of standard RF components are available in the market at lower cost. The use of RF avoids most acoustic-related issues, such as echo cancellation, range, and interference. The use of RF signals also result in higher bit rates. Also, in the PC-to-electronic card transmission direction, the sound card drivers in the PC need not be checked. In fact, a sound system in the PC is not needed at all for this PC-to-electronic card transmission direction.

6.2 MAGNETIC FIELD

In another embodiment of the present invention, the interactive system uses magnetic fields. When audio is played by the speakers, the currents created by driving the speakers are not negligible and thus induce a significant magnetic field. This magnetic field is generated by the speakers and the wires. However, these magnetic fields drop off significantly by a power of 3 so distance from the source of the magnetic field is important.

To pick up the magnetic field, the electronic card must be reasonably close to the source of the magnetic field, i.e., speakers and wires. Referring now to FIG. 39, the electronic card employs a loop antenna

390 instead of an acoustic transducer to pick up the magnetic field. Because the received the magnetic field induces a current in the loop antenna, a current-to-voltage converter 391 is provided. The remainder of the components are similar to that for decoding acoustic signals. In particular, the gain and bandpass filter 392 filters the signal for further processing. An AGC block 394 is provided for SNR improvement. The final processed signal is provided to the microprocessor unit 393 for data processing.

With respect to power, a conventional small-sized battery such as Varta LPF-25 is used. In some other embodiments, electronic card power is obtained from the PC via the Hall effect. The electronic card merely has an antenna with which to pick up signals for processing.

The foregoing description of a preferred embodiment of the invention has been presented for purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise forms disclosed. Obviously, many modifications and variations will be apparent to practitioners skilled in this art. One skilled in the art will readily appreciate that other applications may be substituted for those set forth herein without departing from the spirit and scope of the present invention.

What is claimed is:

CLAIMS

1. A one-way portable device, comprising:

a device body that has a thickness less than 0.8 mm and a switch;

memory logic for storing device information; and

transmission electronics coupled to the switch that emit a wireless signal based on the device information in accordance with a first data format when the switch is activated.

2. The device of claim 1, wherein the wireless signal is an acoustic signal.

3. The device of claim 2, wherein the acoustic signal is an ultrasound acoustic signal.

4. The device of claim 1, wherein the wireless signal is radio frequency (RF) signal.

5. The device of claim 1, wherein the wireless signal is a magnetic signal.

6. The device of claim 2, wherein the first data format further comprises:

a first frequency shift keying (FSK) portion to identify a first frequency in a FSK signaling scheme;

a second frequency shift keying (FSK) portion to identify a second frequency in the FSK signaling scheme;

a synchronization portion for facilitating the proper reception of the wireless signal;

a known portion that both the portable device and a targeted receiver of the wireless signal knows;

a data portion comprising various combinations of the first frequency and the second frequency to represent the device information; and

an error checking code portion to allow some targeted receiver to check for errors in the received data.

7. The device of claim 6, wherein the first data format further comprises;

start and stop bits inserted in selected locations between the first FSK portion and the error checking code portion.

8. A two-way portable device, comprising:

a device body that has a thickness less than 0.8 mm and a switch;

memory logic for storing device information;

reception electronics for receiving wireless signals; and

transmission electronics coupled to the switch that emit a wireless signal based on the device information in accordance with a first data format when the switch is activated.

9. The device of claim 8, wherein the wireless signal is an acoustic signal.

10. The device of claim 9, wherein the acoustic signal is an ultrasound acoustic signal.

11. The device of claim 8, wherein the wireless signal is radio frequency (RF) signal.

12. The device of claim 8, wherein the wireless signal is a magnetic signal.

13. The device of claim 8, wherein the first data format further comprises:

a first frequency shift keying (FSK) portion to identify a first frequency in a FSK signalling scheme;

a second frequency shift keying (FSK) portion to identify a second frequency in the FSK signalling scheme;

a synchronization portion for facilitating the proper reception of the wireless signal by some target receiver;

a known portion that both the portable device and some targeted receiver of the wireless signal know;

a data portion comprising various combinations of the first frequency and the second frequency to represent the device information; and

an error checking code portion to allow some targeted receiver to check for errors in the received data.

14. The device of claim 13, wherein the first data format further comprises;

start and stop bits inserted in selected locations between the first FSK portion and the error checking code portion.

15. A method of transmitting a data stream from a portable device, said data stream including device information in the portable device, comprising steps:

preparing a synchronization portion for facilitating the proper reception of the data stream by some target receiver;

preparing a known portion that both the portable device and some targeted receiver of the wireless signal know;

preparing a data portion to represent the device information; and

preparing an error checking code portion to allow some targeted receiver to check for errors in the received data.

16. The method of claim 15, wherein the preparing the data portion step includes:

reading a counter value from a counter;

assigning a group ID and an individual ID to the portable device;

assigning a secret key in accordance with asymmetric crypto systems; and

calculating a series by applying a first cryptographic algorithm to the secret key, the group ID, and the counter value.

17. The method of claim 16, wherein the first cryptographic algorithm is Data Encryption Standard (DES3).

18. The method of claim 16, wherein the preparing the data portion step further includes:

incrementing the counter value in the counter.

19. The method of claim 18, wherein the preparing the data portion step further includes:

combining the series and the individual ID.

20. The method of claim 19, further comprising step:

placing the synchronization portion, the known portion, the data portion, and the error checking code portion into a send buffer.

21. The method of claim 20, further comprising steps:

transmitting a first frequency shift keying (FSK) portion to identify a first frequency in a FSK signalling scheme; and

transmitting a second frequency shift keying (FSK) portion to identify a second frequency in the FSK signalling scheme.

22. The method of claim 21, further comprising steps:

transmitting a start bit;

transmitting a selected segment of the send buffer; and

transmitting a stop bit.

23. The method of claim 22, further comprising steps;

determining if any more segment is remaining in the send buffer;

if a segment remains, transmitting a start bit;

transmitting the selected segment of the send buffer; and

transmitting a stop bit.

24. The method of claim 16, wherein the individual ID includes a credit card number.

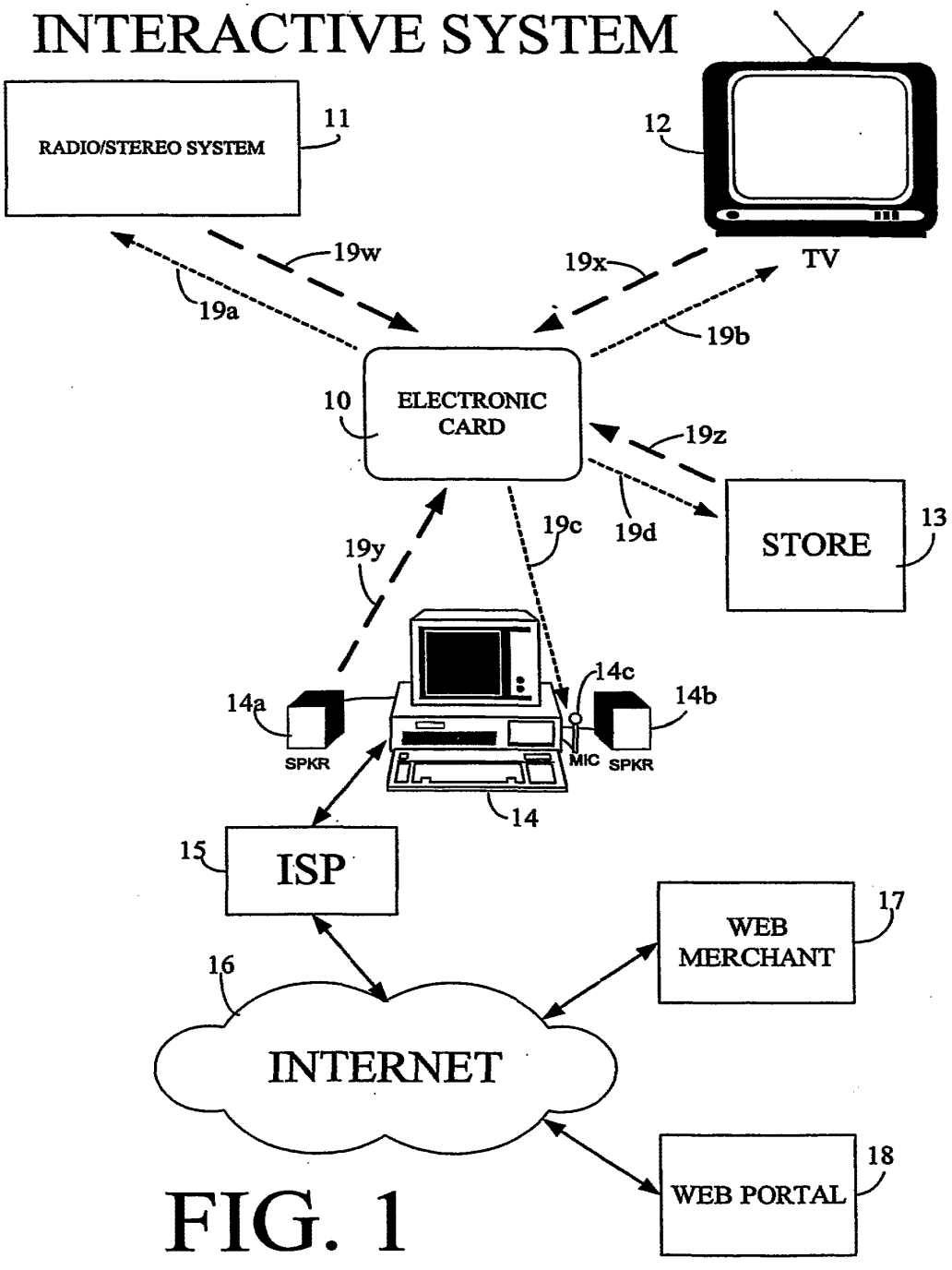

INTERACTIVE SYSTEM
RADIO/STEREO SYSTEM
11
12
TV
19w
19x
19a
19b
10
ELECTRONIC CARD
19z
19c
19d
19y
STORE
13
14a
14c
14b
SPKR
MIC
SPKR
14
15
ISP
17
WEB MERCHANT
16
INTERNET
18
WEB PORTAL

FIG. 1

ONE-WAY TX CARD

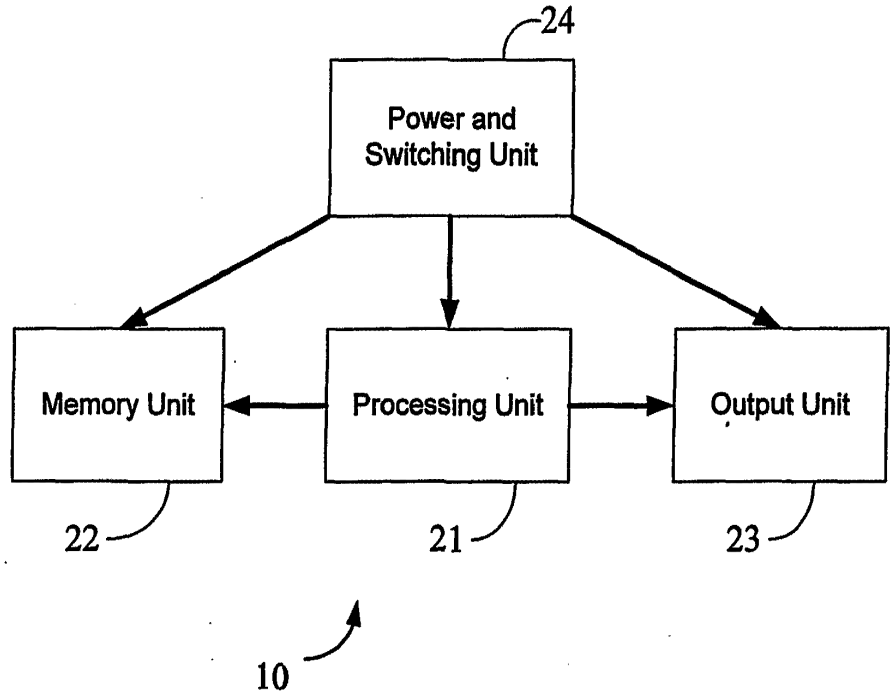


FIG. 2

TWO-WAY CARD

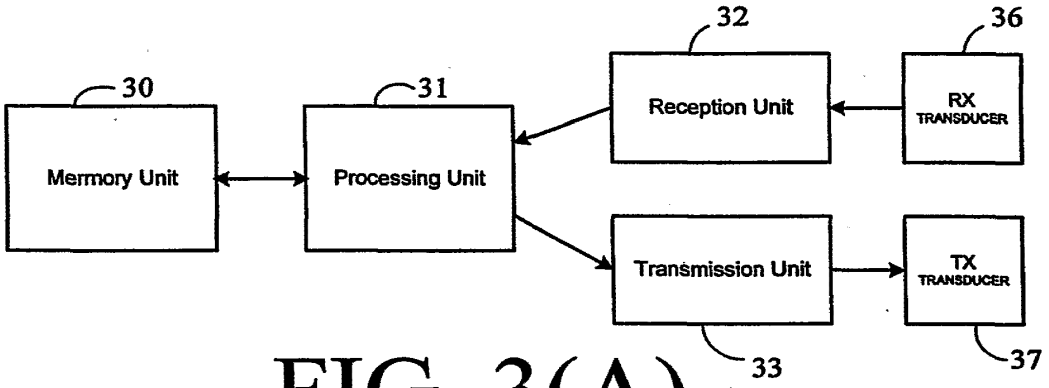


FIG. 3(A)

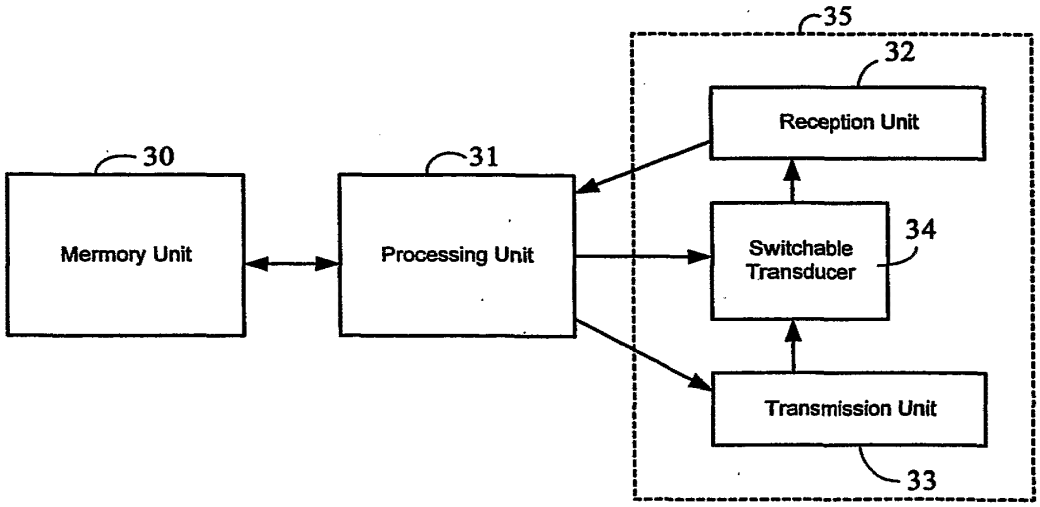


FIG. 3(B)

CARD RECEIVER

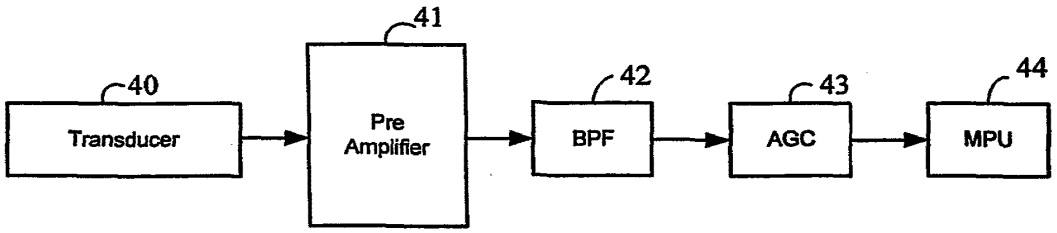


FIG. 4(A)

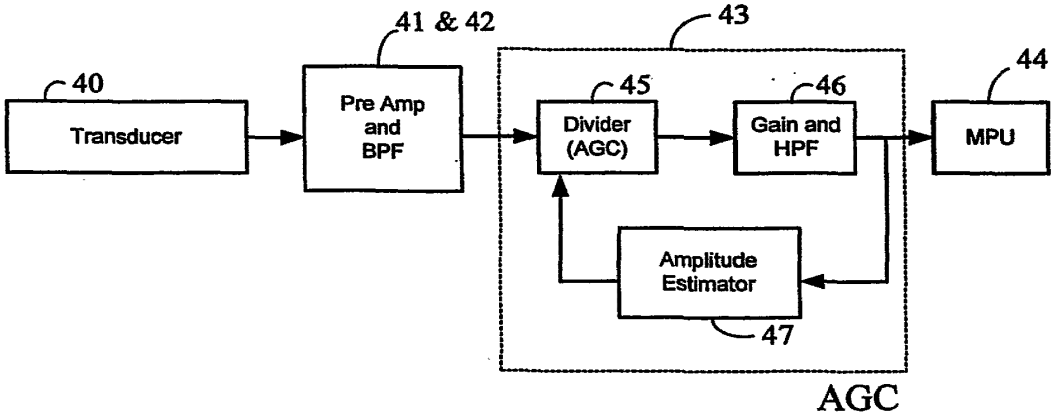


FIG. 4(B)

DATA FORMAT

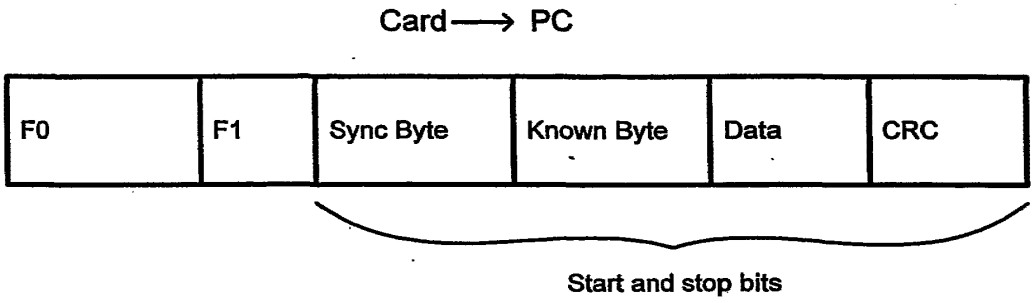


FIG. 5(A)

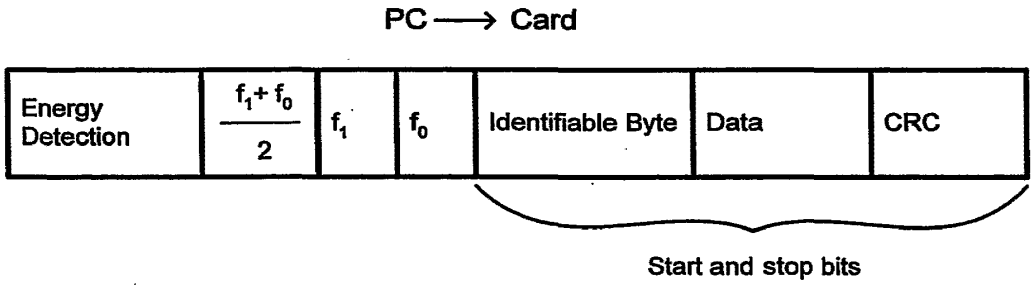


FIG. 5(B)

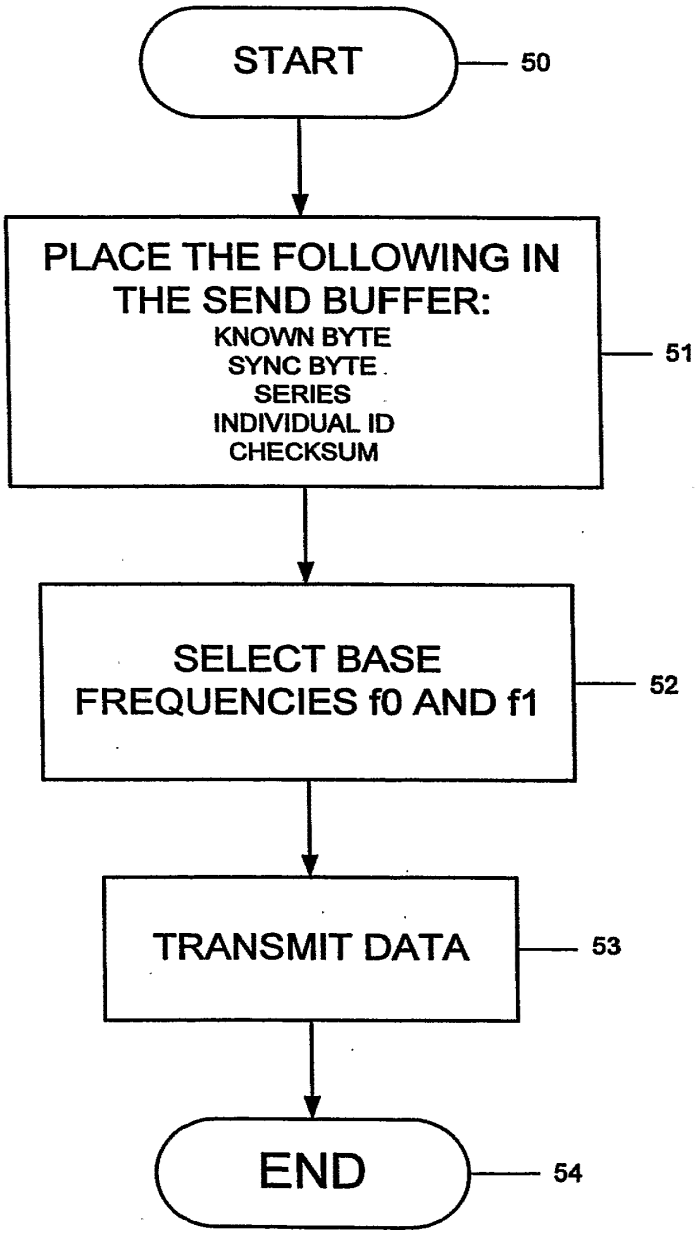

START
50
PLACE THE FOLLOWING IN THE SEND BUFFER:
KNOWN BYTE
SYNC BYTE
SERIES
INDIVIDUAL ID
CHECKSUM
51
SELECT BASE FREQUENCIES f0 AND f1
52
TRANSMIT DATA
53
END
54

FIG. 6(A)

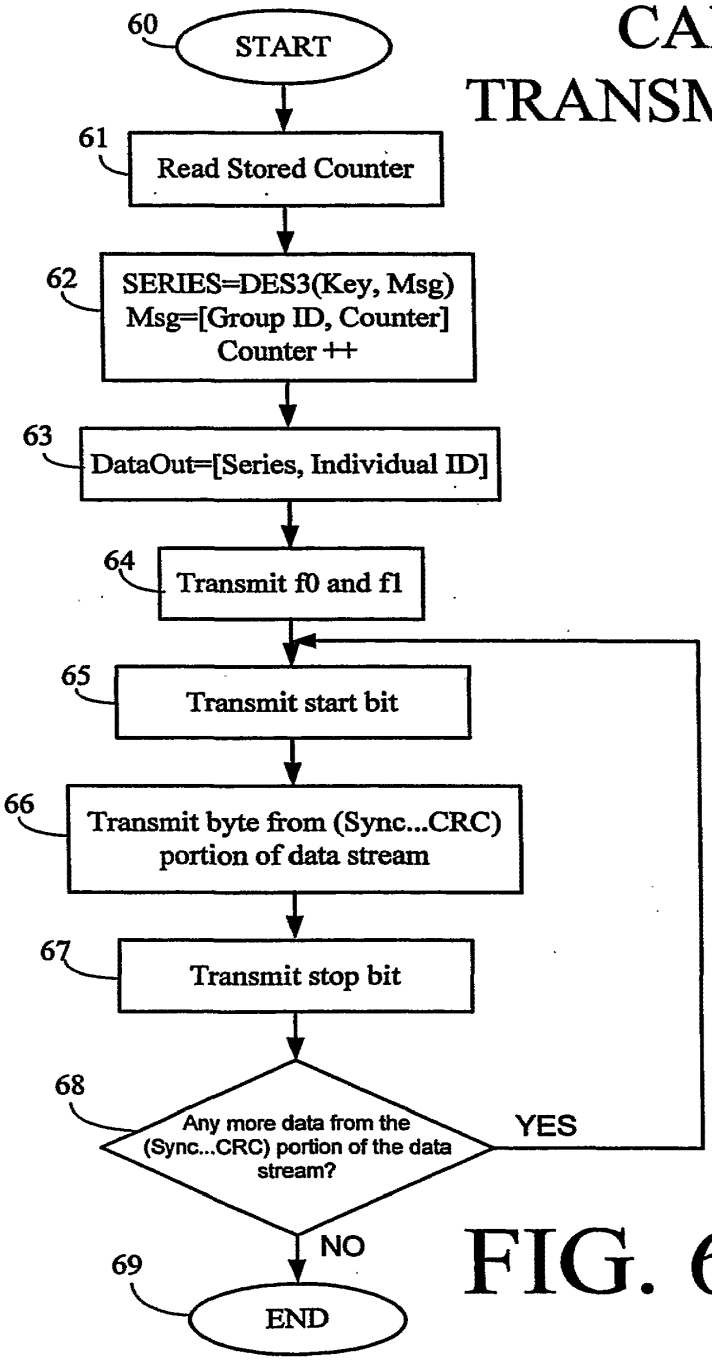

CARD TRANSMISSION
60
START
61
Read Stored Counter
62
SERIES=DES3(Key, Msg)
Msg=[Group ID, Counter]
Counter ++
63
DataOut=[Series, Individual ID]
64
Transmit f0 and f1
65
Transmit start bit
66
Transmit byte from (Sync...CRC) portion of data stream
67
Transmit stop bit
68
Any more data from the (Sync...CRC) portion of the data stream?
YES
NO
69
END

FIG. 6(B)

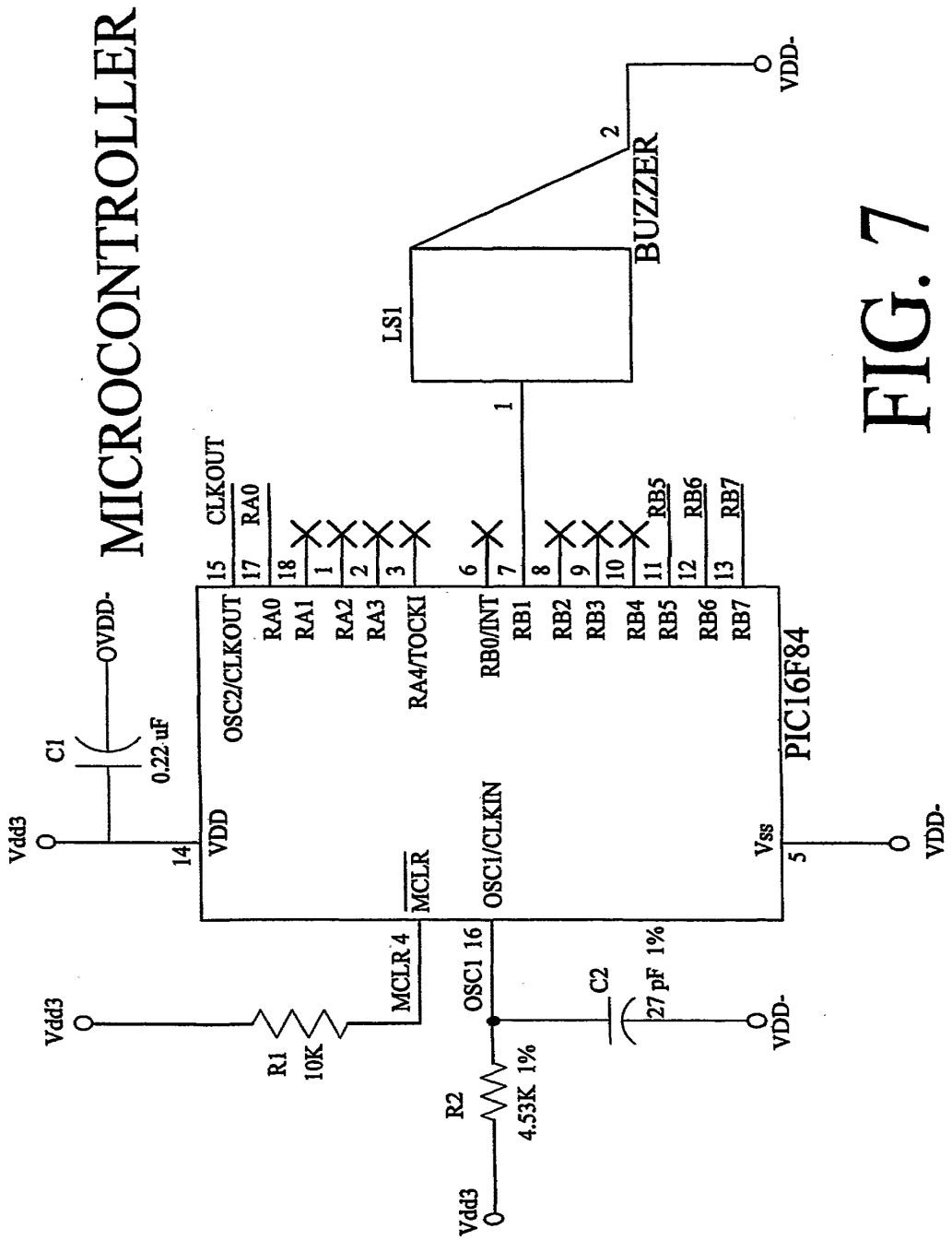

MICROCONTROLLER
PIC16F84
OSC2/CLKOUT
RA0
RA1
RA2
RA3
RA4/TOCKI
RB0/INT
RB1
RB2
RB3
RB4
RB5
RB6
RB7
VDD
MCLR
OSC1/CLKIN
Vss
CLKOUT
15
17
18
1
2
3
6
7
8
9
10
11
12
13
14
5
4
16
LS1
BUZZER
C1
0.22 uF
C2
27 pF 1%
R1
10K
R2
4.53K 1%
Vdd3
VDD-
OSC1
MCLR

FIG. 7

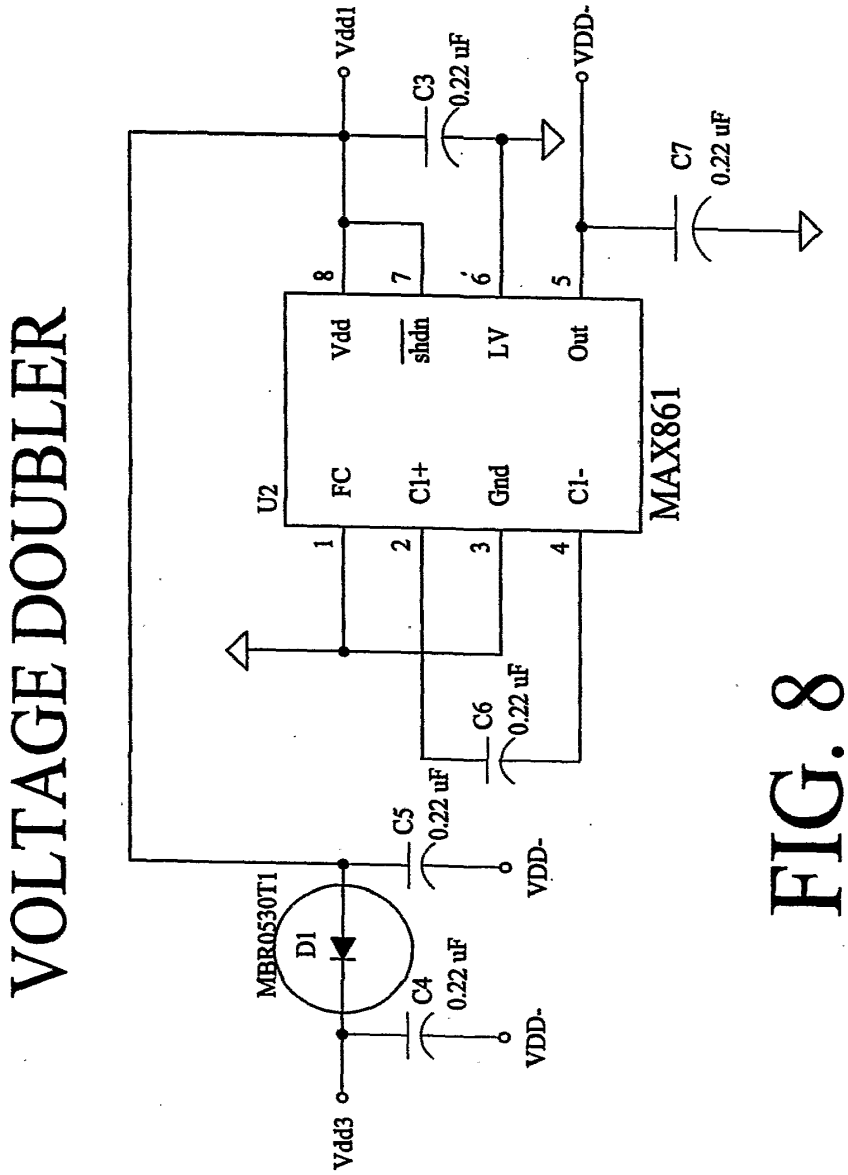

VOLTAGE DOUBLER
Vdd1
C3
0.22 uF
VDD-
C7
0.22 uF
U2
FC
C1+
Gnd
C1-
Vdd
shdn
LV
Out
MAX861
1
2
3
4
8
7
6
5
C6
0.22 uF
C5
0.22 uF
VDD-
MBR0530T1
D1
C4
0.22 uF
VDD-
Vdd3

FIG. 8

POWER AND SWITCHING CIRCUIT

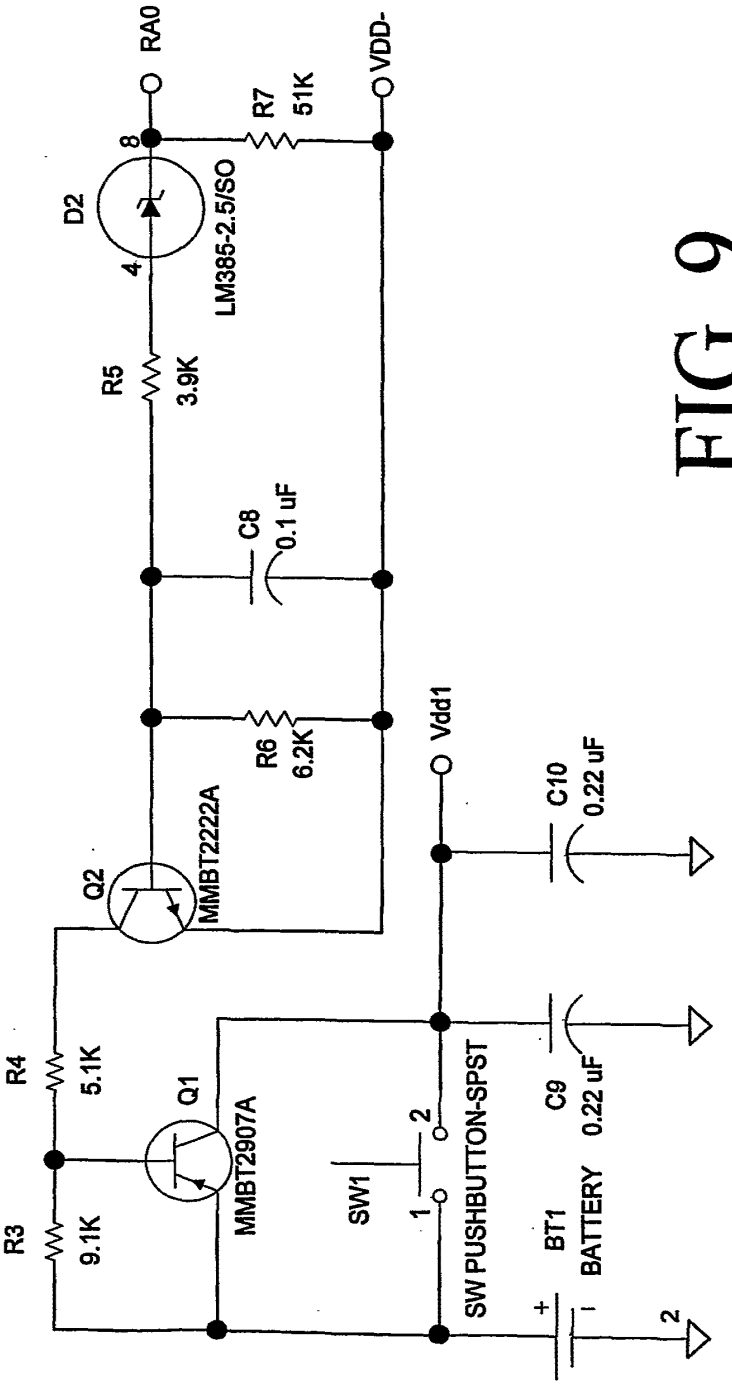


FIG. 9

SMART CARD CONNECTOR

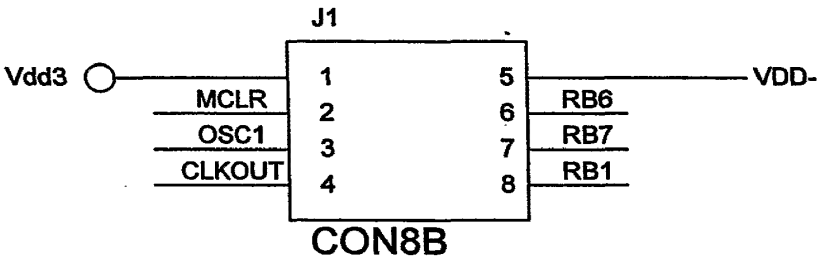


FIG. 10

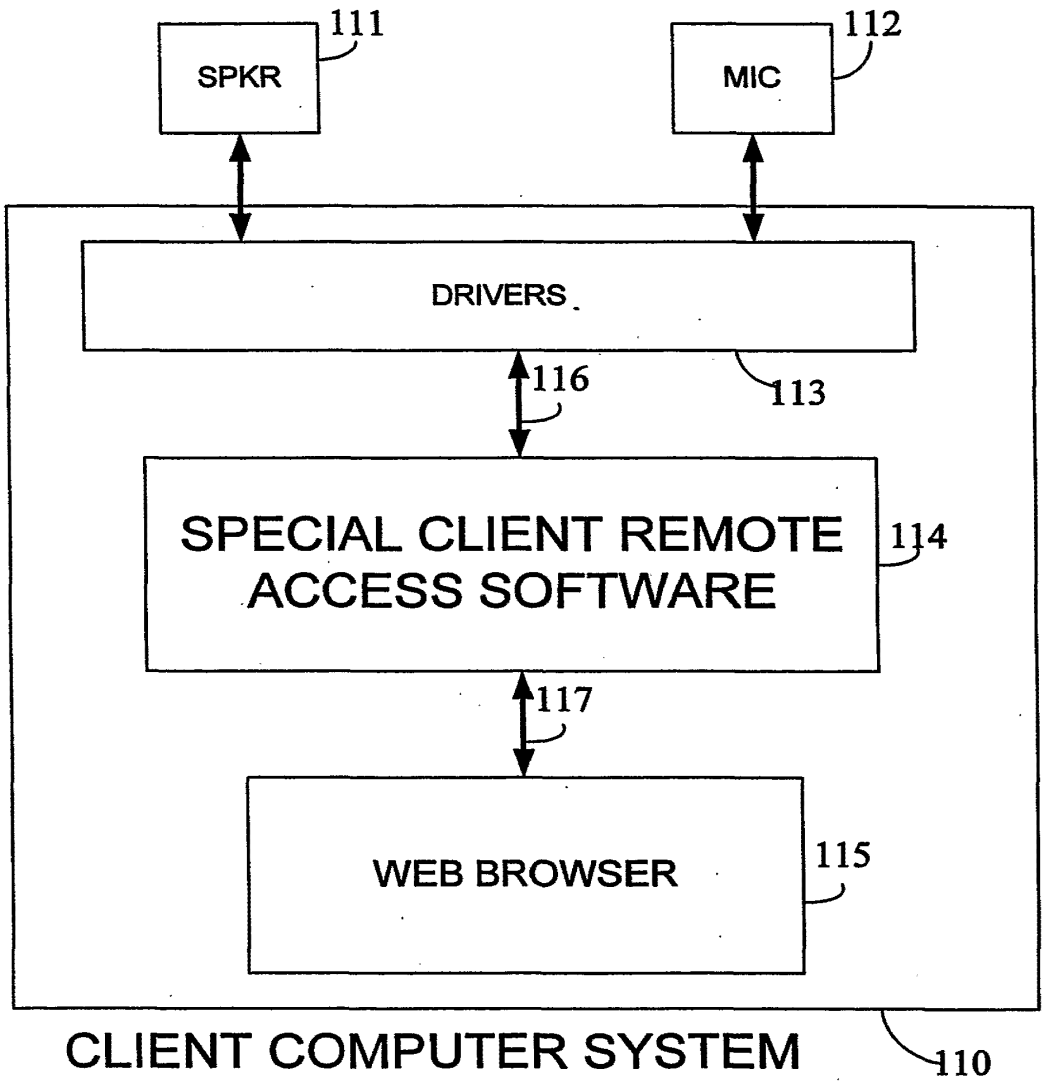

111
SPKR
112
MIC
DRIVERS
116
113
SPECIAL CLIENT REMOTE ACCESS SOFTWARE
114
117
WEB BROWSER
115
CLIENT COMPUTER SYSTEM
110

FIG. 11

CARD RECEPTION SOFTWARE

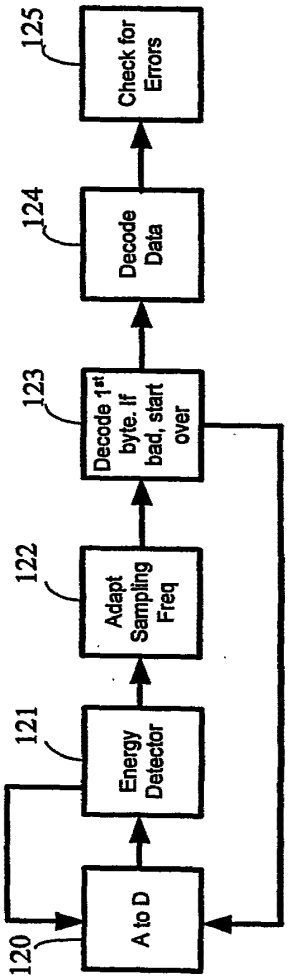
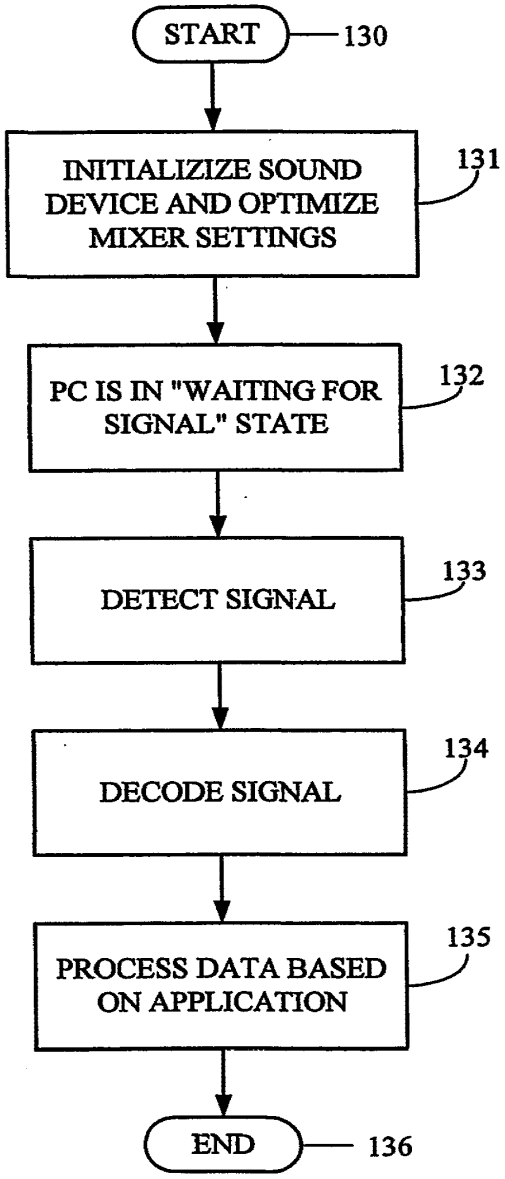


FIG. 12



PC RX SOFTWARE

FIG. 13

SIGNAL DECODER

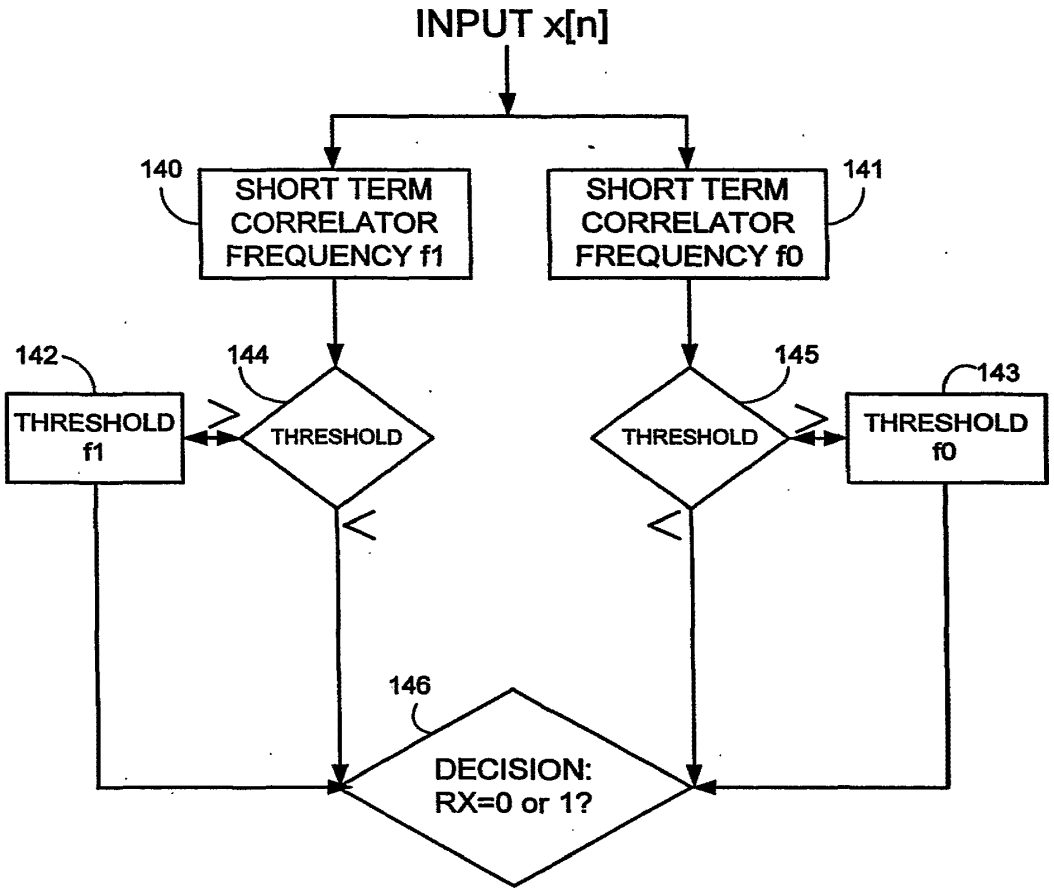
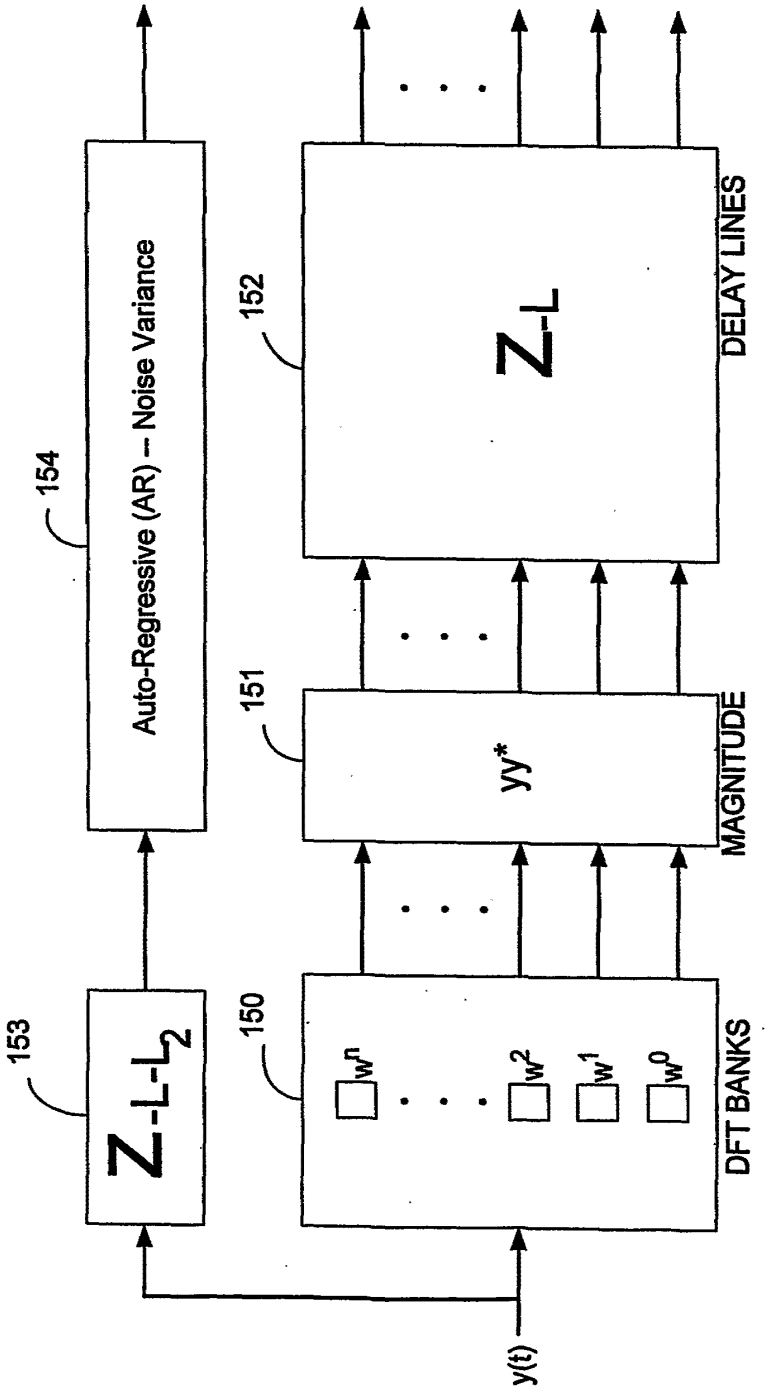


FIG. 14

FIG. 15


SIGNAL DETECTION
DFT BANKS
MAGNITUDE
DELAY LINES
Auto-Regressive (AR) -- Noise Variance
Z_{-L-L_2}
Z_{-L}
yy*
w^n
w^2
w^1
w^0
y(t)
150
151
152
153
154

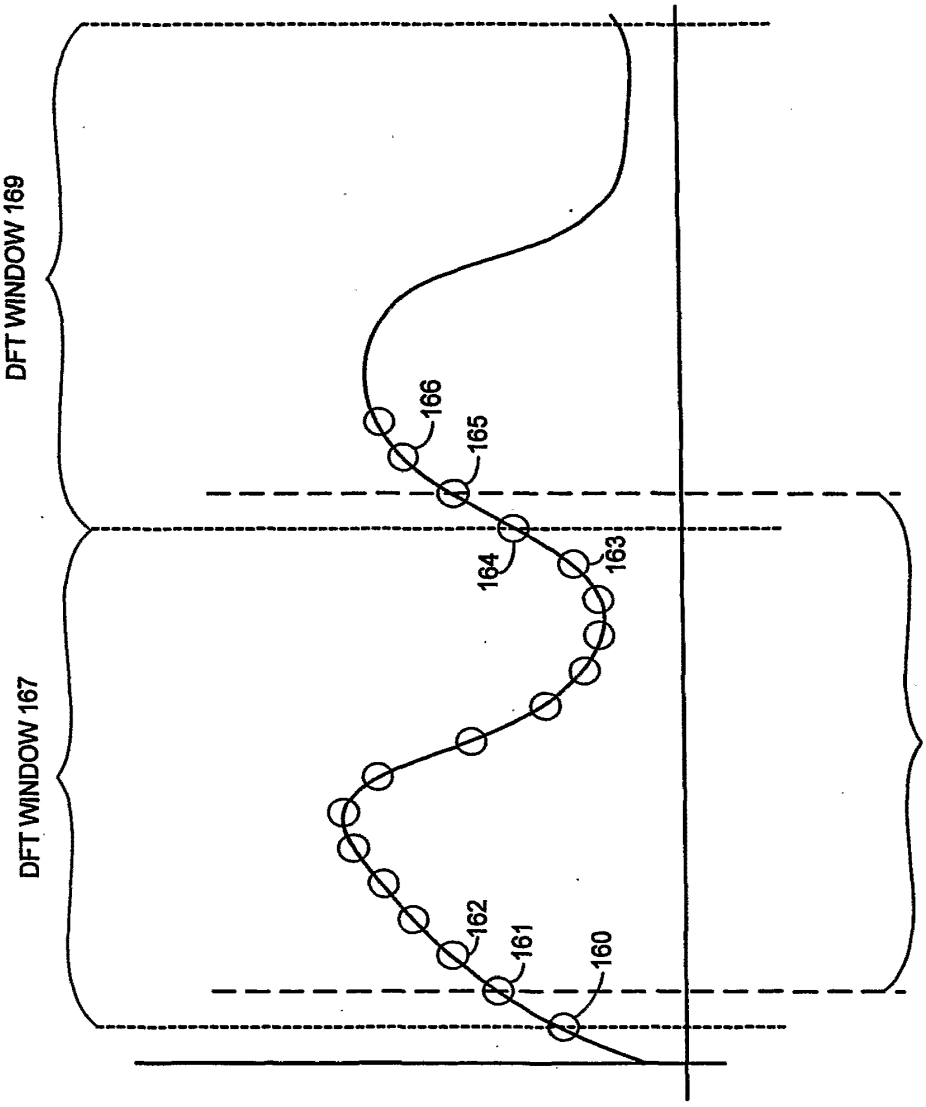

DFT WINDOW 169
DFT WINDOW 167
DFT WINDOW 168
166
165
164
163
162
161
160

FIG. 16

ALTERNATIVE EMBODIMENT
-- ONE-WAY TX HARDWARE

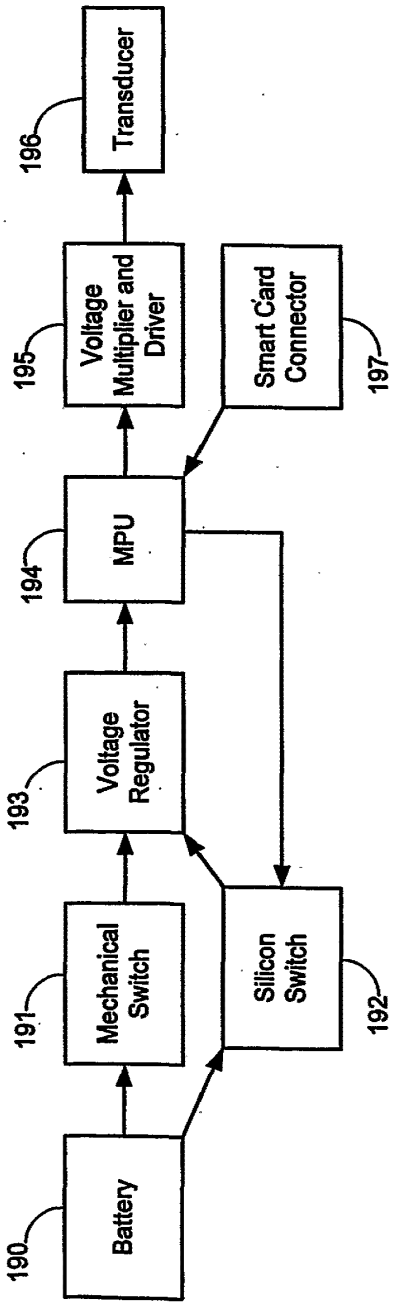
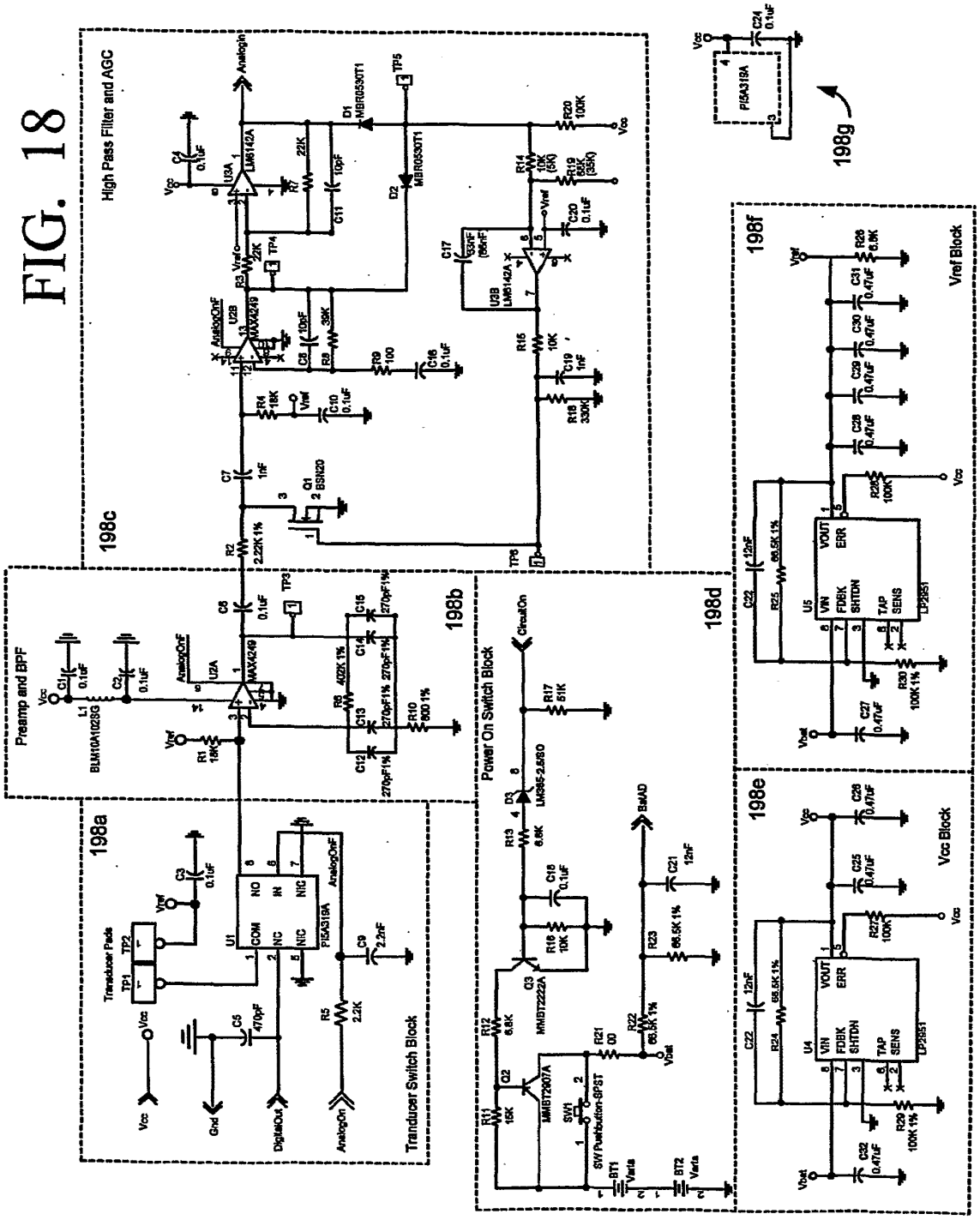


FIG. 17

FIG. 18


198a
Transducer Switch Block
198b
Preamp and BPF
198c
High Pass Filter and AGC
198d
Power On Switch Block
198e
Vcc Block
198f
Vref Block
198g

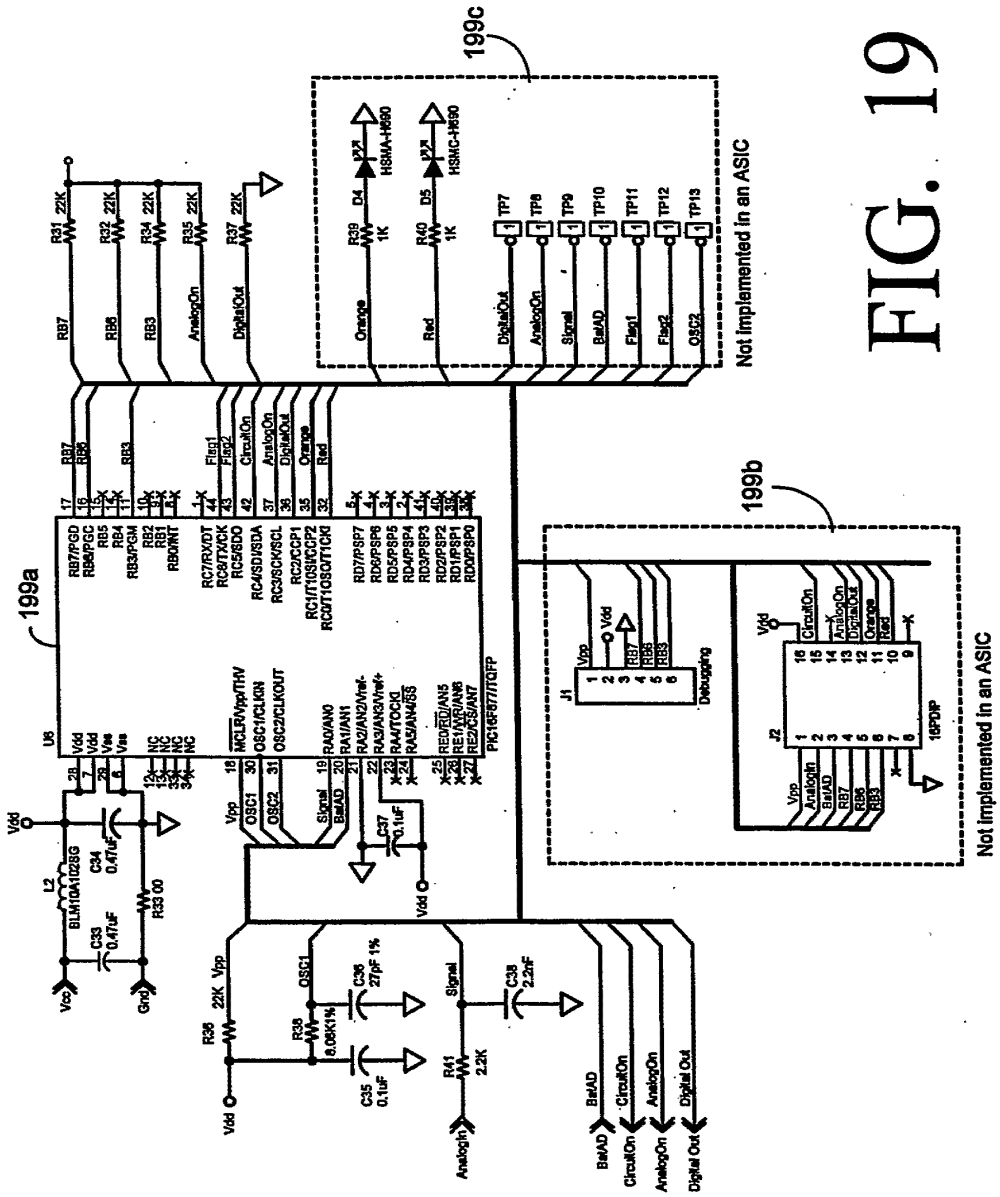

199c
Not Implemented in an ASIC
199b
Not implemented in an ASIC
199a
U6
PIC16F877/TQFP
J1
Debugging
J2
18PDIP
L2
BLM10A11023G
C33 0.47uF
C34 0.47uF
R33 00
C37 0.1uF
R36 22K
R38 8.06K1%
C36 27pF 1%
C35 0.1uF
R41 2.2K
C38 2.2nF
R31 22K
R32 22K
R34 22K
R35 22K
R37 22K
R39 1K
R40 1K
D4 HSMA-H660
D5 HSMC-H660
TP7
TP8
TP9
TP10
TP11
TP12
TP13
Vdd
Vpp
Gnd
Signal
BatAD
CircuitOn
AnalogOn
Digital Out
Analog In

FIG. 19

CARD ARCHITECTURE
-- ANALOG RECORDING

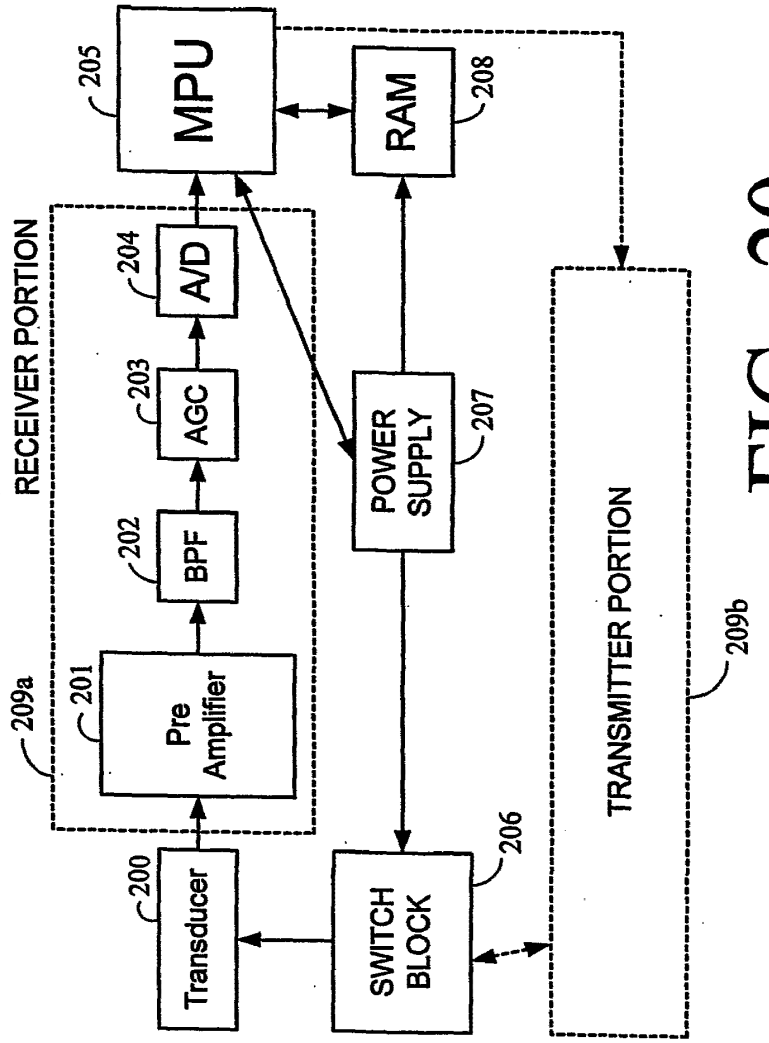


FIG. 20

SERVER ARCHITECTURE

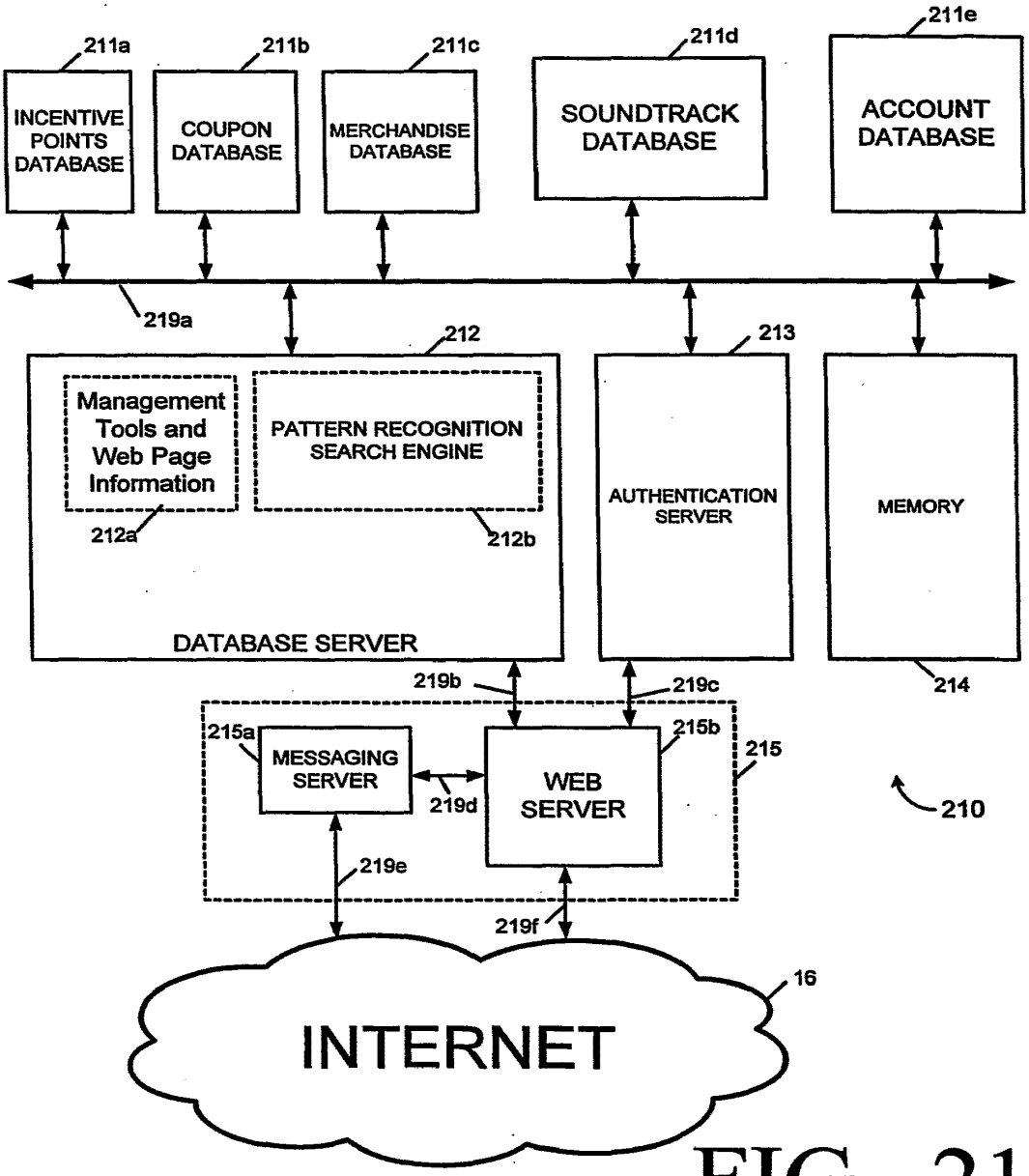


FIG. 21

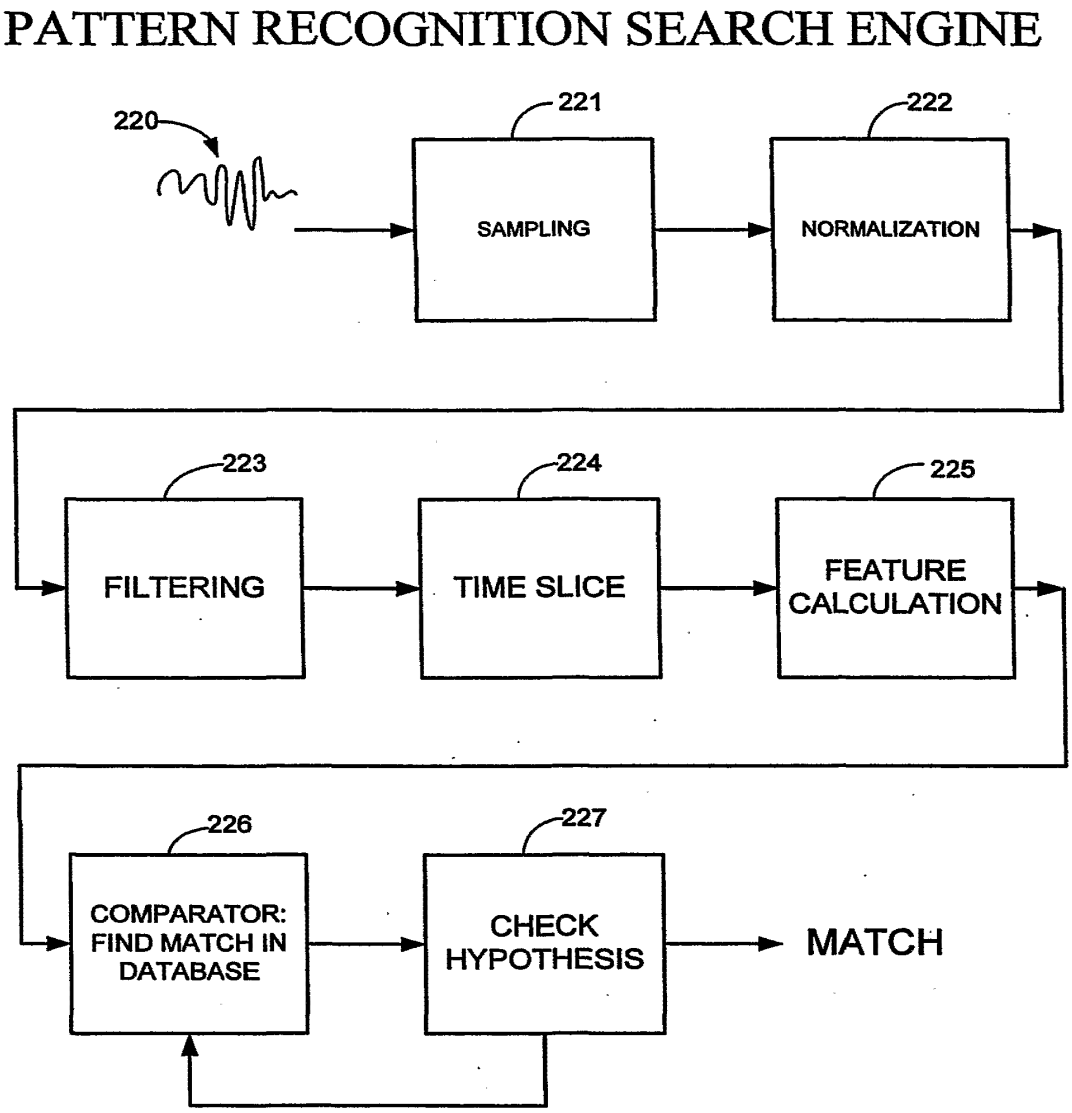

PATTERN RECOGNITION SEARCH ENGINE
220
221
SAMPLING
222
NORMALIZATION
223
FILTERING
224
TIME SLICE
225
FEATURE CALCULATION
226
COMPARATOR: FIND MATCH IN DATABASE
227
CHECK HYPOTHESIS
MATCH

FIG. 22

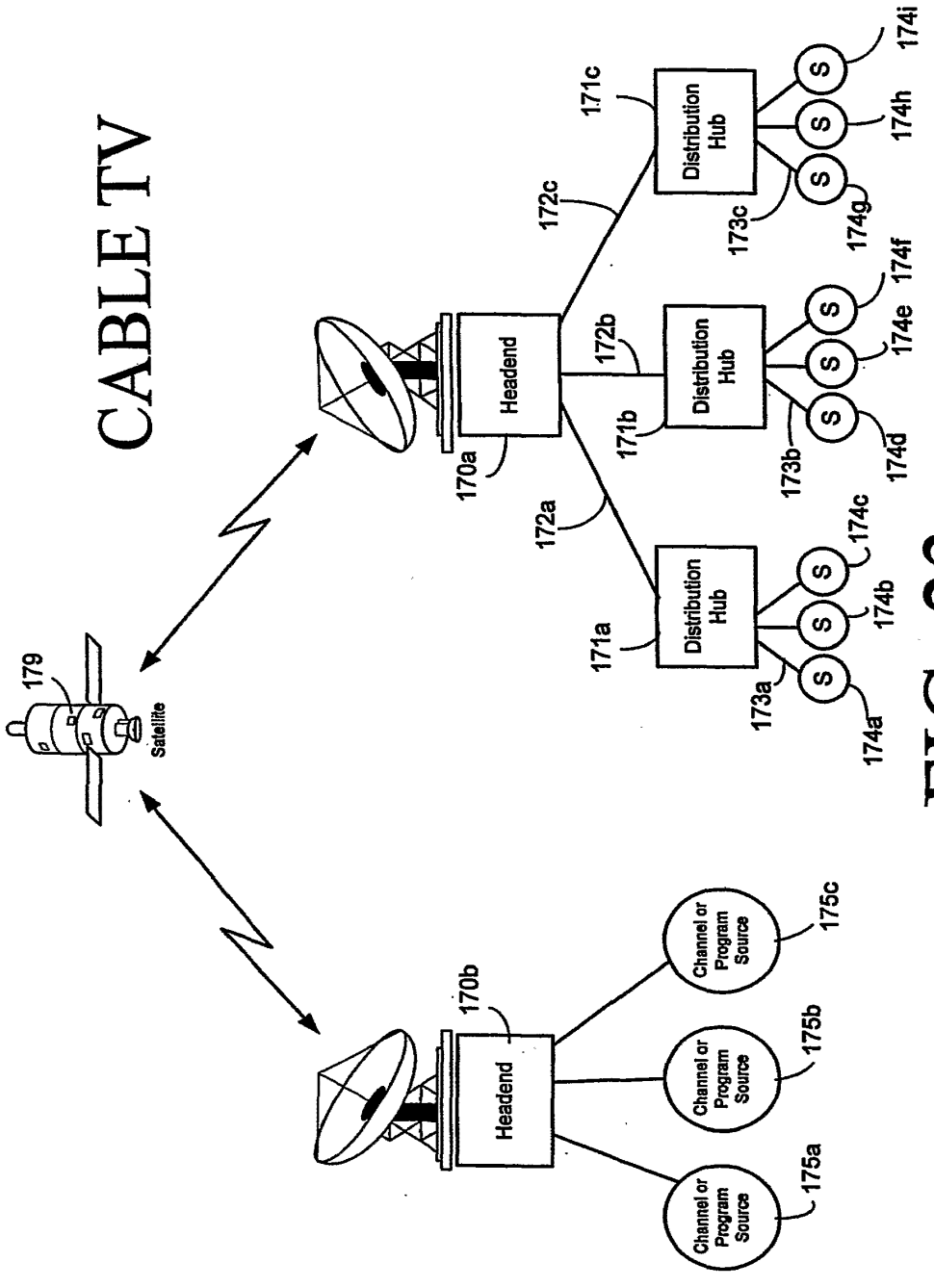

CABLE TV
179
Satellite
Headend
170a
Headend
170b
Distribution Hub
171a
Distribution Hub
171b
Distribution Hub
171c
172a
172b
172c
Channel or Program Source
175a
Channel or Program Source
175b
Channel or Program Source
175c
173a
173b
173c
174a
174b
174c
174d
174e
174f
174g
174h
174i

FIG. 23

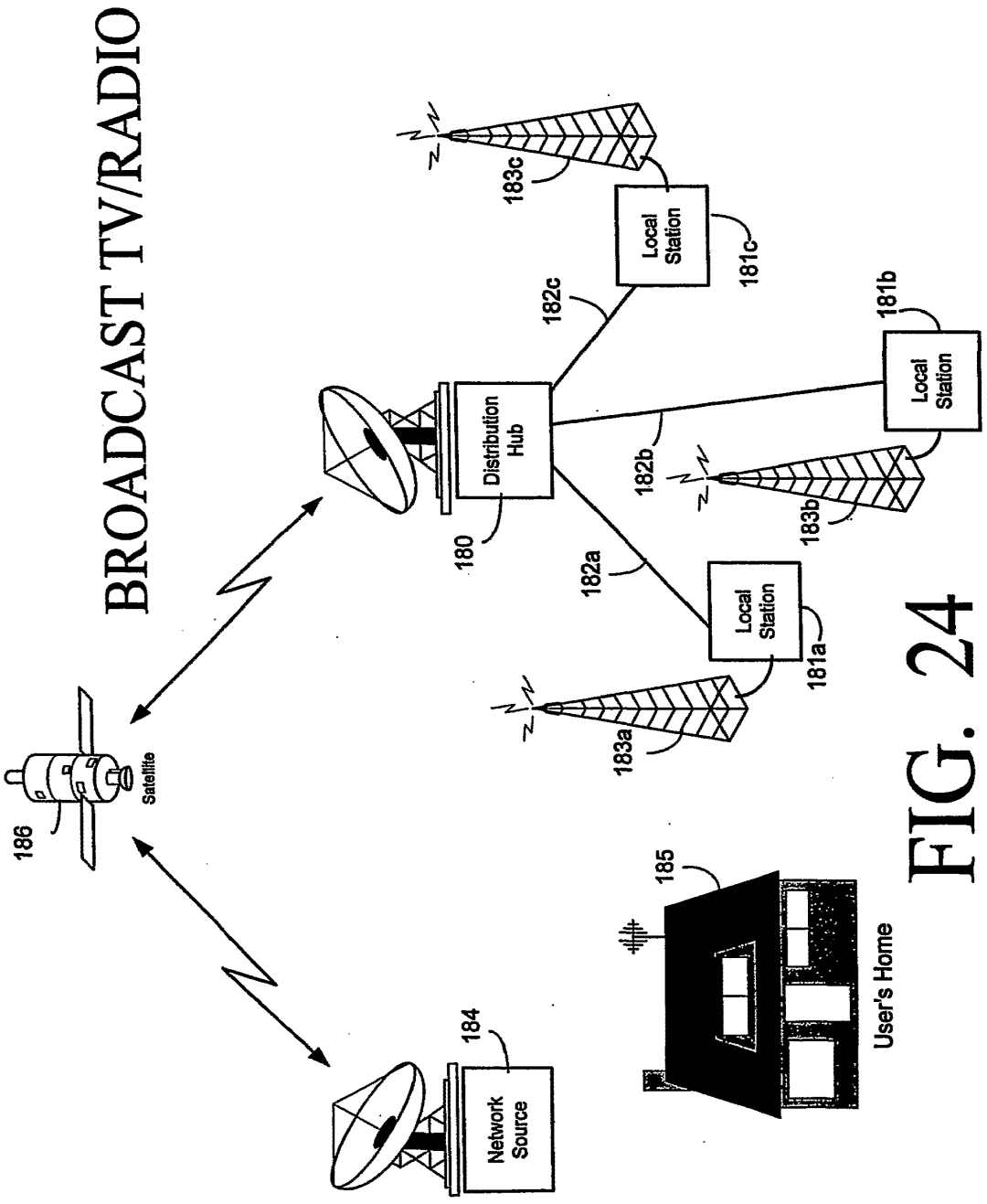

BROADCAST TV/RADIO
Satellite
186
Network Source
184
Distribution Hub
180
Local Station
181a
Local Station
181b
Local Station
181c
182a
182b
182c
183a
183b
183c
185
User's Home

FIG. 24

COMPONENT LAYOUT #1

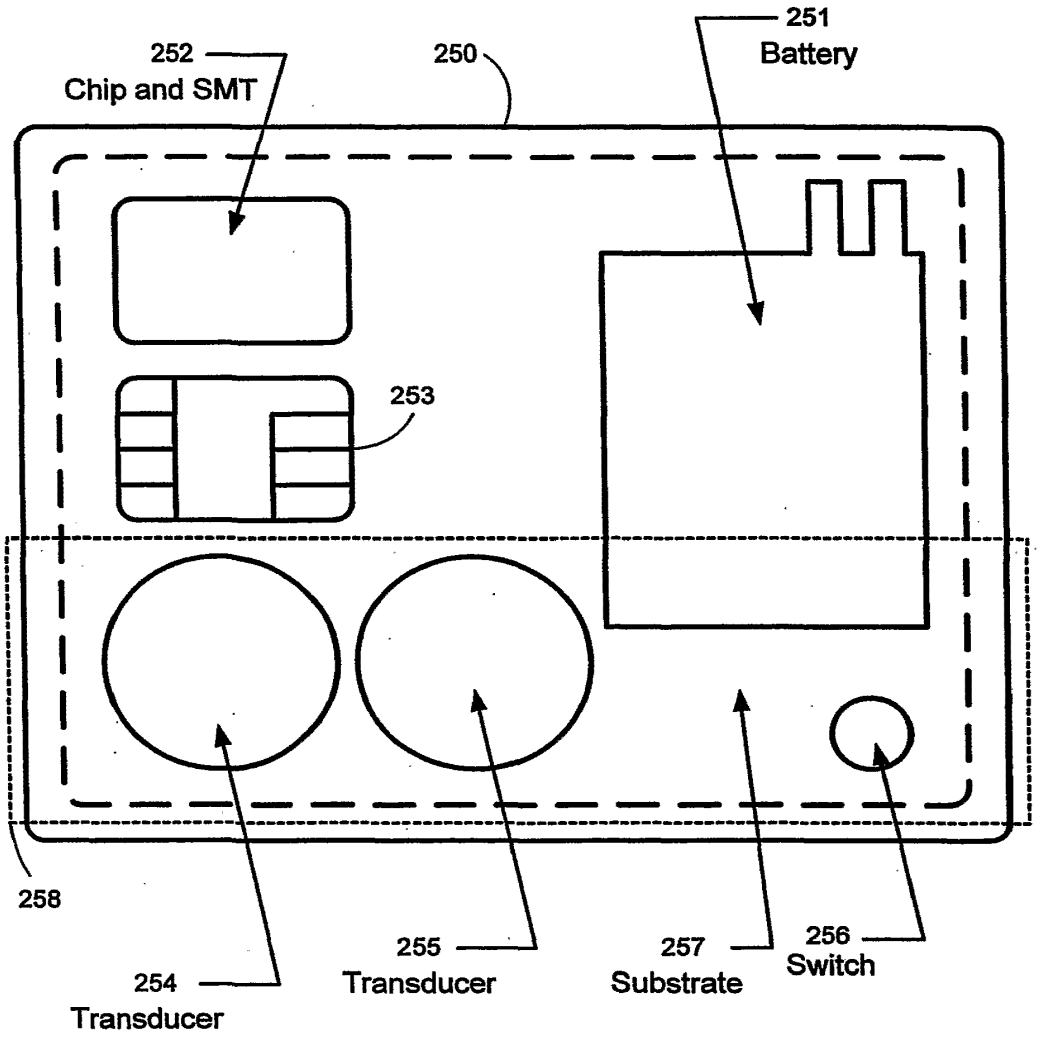


FIG. 25(A)

COMPONENT LAYOUT #2

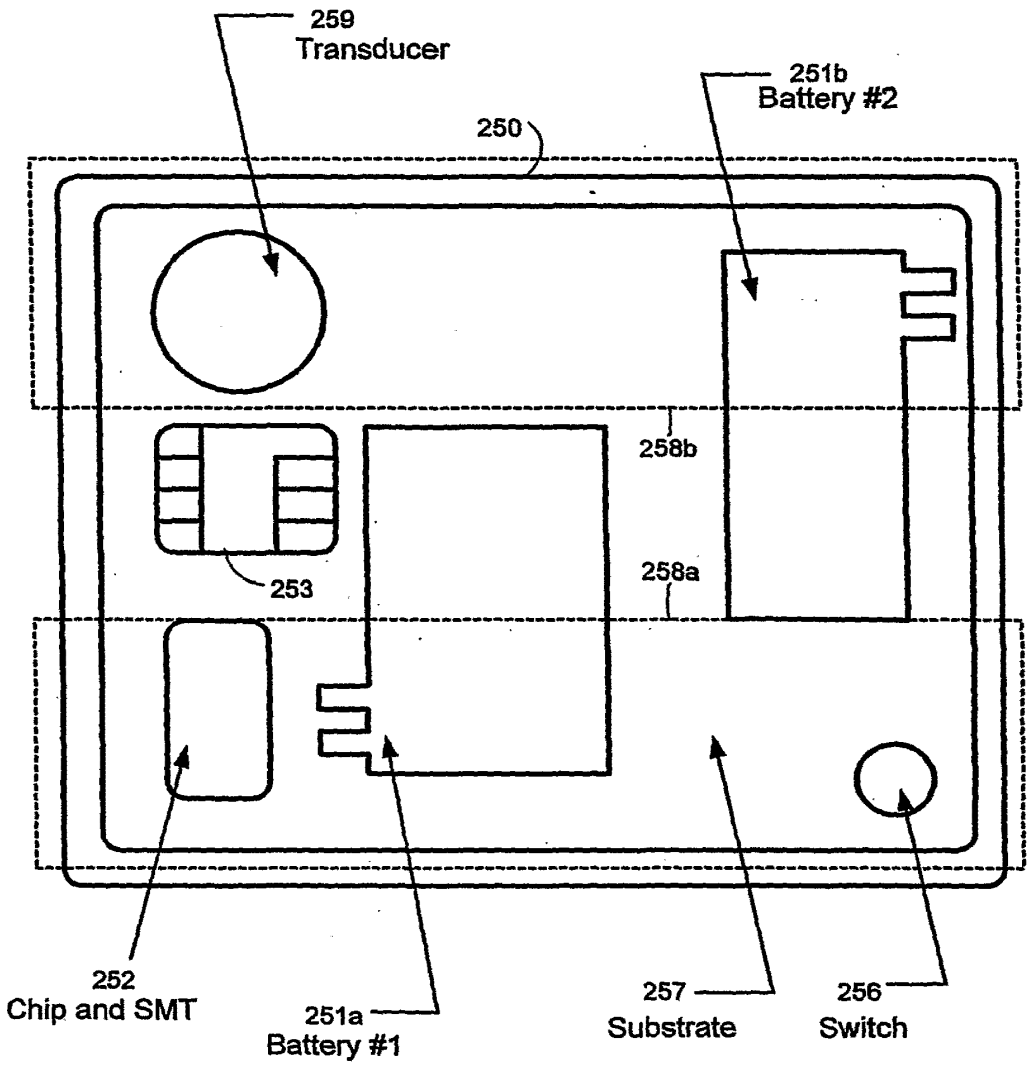


FIG. 25(B)

COMPONENT LAYOUT #3

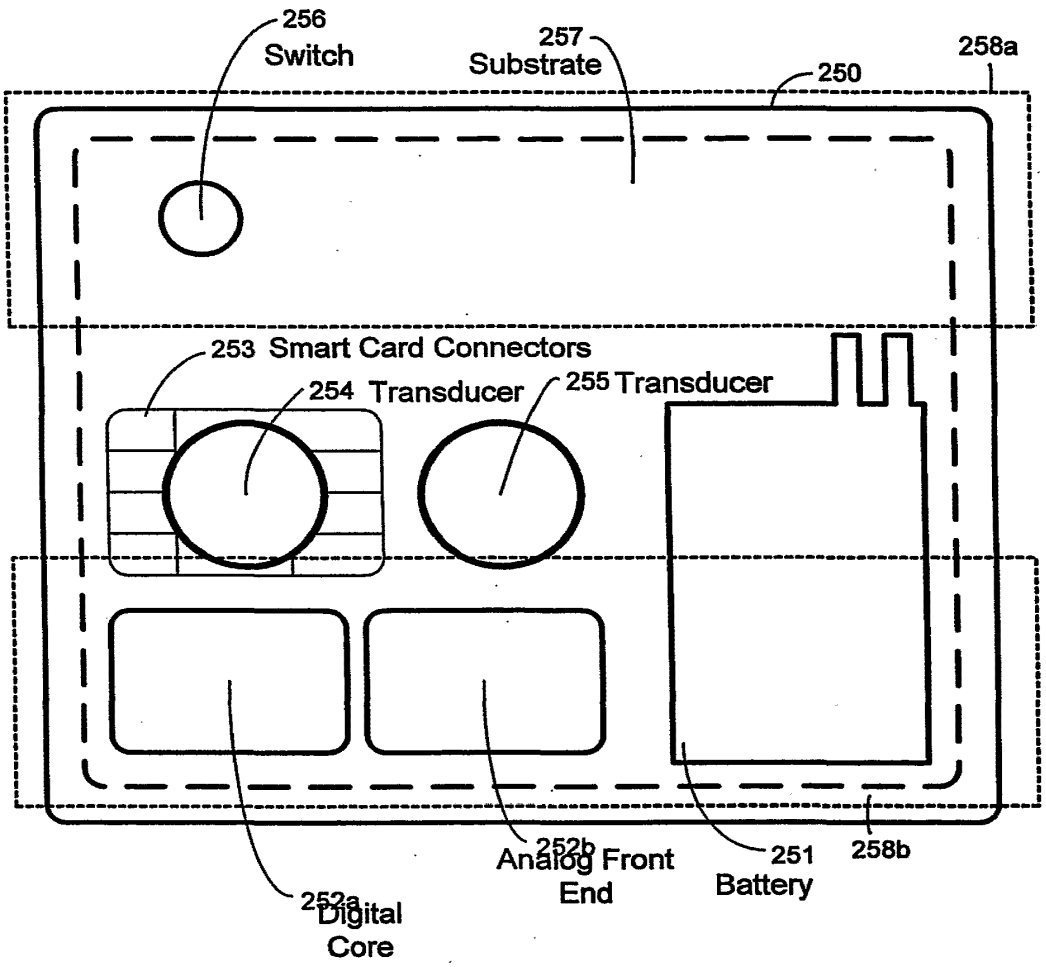


FIG. 25(C)

CARD FABRICATION

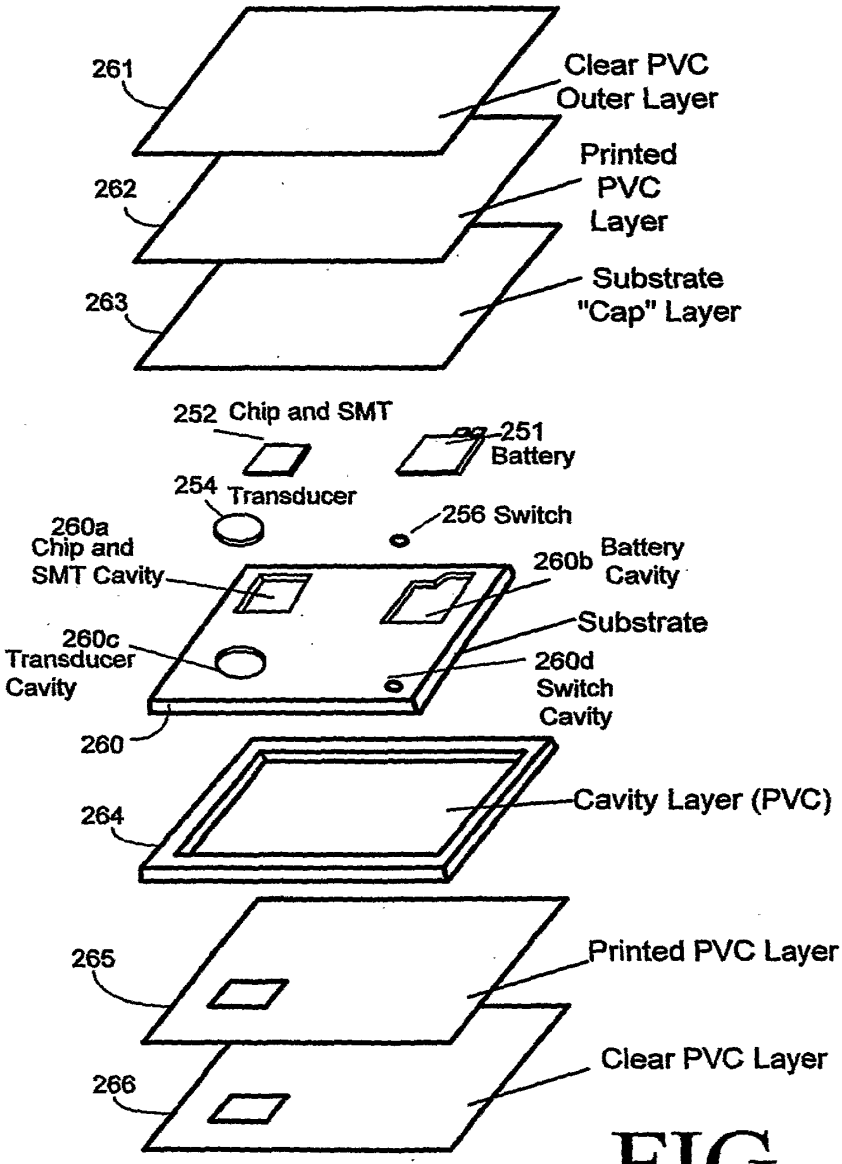


FIG. 26

TRANSDUCER FABRICATION

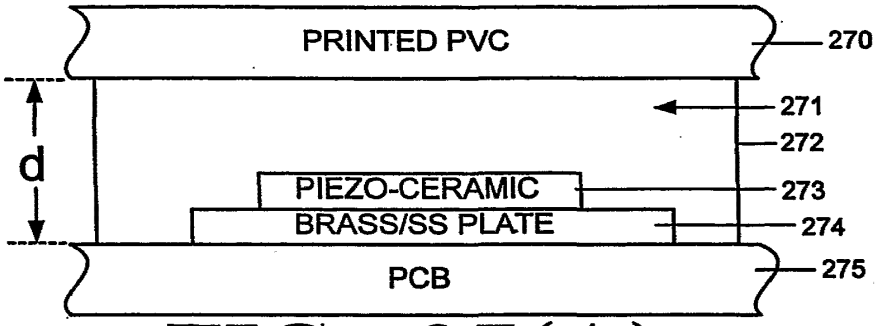


FIG. 27(A)

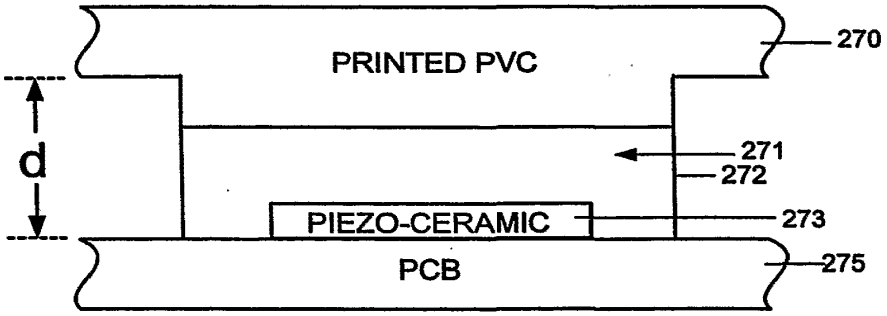


FIG. 27(B)

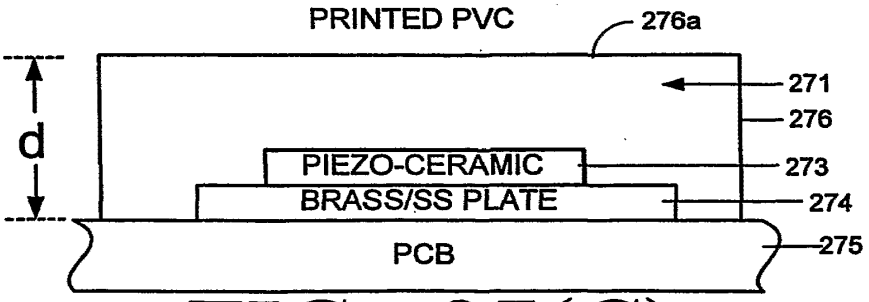


FIG. 27(C)

MULTI-MODE SWITCH

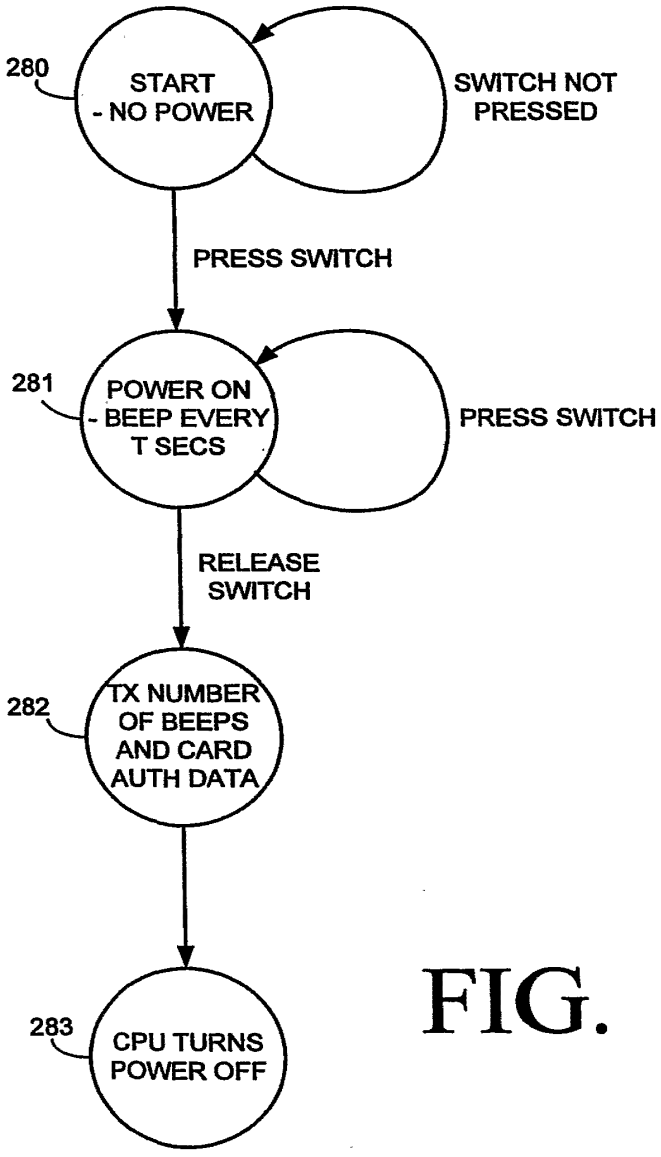


FIG. 28

E-WALLET SYSTEM

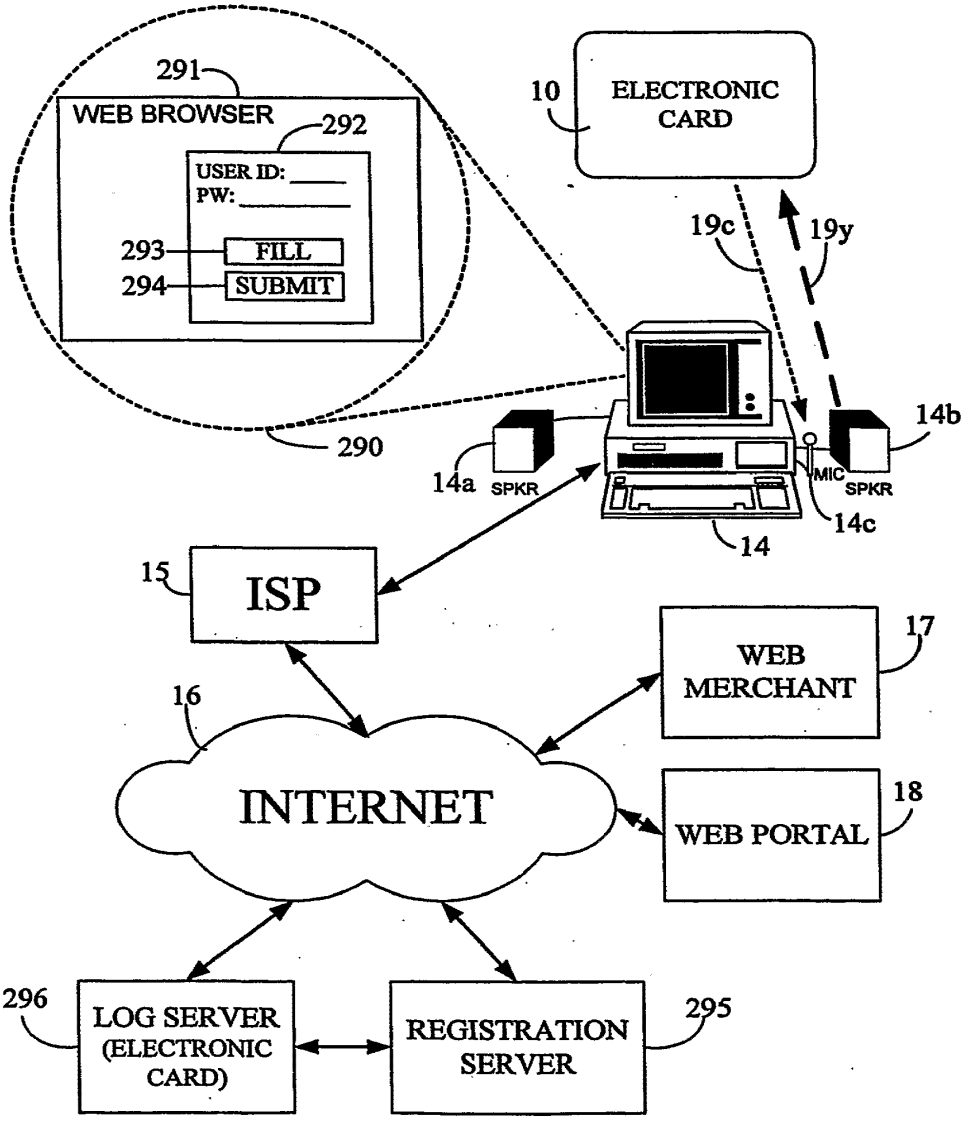
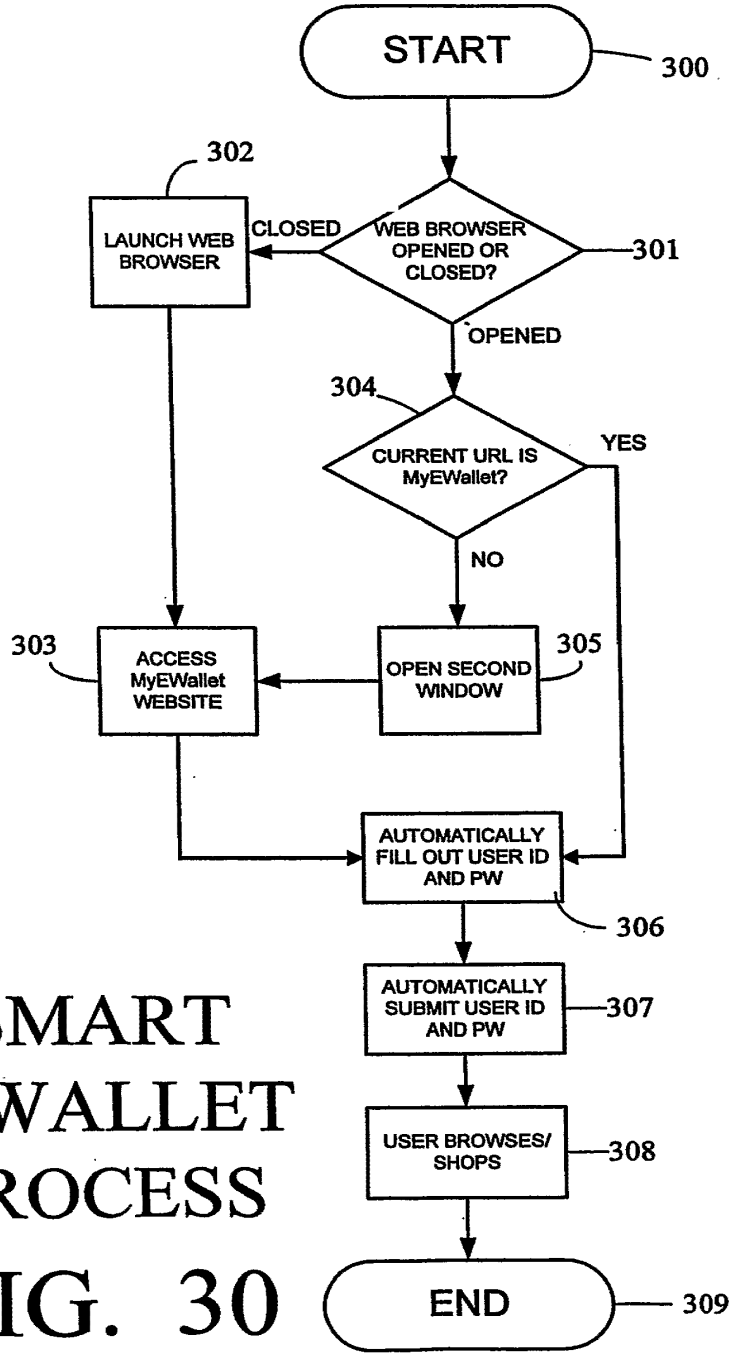


FIG. 29



SMART E-WALLET PROCESS

FIG. 30

CREDIT CARD TRANSACTION MODEL

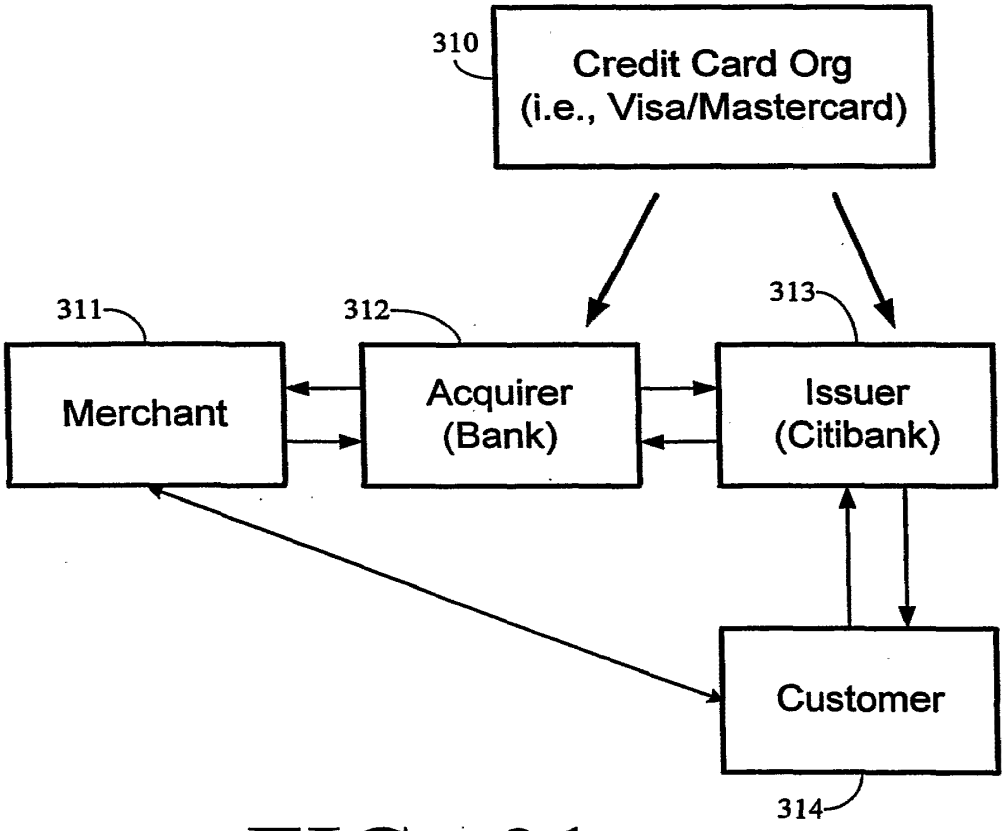


FIG. 31

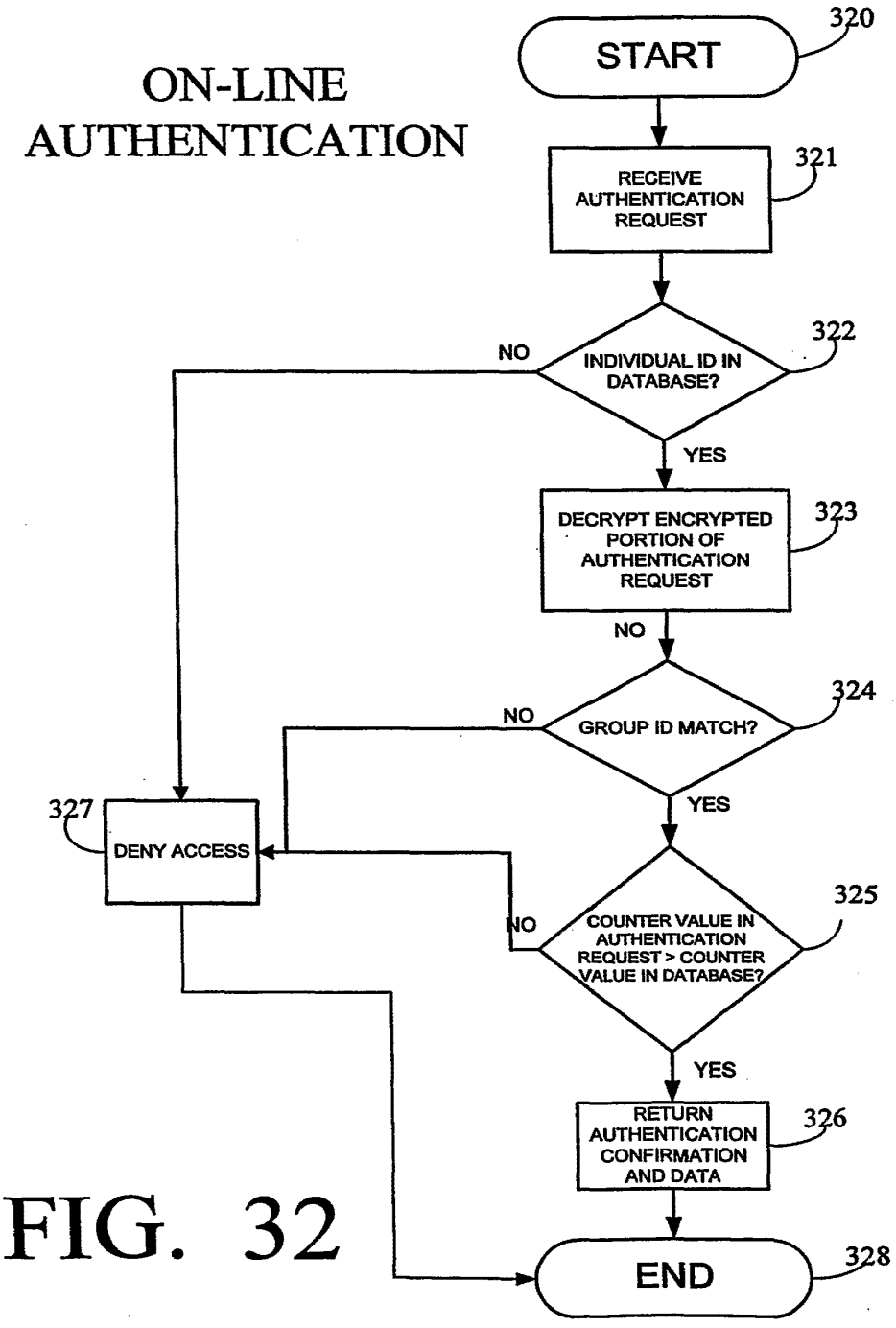

ON-LINE AUTHENTICATION
START
320
RECEIVE AUTHENTICATION REQUEST
321
INDIVIDUAL ID IN DATABASE?
322
NO
YES
DECRYPT ENCRYPTED PORTION OF AUTHENTICATION REQUEST
323
NO
GROUP ID MATCH?
324
NO
YES
DENY ACCESS
327
COUNTER VALUE IN AUTHENTICATION REQUEST > COUNTER VALUE IN DATABASE?
325
NO
YES
RETURN AUTHENTICATION CONFIRMATION AND DATA
326
END
328

FIG. 32

CHALLENGE-RESPONSE: CUSTOMER CHECKS MERCHANT

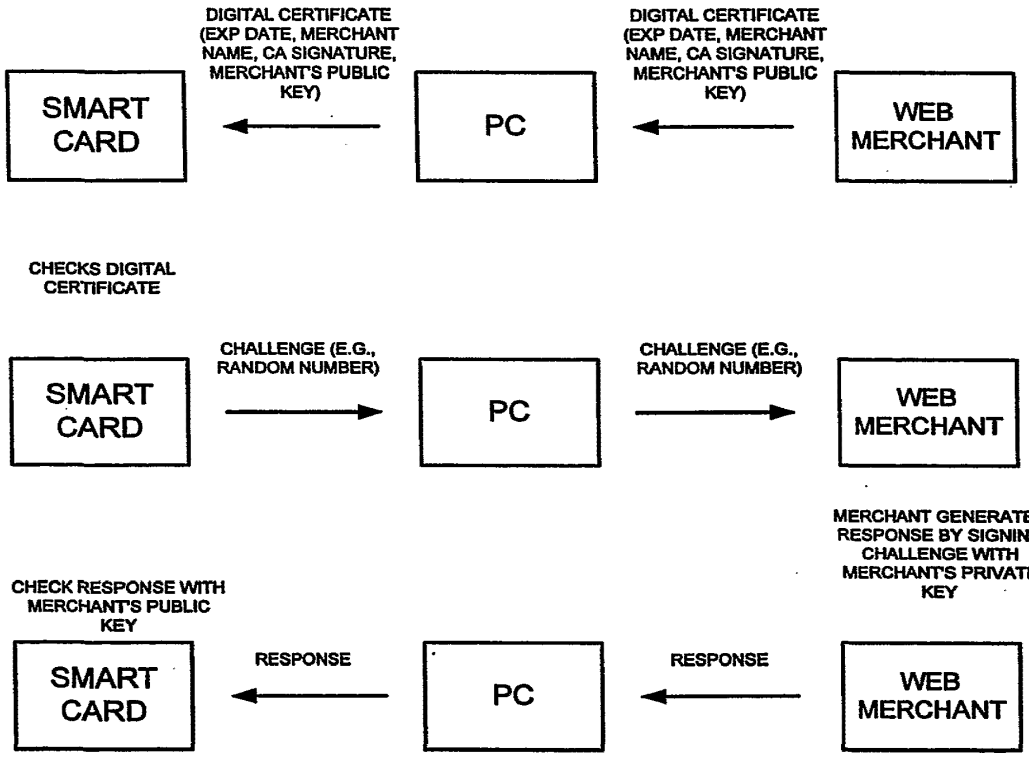


FIG. 33

CHALLENGE-RESPONSE: MERCHANT CHECKS CUSTOMER

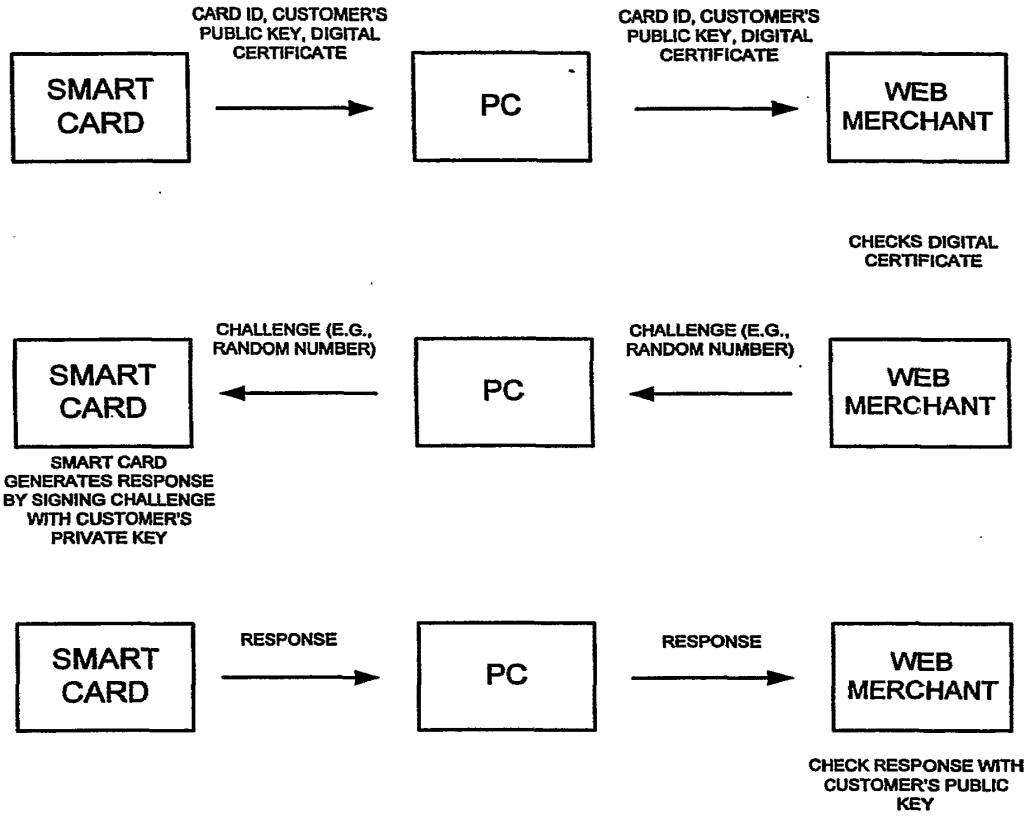


FIG. 34

CONCURRENT CHALLENGE-RESPONSE: MERCHANT AND CUSTOMER CHECK EACH OTHER

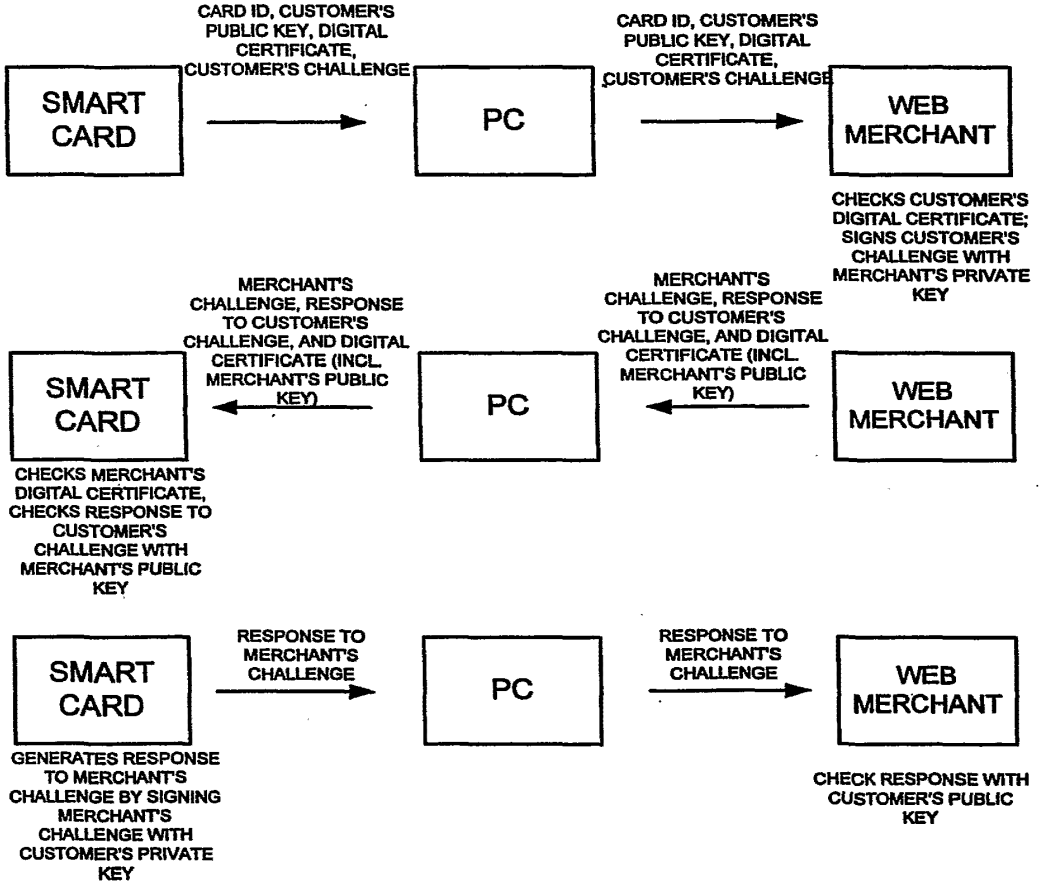


FIG. 35

CSP EMBODIMENT

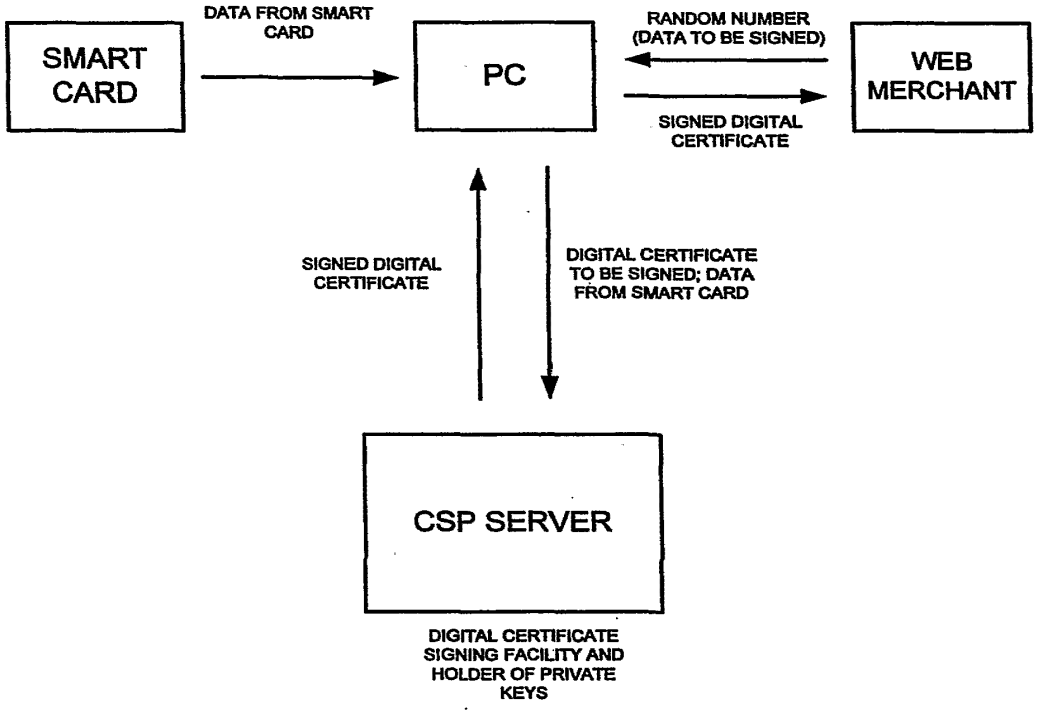


FIG. 36

FM IF System for RF Decoding (1)

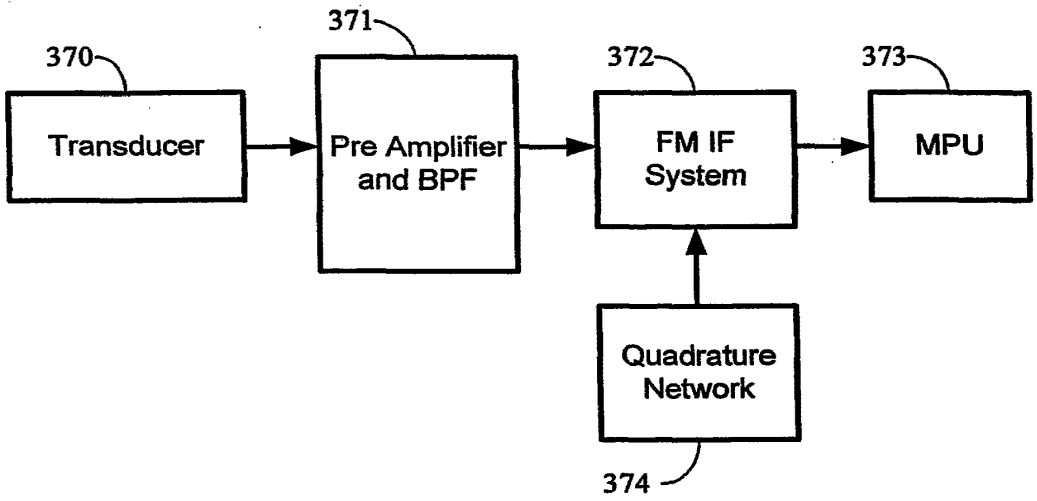


FIG. 37

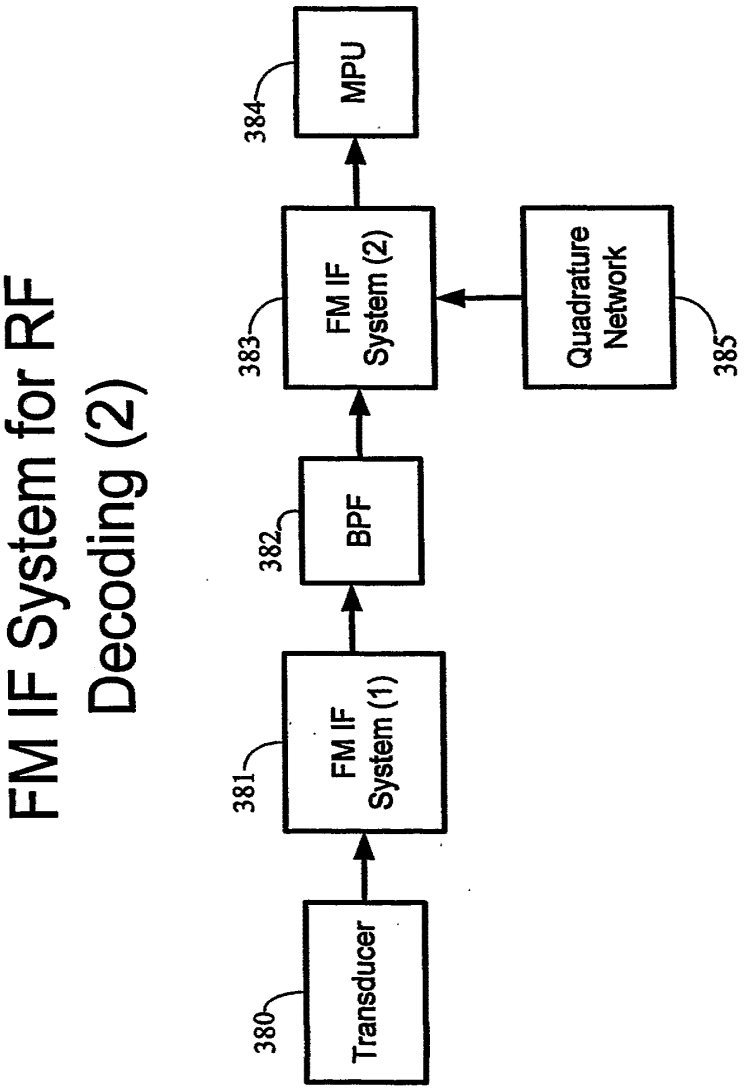

FM IF System for RF Decoding (2)
Transducer
380
FM IF System (1)
381
BPF
382
FM IF System (2)
383
MPU
384
Quadrature Network
385

FIG. 38

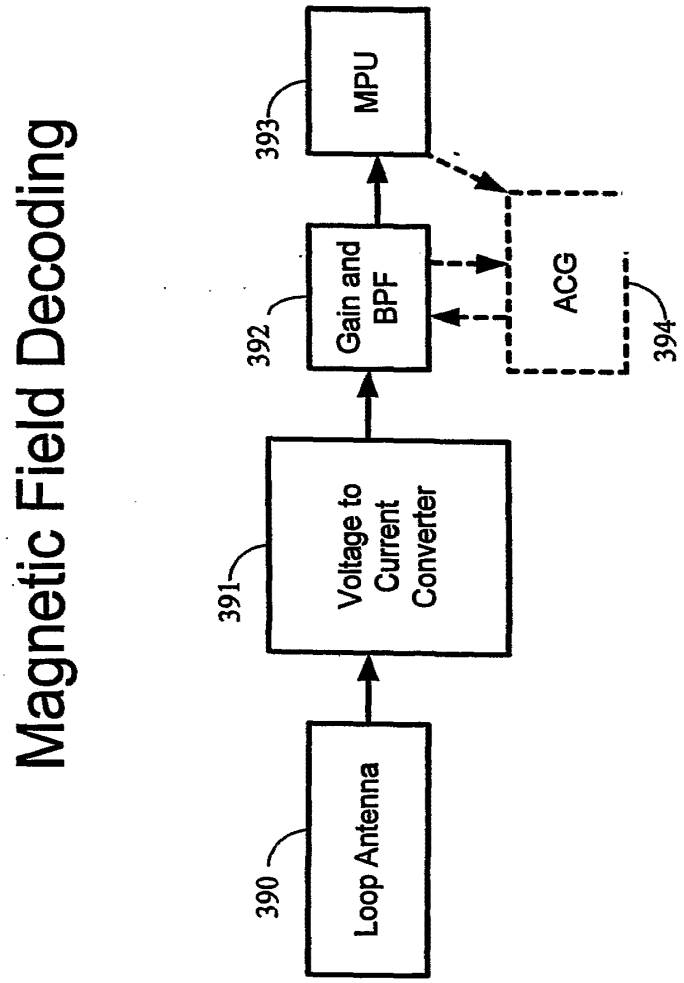

Magnetic Field Decoding
Loop Antenna
390
Voltage to Current Converter
391
Gain and BPF
392
MPU
393
ACG
394

FIG. 39

Using Hardware PLL for Decoding

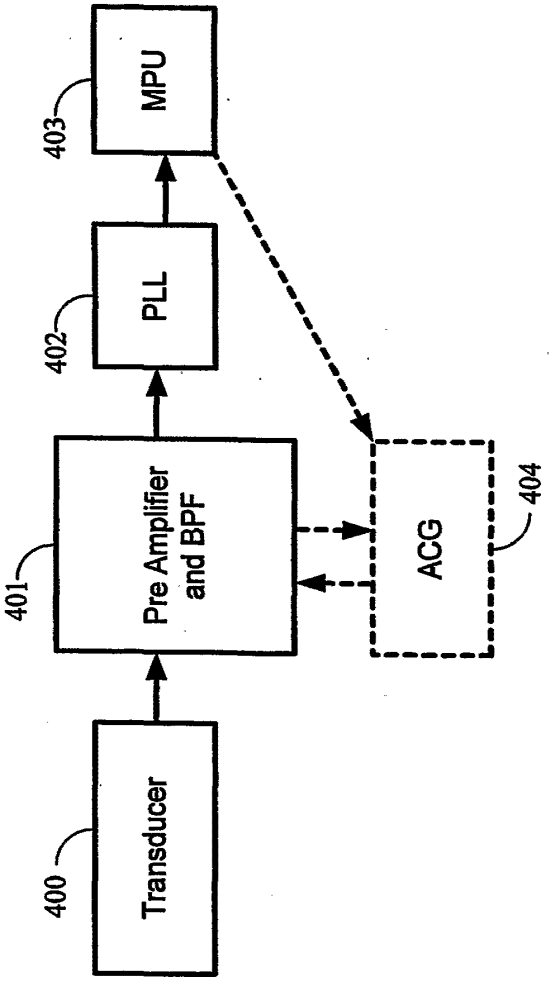


FIG. 40

Using Software PLL for Decoding

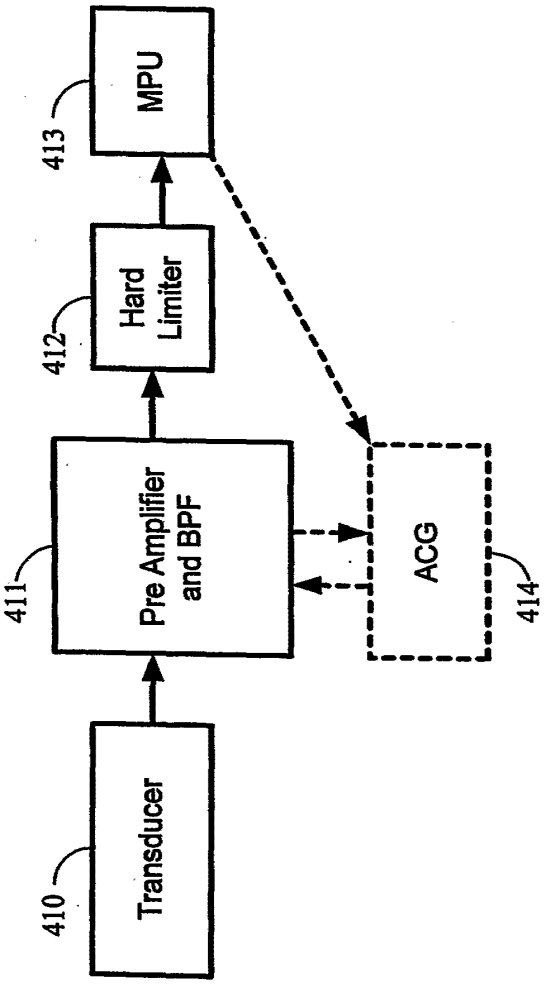


FIG. 41

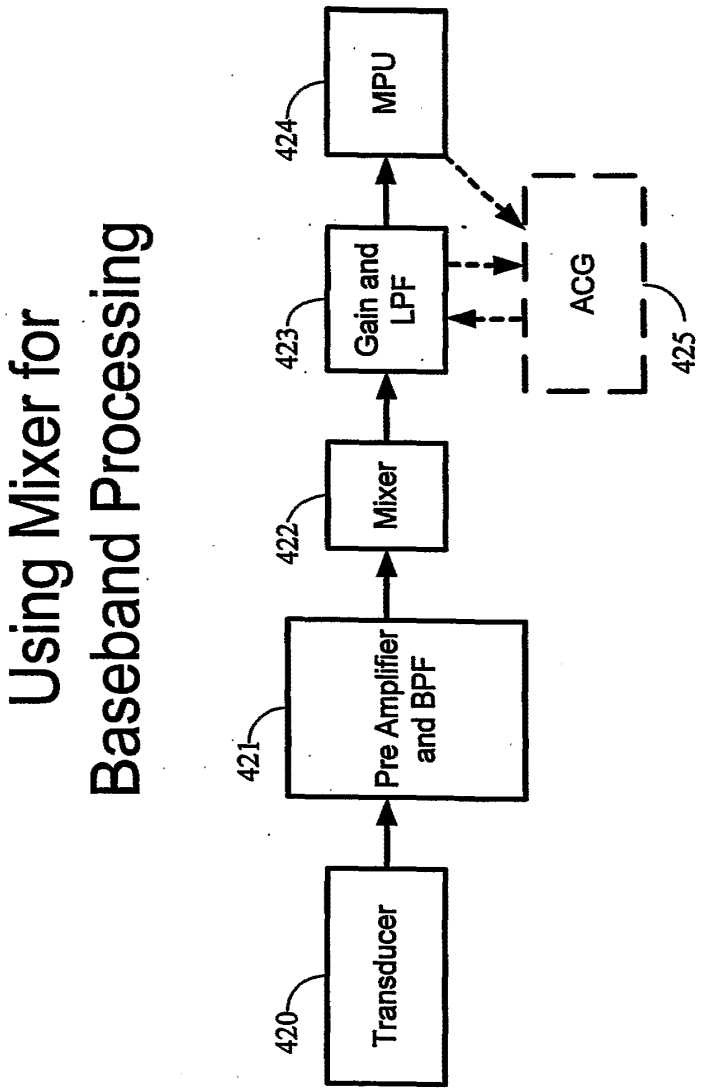

Using Mixer for Baseband Processing
Transducer
420
Pre Amplifier and BPF
421
Mixer
422
Gain and LPF
423
MPU
424
ACG
425

FIG. 42

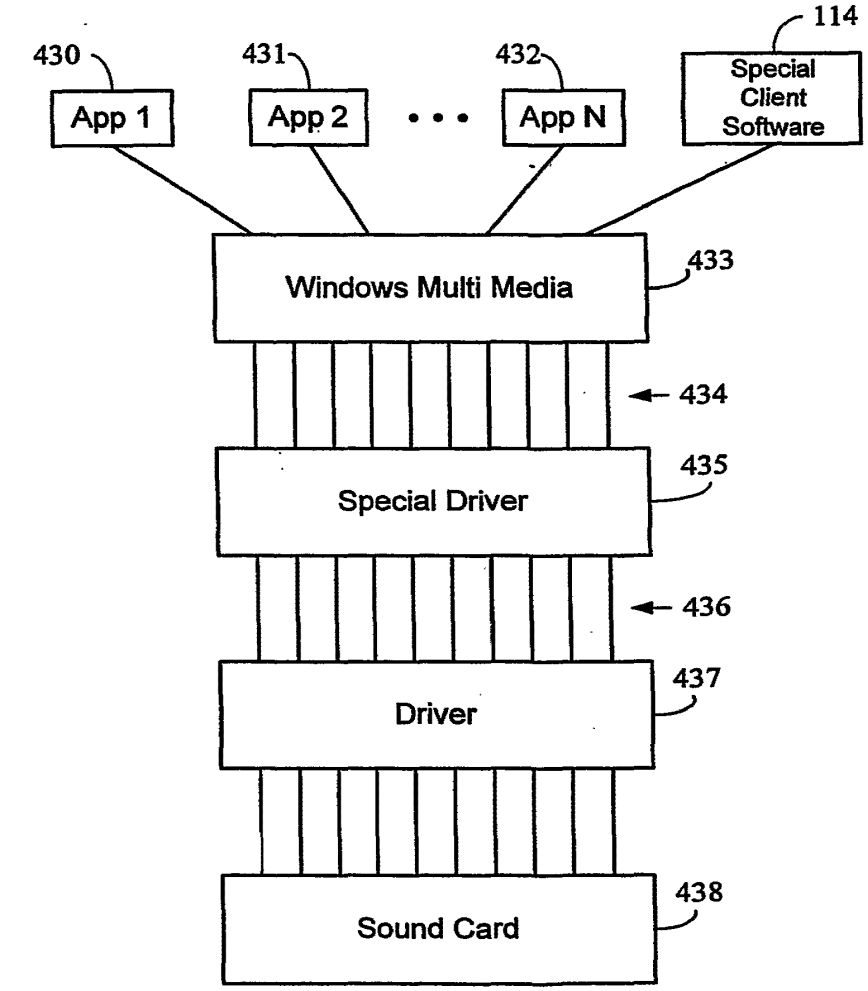

CONCURRENT OPERATION OF MULTIPLE RECORDING SOFTWARE
114
430
431
432
App 1
App 2
App N
Special Client Software
Windows Multi Media
433
434
Special Driver
435
436
Driver
437
Sound Card
438

FIG. 43

CONCURRENT OPERATION OF MULTIPLE RECORDING SOFTWARE

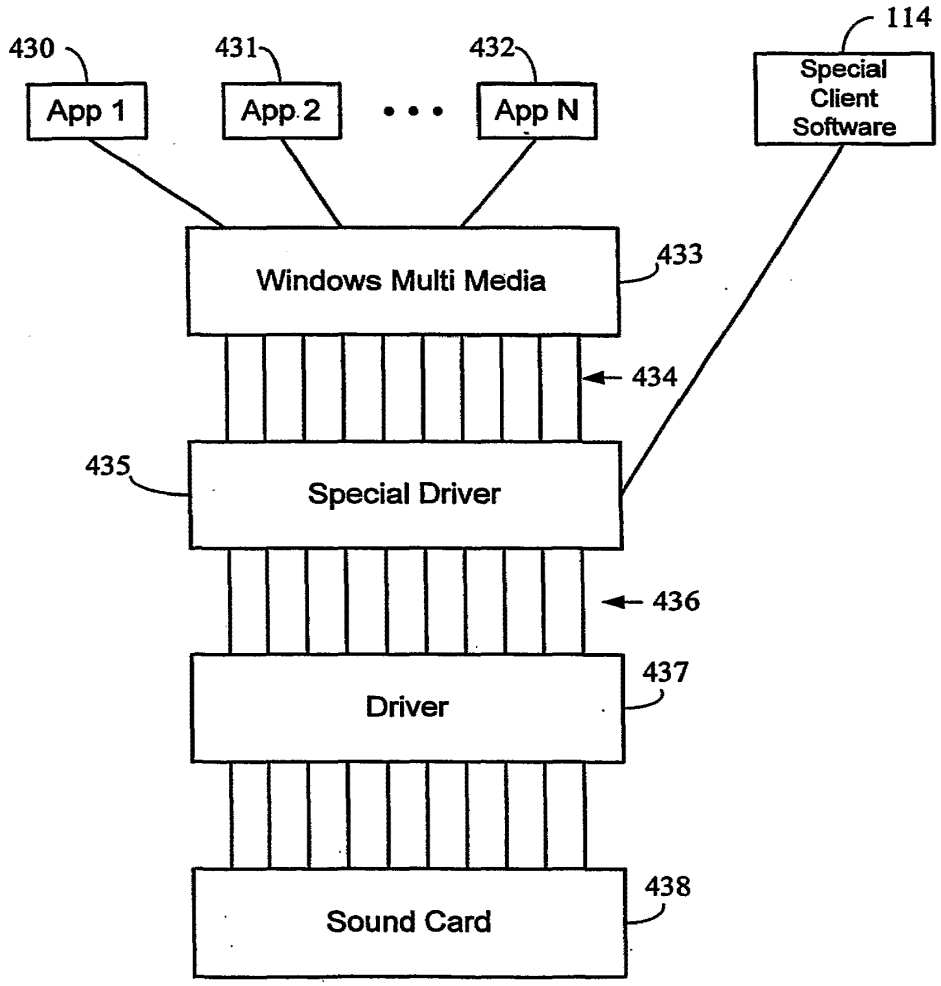


FIG. 44

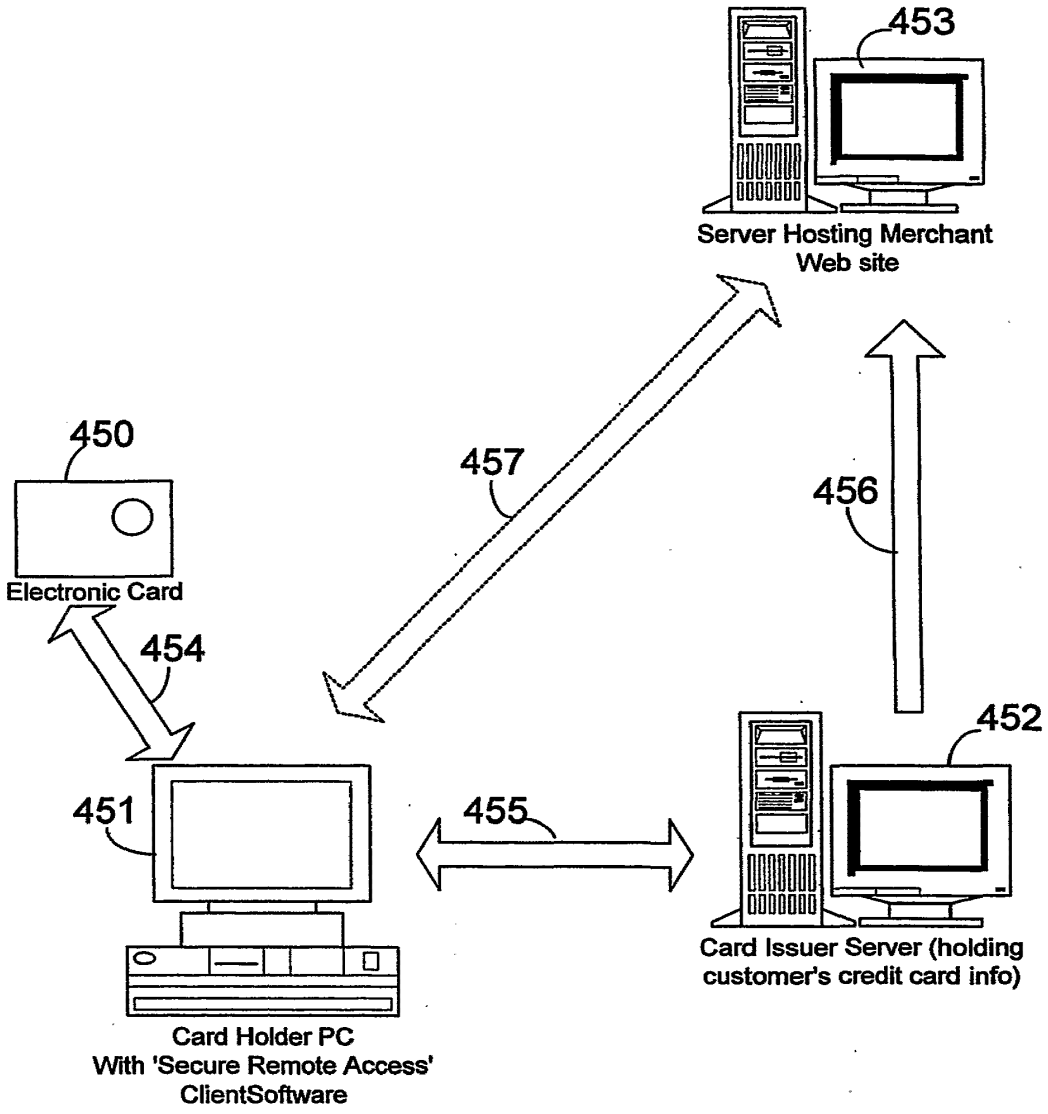

453
Server Hosting Merchant Web site
450
Electronic Card
457
456
454
452
451
455
Card Issuer Server (holding customer's credit card info)
Card Holder PC With 'Secure Remote Access' ClientSoftware

FIG. 45

APPLICATIONS

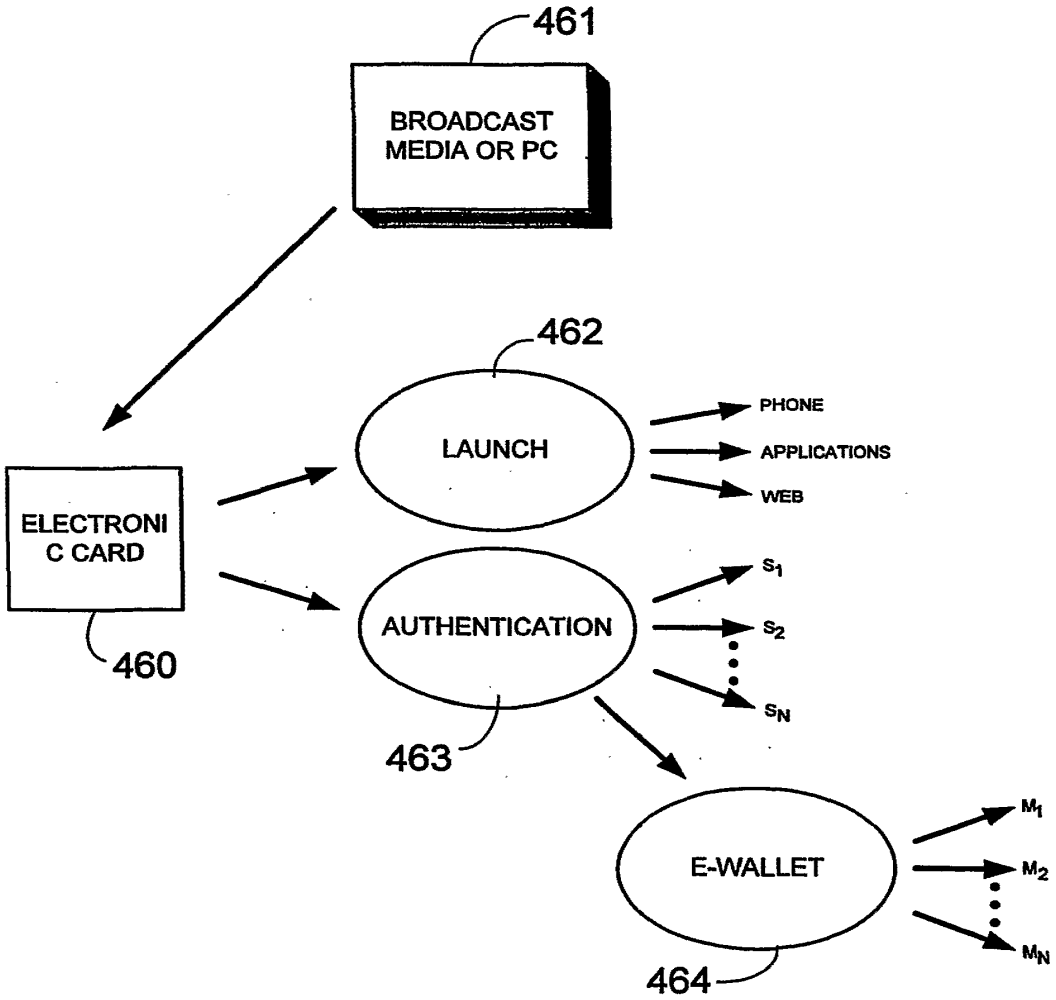


FIG. 46

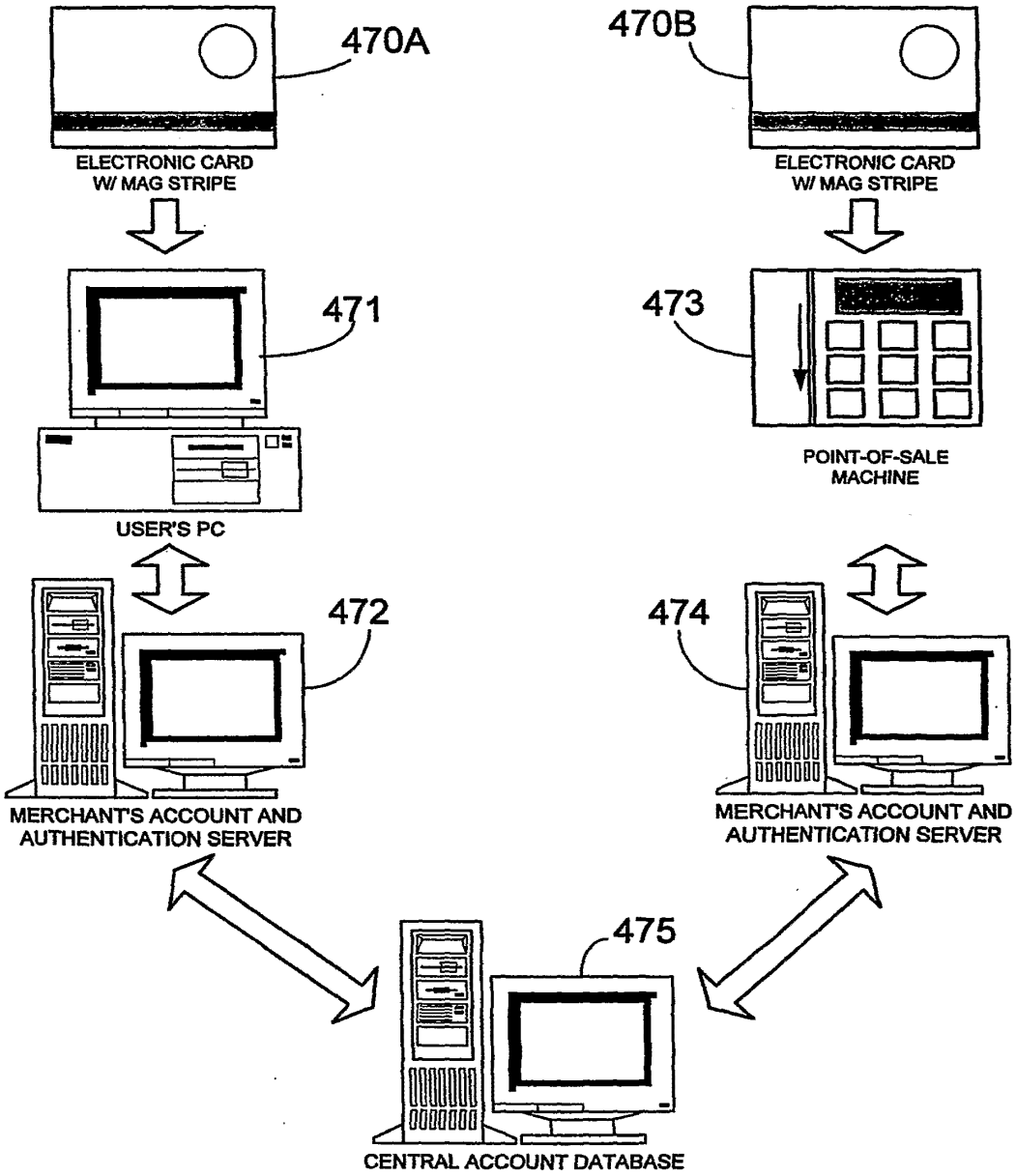

470A
ELECTRONIC CARD
W/ MAG STRIPE
470B
ELECTRONIC CARD
W/ MAG STRIPE
471
USER'S PC
473
POINT-OF-SALE
MACHINE
472
MERCHANT'S ACCOUNT AND
AUTHENTICATION SERVER
474
MERCHANT'S ACCOUNT AND
AUTHENTICATION SERVER
475
CENTRAL ACCOUNT DATABASE

FIG. 47

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 November 2012 (15.11.2012)

WIPO | PCT

(10) International Publication Number
WO 2012/154915 A1

(51) International Patent Classification:
G06Q 40/02 (2012.01)

(21) International Application Number:
PCT/US2012/037237

(22) International Filing Date:
10 May 2012 (10.05.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

61/484,588	10 May 2011 (10.05.2011)	US
61/484,566	10 May 2011 (10.05.2011)	US
61/484,576	10 May 2011 (10.05.2011)	US
61/484,547	10 May 2011 (10.05.2011)	US

(71) Applicant *(for all designated States except US)*: **DYNAMICS INC.** [US/US]; 493 Nixon Road, Cheswick, PA 15024 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **MULLEN, Jeffrey, D.** [US/US]; 731 South Negley Avenue, Apartment #2, Pittsburgh, PA 15232 (US). **RIGATTI, Christopher, J.** [US/US]; 321 Jacksonia Street, Pittsburgh, PA 15212 (US). **WALLACE, Michael, T.** [US/US]; 202 North Trailwood Road, Payson, AZ 15024 (US).

(74) Agent: **WALLACE, Michael, T.**; 493 Nixon Road, Cheswick, PA 15024 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) **Title**: SYSTEMS, DEVICES, AND METHODS FOR MOBILE PAYMENT ACCEPTANCE, MOBILE AUTHORIZATIONS, MOBILE WALLETS, AND CONTACTLESS COMMUNICATION MECHANISMS

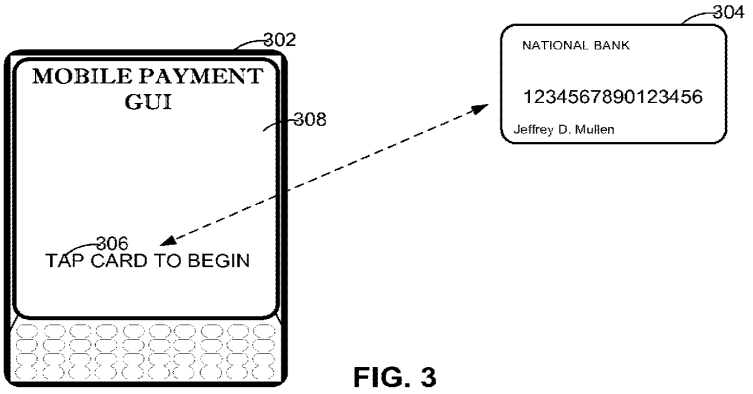


FIG. 3

(57) **Abstract**: A mobile device may provide payment acceptance and/or payment authorization for purchases, payments and/or money transfers by accepting payment information from a powered, or a non-powered, card using a contactless communication channel formed between the card and the mobile device. The payment information may be communicated by the mobile device to network entities that may be used to settle/authorize such purchase, payment and/or money transfer transactions. Physical cards may be presented to a mobile device to establish a contactless communication channel between the physical card and the mobile device. Information communicated by the physical card may be received, stored, and used by the mobile device to generate a mobile wallet of virtual cards.

WO 2012/154915 A1

SYSTEMS, DEVICES, AND METHODS FOR MOBILE PAYMENT ACCEPTANCE, MOBILE AUTHORIZATIONS, MOBILE WALLETS, AND CONTACTLESS COMMUNICATION MECHANISMS

Background of the Invention

[0001] This invention relates to mobile devices and related systems.

Summary of the Invention

[0002] A mobile device is provided that may be used as a point-of-sale terminal. A contactless communication channel may, for example, be formed between the mobile device and a payment card to communicate payment information from the payment card to the mobile device. The mobile device may, for example, use the communicated payment information to complete a purchase transaction that may be initiated by the mobile device. Accordingly, for example, no payment information need reside on the mobile terminal to complete a payment transaction. Instead, an application may be remotely activated, or a user of a mobile device may activate an application on the mobile device, that allows the mobile device to accept payment

information directly from a payment card before and/or during a payment transaction.

[0003] A mobile device may, for example, provide a browsing activity where goods and/or services may be located for purchase on a website (e.g., an Amazon or eBay website). An application may, for example, be executed on a mobile device that may communicate with a checkout application running on a website. Payment information may be exchanged directly from a user's payment card to the checkout application using the user's mobile device. In so doing, for example, a mobile device may be used as a contactless payment acceptance terminal.

[0004] A user may be provided an option of storing payment information associated with a payment card within a memory of the mobile device. Accordingly, for example, a mobile device may store payment information associated with one or more payment accounts. In so doing, for example, a mobile device may store multiple payment accounts that may be recalled from a memory of the mobile device at the user's request to complete a payment transaction.

[0005] A mobile device may detect the presence of a card that is brought within a communication distance of a contactless interface of the mobile device. For example, a card having RFID capability may communicate with an RFID device of a mobile device when the card comes within a distance (e.g., up to 2 inches) of the mobile device. Accordingly, for example, a card type (e.g., a powered card or a non-powered card) may be identified by the mobile device.

[0006] A non-powered card may, for example, communicate one, two, and/or three tracks of magnetic

stripe data to a mobile device via a contactless interface of the mobile device. Accordingly, a processor of a mobile device may identify an account type (e.g., credit or debit) that may be associated with the non-powered card by inspection of magnetic stripe data (e.g., account number) received from the non-powered card.

[0007] A powered card may, for example, communicate information (e.g., information within discretionary data fields) to a contactless interface of a mobile device. In so doing, for example, the additional information may be analyzed by a processor of the mobile device to determine that a detected card is a powered card having increased capability. Accordingly, for example, a user of a powered card may select a feature (e.g., pay with credit) on the powered card and a processor of a mobile device may detect that such a feature is selected based upon an analysis of information (e.g., discretionary data) received from the powered card.

[0008] A mobile device may validate a payment card. For example, a mobile device may request entry of a PIN after a payment card is presented to the mobile device and payment information is communicated to the mobile device by the payment card. Once entered, a mobile device may, for example, access a server associated with the payment card's issuing entity to validate the PIN. Alternately, for example, a processor of a mobile device may compare the PIN entry against local memory contents of the mobile device to validate the entered PIN.

[0009] As per another example, a mobile device may validate a payment card by requiring that the physical

payment card be present during a payment transaction. Accordingly, for example, a mobile device may require that a physical payment card be tapped against the mobile device so that a contactless communication channel may be formed between the payment card and the mobile device to verify the identity of the payment card. Accordingly, for example, identifying information communicated by the payment card to the mobile device may be compared against information previously stored within a memory of the mobile device that may be associated with the payment card.

[0010] One or more payment cards may, for example, be presented to a mobile device to complete a purchase transaction. Accordingly, for example, split-payment options may be offered by a mobile device. In so doing, for example, a first payment card may be tapped against a mobile device and accepted by the mobile device as a first form of partial payment, a second payment card may be tapped against a mobile device and accepted by the mobile device as a second form of partial payment, and so on. A mobile device may, for example, allow a user to select an amount for each partial payment and may settle each partial payment amount with each respective issuer of each payment card presented for partial payment.

[0011] A mobile device may provide checkout options to a user. For example, a mobile device may allow a user to associate purchase categories (e.g., groceries, auto repair, or entertainment) to purchases transacted by the mobile device so that the user may prepare a more detailed accounting of his or her expenditures. As per another example, a rewards card may be tapped against a mobile device so that rewards card

information may be credited with purchases transacted by the mobile device.

[0012] A mobile device may provide receipt delivery options to a user. For example, a mobile device may allow a user to select one of many receipt delivery options (e.g., text messaging, email or autonomous delivery to accounting software executed by a processor of the mobile device). Other receipt options may be provided by a mobile device in a graphical format (e.g., a barcode) so that proof-of-purchase may be verified by a reader (e.g., a barcode reader).

[0013] Money transfers may, for example, be transacted by a mobile device. One or more payment accounts (e.g., a car account or a utility account) may be selected by a user of a mobile device to receive a payment transacted by the mobile device. Payment information may be recalled from memory and/or entered by a user of the mobile device and then communicated to network entities by the mobile device to complete payment transactions.

[0014] Person to person transfers may, for example, be transacted by a mobile device. A user of a mobile device may, for example, tap a payment card against the mobile device to communicate source account information to the mobile device where funds are to be withdrawn. A person receiving a transfer of funds may, for example, tap his or her payment card against a device (e.g., a mobile device) to communicate target account information where funds are to be deposited. A mobile device may, for example, gather source and target account information and communicate such information to network entities to complete the funds transfer transaction.

[0015] A mobile device may, for example, provide a scanning capability (e.g., via a camera) to scan images (e.g., barcodes) that may be analyzed by a processor of the mobile device. Accordingly, for example, a mobile device may be used to scan product information from a product tag (e.g., a barcode) to select an item for purchase. As items are selected for purchase, scanned information is processed and displayed by the mobile device to produce a summary of items that may be selected for purchase. The mobile device may, for example, collect payment information from a payment card via a contactless communication channel and then use the payment information to complete a purchase transaction for the items scanned by the mobile device.

[0016] A mobile device may access electronic billing information via one or more communication capabilities of the mobile device. A merchant (e.g., a restaurant) may provide access to an electronic tab generated by the merchant (e.g., a bill generated by a restaurant for a dinner for two). Items billed by the merchant may be accessed by a user of a mobile device and displayed by the mobile device to produce a summary of items billed. The mobile device may, for example, collect payment information from a payment card via a contactless communication channel and then use the payment information to complete a purchase transaction for the billed items.

[0017] Any mobile device, such as a laptop computer, a mobile telephonic device (e.g., a cellular phone), a PDA, an MP3 player, or a positioning device (e.g., a GPS) may be a point-of-sale terminal. Accordingly, for example, a mobile device may accept payment information from any payment card, communicate such payment

information via a network, complete a settlement process with network entities (e.g., an issuer or a payment server) on such a network, and provide results (e.g., an electronic receipt) of the completed purchase transaction to a user of the mobile device.

[0018] A mobile device may include a contactless communication device. Accordingly, for example, a mobile device may communicate with any card having contactless communication capability. For example, a card (e.g., a non-powered card) may include a near-field communication device (e.g., an RFID tag) that may communicate with a contactless communication device of a mobile device to form a two-way communication channel between the card and the mobile device. In so doing, for example, a non-powered card may communicate one, two, and/or three tracks of magnetic stripe information to a mobile device before and/or during a purchase transaction conducted by the mobile device.

[0019] A card (e.g., a powered card) may include a near-field communication device (e.g., an RFID) that may communicate with a contactless communication device of a mobile device. A powered card may, for example, include a battery, a processor, memory, and a manual input interface (e.g., one or more buttons) that may allow a user of the powered card to programmably communicate information to a mobile device. For example, a powered payment card may include a feature associated with a button that allows a user to, for example, pay with credit or pay with debit. Accordingly, for example, a powered payment card may communicate such a payment selection within discretionary data fields of one or more tracks of magnetic stripe data.

[0020] A powered card may, for example, include circuitry to simulate touch (e.g., a capacitance change) in order to form a contactless communication channel with a mobile device. Accordingly, for example, a powered card may be pressed against a touch-sensitive display of a mobile device and information may be communicated by the powered card to the mobile device through a series of card-simulated touches that may be detected by the touch-sensitive display of the mobile device and processed by a processor of the mobile device as data communicated by the powered card.

[0021] A powered card may, for example, include a light sensor to form a contactless communication channel with a mobile device. Accordingly, for example, a powered card may be pressed against a display of a mobile device and information may be communicated from the mobile device to the powered card through a series of light pulses generated by the display of the mobile device. A frequency, pulse width, and/or a pulse intensity of light pulses may, for example, be detected by a processor of a powered card as data communicated by a mobile device.

[0022] A powered card may, for example, include a light source (e.g., an LED) to form a contactless communication channel with a mobile device. Accordingly, for example, a powered card may emit varying light pulses from an LED that may be detected by a motion-capture device (e.g., a camera) of a mobile device as data communicated by the powered card. A powered card may, for example, include sound emission capabilities that may be detected by a microphone of a mobile device as data communicated by the powered card through a contactless communication channel. A mobile

device may, for example, include sound emission capabilities that may be detected by a microphone of a powered card as data communicated by the mobile device through a contactless communication channel.

[0023] A user may communicate information directly from a card to a memory location of a mobile device via a contactless communication channel between the card and the mobile device. Accordingly, for example, a mobile device may store information (e.g., payment information) associated with one or more cards (e.g., one or more payment cards) that have been presented within a proximity to the mobile device. In so doing, for example, a mobile device may be a mobile wallet having multiple accounts (e.g., payment, identification, and travel accounts) stored within a memory of the mobile wallet where each account may be recalled from a memory of the mobile wallet at the user's request to perform a function (e.g., to complete a payment transaction).

[0024] A mobile device may detect the presence of a card that is brought within a communication distance of a contactless interface of the mobile device. A card may, for example, provide RFID capability that may communicate with an RFID device of a mobile device when the card comes within a communication distance of the mobile device. Accordingly, for example, a card type may be identified by the mobile device and information associated with the card type may be communicated from the card to the mobile device. Information received by the mobile device from the card may be autonomously categorized by the mobile device in accordance with a card type and the information may be stored and

displayed to a user in accordance with the categorization.

[0025] A card (e.g., a non-powered payment card) may, for example, communicate one, two, and/or three tracks of magnetic stripe data to a mobile device via a contactless interface. Accordingly, for example, a processor of a mobile device may identify a card type (e.g., a payment card) by analyzing the magnetic stripe data received from the card. A processor of a mobile device may, for example, determine an account type (e.g., credit or debit) that may be associated with the non-powered payment card by inspection of magnetic stripe data (e.g., account number) received from the non-powered card.

[0026] A powered card may, for example, communicate information to a contactless interface of a mobile device. In so doing, for example, additional information (e.g., information presented in discretionary data) may be identified by a processor of the mobile device to determine that a detected card is a powered card having increased capability. Accordingly, for example, a user of a powered card may select a feature (e.g., pay with credit) on the powered card and a processor of a mobile device may detect that such a feature is selected based upon an analysis of the information received from the powered card.

[0027] A mobile device may, for example, validate a payment card. For example, a mobile device may request entry of a PIN after a payment card is presented to the mobile device. Once a PIN is entered, a mobile device may, for example, access a server associated with the issuing entity to validate the PIN. A processor of a mobile device may, for example, compare the PIN entry

against memory contents of the mobile device to locally validate the entered PIN.

[0028] Data received from a card may, for example, be encrypted. Accordingly, for example, data received from a card may be stored in an encrypted state and decrypted upon receipt of a decryption key. A decryption key may, for example, be received from a sponsoring entity of the card (e.g., a card issuer's server). Decrypted data may, for example, be destroyed such that each usage of encrypted data may require a decryption key prior to usage. Alternately, for example, decrypted data may be stored within a protected memory of the mobile device and kept for future use.

[0029] A user of a mobile device may, for example, extract physical, or real, cards (e.g., payment, identification, travel, and rewards cards) from the user's physical wallet or purse and may convert each physical card into a virtual equivalent card that resides electronically within the mobile device. Accordingly, for example, each physical card (e.g., a powered card or a non-powered card) may be brought within a proximate, or touching, relationship with a mobile device to create a contactless communication channel. Card information (e.g., cardholder data, card data, and card configuration data) may, for example, be communicated by the card to the mobile device via such a contactless communication channel. In so doing, for example, a virtual card may be created within the mobile device that is both visibly and functionally equivalent to its physical counterpart.

[0030] A non-powered card may, for example, be virtually rendered onto a display of a mobile device in

a manner that resembles its physical counterpart. Card and cardholder information may, for example, be communicated by the non-powered card to the mobile device and rendered onto a virtual card that may be displayed by a processor of the mobile device. Accordingly, for example, the functionality of the physical card (e.g., a non-powered payment card) may be imparted to the virtual card by the mobile device when the mobile device communicates information (e.g., payment information) that may be associated with the non-powered payment card. As per one example, a mobile device may communicate payment information associated with a virtual card that may be displayed on a GUI of the mobile device when the mobile device is brought within a communication distance of a merchant terminal to complete a purchase transaction (e.g., an RFID device of the mobile device may communicate with an RFID device of a merchant terminal to exchange payment information between the mobile device and the merchant terminal to complete the purchase transaction). As per another example, a mobile device may communicate payment information associated with a virtual card when the mobile device accesses a network entity (e.g., a payment server) via a wireless network (e.g., a cellular network or a Wi-Fi hotspot) to complete a purchase transaction using the communicated payment information.

[0031] A powered card may, for example, be virtually rendered onto a display of a mobile device in a manner that resembles its physical counterpart. A powered card may, for example, be virtually rendered onto a display of a mobile device in a manner that provides user interface functionality that may be associated

with the physical counterpart. A powered card may, for example, communicate configuration information (e.g., button placement and associated functionality, display placement and associated functionality and input/output functionality) to a processor of a mobile device and the processor may render such a configuration onto a virtual card such that the configuration of the virtual card provides substantially identical functionality as compared to its physical counterpart.

[0032] As per one example, a powered card (e.g., a powered payment card) may include one or more buttons that when activated determine a method of payment to be used to complete a transaction (e.g., pressing one button may invoke a credit payment transaction while pressing another button may invoke a debit payment transaction). Accordingly, for example, a virtual card may be rendered onto a display of a mobile device that includes the same functionality, such that when one virtual button is touched on the virtual card, a credit payment message is communicated by the mobile device and when another virtual button is touched on the virtual card, a debit payment message is communicated by the mobile device.

[0033] As per another example, a powered card may be programmed for a particular feature by pressing a button on the powered card associated with that feature. Accordingly, for example, a powered card may communicate information associated with a selected feature to a mobile device and a processor of the mobile device may render a virtual card on a GUI of the mobile device in accordance with the selected feature. In so doing, for example, a powered card may be selected as a powered payment card with a debit feature

and the selected feature may be communicated to a mobile device (e.g., the debit feature may be communicated to a mobile device within a discretionary data field of a magnetic stripe message). The resulting virtual payment card rendered onto a display of the mobile device may, for example, provide a virtual payment card having a fixed payment feature (e.g., a fixed debit payment feature).

[0034] A mobile device may, for example, challenge a user of the mobile device to enter a password (e.g., a PIN) that may be associated with a card. A mobile device may, for example, require a password before a virtual card may be created and stored within the mobile device. A mobile device may, for example, allow a virtual card to be created and stored within a mobile device, but may challenge a user of the mobile device to enter a password associated with the virtual card before it can be recalled from a memory of the mobile device and used (e.g., used to complete a purchase transaction).

[0035] A user may, for example, participate in the personalization of a virtual card that may be stored within a memory of a mobile device. A mobile device may, for example, store various logos (e.g., issuer logos, network brand logos, and merchant logos) within a memory of the mobile device and may allow a user of the mobile device to use a GUI of the mobile device to personalize an appearance of a virtual card with such logos. Accordingly, for example, a user may perform drag-and-drop operations, alphanumeric entry operations, and any other operation to personalize an appearance of a virtual card stored within a memory of the mobile device.

[0036] A processor of a mobile device may, for example, organize two or more virtual cards for display on a GUI of the mobile device. A mobile device may, for example, keep track of a number of usages of one or more virtual cards and may sort such virtual cards within a list of displayed virtual cards so that a user may easily access his or her most used virtual card from a top of the displayed list. A mobile device may, for example, track a location of a user of the mobile device and organize a list of virtual cards in accordance with such a location. Accordingly, for example, a user may be shopping within a general merchandise store (e.g., Target), a processor of the user's mobile device may track the user's position to the Target store and the processor of the user's mobile device may display a virtual card (e.g., a Target gift card) at the top of a displayed list of virtual cards based upon the user's location. In so doing, for example, a virtual card most pertinent to the user's location may be sorted to the top of a displayed list of virtual cards for easy and convenient access by the user.

[0037] A user may, for example, select one virtual card from a list of virtual cards presented by a GUI of a mobile device and may perform one of many operations on the selected virtual card. A user may, for example, conduct a purchase transaction using a virtual payment card selected from a list of virtual cards. Accordingly, for example, a user may place a mobile device within a vicinity of a merchant terminal and may communicate payment information associated with a selected payment card to the merchant terminal. As per another example, payment information associated with a

selected virtual card may be communicated to a network entity (e.g., a payment server or an issuer's server) by the mobile device to complete a purchase transaction.

[0038] A mobile device may, for example, receive an electronic receipt for the purchase transaction either via a communication channel established between the mobile device and the merchant terminal or via other communication channels (e.g., text messaging or email exchange with a network entity such as a payment server). A user may, for example, view documents (e.g., receipts or bank statements) that may be associated with a virtual card. Accordingly, for example, a mobile device may collect and store documents associated with a virtual payment card and may display the associated documents upon request from the user. A GUI of a mobile device may, for example, allow a user to annotate documents that may be associated with a virtual card (e.g., a user may make a note that may be electronically attached to an electronic receipt that may be associated with a virtual payment card).

[0039] Other cards (e.g., other virtual cards) may be associated with a selected virtual card and those associations may be viewed from a GUI of the mobile device. For example, a payment card may be associated with a rewards card, such that in response to a request from a user of a mobile device, a processor of the mobile device may display the associations to the payment card and may use the associated virtual cards in support of a purchase transaction (e.g., the associated rewards card may be used during a payment transaction conducted with the selected virtual payment

card so that the rewards account may accrue rewards points for the purchase transaction).

[0040] A mobile device may, for example, allow a user of the mobile device to cancel an account that may be associated with a virtual card stored within the mobile device. Accordingly, for example, a virtual payment card may be stored within a mobile device and may be associated with a payment account that is administered by an issuing entity of the payment account. A mobile device may, for example, communicate with such an issuing entity to cancel a payment account that may be associated with a virtual payment card stored within the mobile device. A mobile device may, for example, negotiate with other issuing entities to determine when new payment card offers may be available and to allow a user of the mobile device to accept such payment card offers. Once accepted, a user of a mobile device may conduct other transactions with the newly accepted payment card offers (e.g., account balance(s) associated with existing virtual cards may be transferred to the newly accepted payment card via a request made by the mobile device and an issuing server).

[0041] Any mobile device, such as a laptop computer, a mobile telephonic device (e.g., a cellular phone), a PDA, an MP3 player, or a positioning device (e.g., a GPS) may be a mobile wallet. Accordingly, for example, a mobile device may accept payment and other information from any payment card, store and display such information as a virtual card on a GUI of the mobile device, communicate such payment information via a wired and/or a wireless network, complete a settlement process with network entities (e.g., an

issuer or a payment server) on such a network, and provide results (e.g., an electronic receipt) of the completed purchase transaction to a display of the mobile device.

[0042] A mobile device may include a contactless communication device. Accordingly, for example, a mobile device may communicate with any card having contactless communication capability. For example, a card (e.g., a non-powered card) may include a near-field communication device (e.g., an RFID tag) that may communicate with a contactless communication device of a mobile device to form a two-way communication channel between the card and the mobile device. In so doing, for example, a non-powered card may communicate one, two, and/or three tracks of magnetic stripe information to a mobile device before and/or during a purchase transaction conducted by the mobile device.

[0043] A card (e.g., a powered card) may include a near-field communication device (e.g., an RFID) that may communicate with a contactless communication device of a mobile device. A powered card may, for example, include a battery, a processor, memory, and a manual input interface (e.g., one or more buttons) that may allow a user of the powered card to programmably communicate information to a mobile device. For example, a powered payment card may include a feature associated with a button that allows a user to, for example, pay with credit or pay with debit. Accordingly, for example, a powered payment card may communicate such a payment selection within discretionary data fields of one or more tracks of magnetic stripe data.

[0044] A powered card may, for example, include circuitry to simulate touch (e.g., a capacitance change) in order to form a contactless communication channel with a mobile device. Accordingly, for example, a powered card may be pressed against a touch-sensitive display of a mobile device and information may be communicated by the powered card to the mobile device through a series of card-simulated touches that may be detected by the touch-sensitive display of the mobile device and processed by a processor of the mobile device as data communicated by the powered card.

[0045] A powered card may, for example, include a light sensor to form a contactless communication channel with a mobile device. Accordingly, for example, a powered card may be pressed against a display of a mobile device and information may be communicated from the mobile device to the powered card through a series of light pulses generated by the display of the mobile device. A frequency, pulse width, and/or a pulse intensity of light pulses may, for example, be detected by a processor of a powered card as data communicated by a mobile device.

[0046] A powered card may, for example, include a light source (e.g., an LED) to form a contactless communication channel with a mobile device. Accordingly, for example, a powered card may emit varying light pulses from an LED that may be detected by a motion-capture device (e.g., a camera) of a mobile device as data communicated by the powered card. A powered card may, for example, include sound emission capabilities that may be detected by a microphone of a mobile device as data communicated by the powered card through a contactless communication channel. A mobile

device may, for example, include sound emission capabilities that may be detected by a microphone of a powered card as data communicated by the mobile device through a contactless communication channel.

[0047] A mobile device may be used as an authorization terminal to conduct transactions (e.g., purchase transactions) using the mobile device. Purchase transactions may, for example, be completed by a mobile device using payment information stored within a memory of the mobile device. In order to conduct a purchase transaction, a processor of a mobile device may, for example, first require security credentials to authorize a purchase transaction. Security credentials may, for example, be any type of information that may be communicated to a mobile device by a contactless device using a contactless communication channel (e.g., an RFID communication channel).

[0048] Security credentials may, for example, be payment information that may be communicated to a processor of a mobile device by a payment card (e.g., a powered or a non-powered payment card). Accordingly, for example, if payment information communicated to a processor of a mobile device by a physical payment card matches payment information previously stored within a memory of the mobile device, the mobile device may authorize the purchase transaction.

[0049] As per an example, a mobile device may receive payment information (e.g., a payment account number and an expiration date) from a payment card via a contactless communication channel and may store such payment information within a memory of the mobile device for future use. Prior to conducting a requested purchase transaction, a processor of a mobile device

may first require that a physical payment card be used to authorize the purchase transaction. Accordingly, for example, the same physical payment card that was used to originally communicate payment information to a processor of the mobile device may be required to once again communicate payment information in order to authorize the purchase transaction. Upon verification that the newly communicated payment information matches at least a portion of payment information contained within a memory of the mobile device, the mobile device may authorize the payment transaction.

[0050] A powered card may, for example, communicate security credentials that may contain a dynamic security code and other information (e.g., at least a portion of a payment account number or a cardholder's name). Accordingly, for example, an application executed by a processor of a mobile device may synchronize with a dynamic security code generation algorithm that may be executed by a processor of the powered card. In so doing, for example, a processor of the mobile device may generate a dynamic security code in accordance with the security code generation algorithm and may compare the generated dynamic security code to a security code received from a powered card during authorization of a purchase transaction. If a match exists, for example, the purchase transaction may be authorized by the mobile device.

[0051] A mobile device may, for example, communicate security credentials received from a physical card via a contactless communication channel to a network entity (e.g., an authorization server). Accordingly, for example, the authorization server may analyze the

received security credentials and may either confirm or deny that the security credentials are authentic. A message may, for example, be communicated from the authorization server to the mobile device to either authorize or deny the purchase transaction.

[0052] A mobile device may, for example, arrange security credentials (e.g., payment information) stored within a memory of the mobile device as one or more virtual payment cards that may be provided on a display of the mobile device. Accordingly, for example, a user of a mobile device may select one or more virtual cards from a displayed list of virtual cards for use during a purchase transaction. In so doing, for example, a user may retrieve a physical payment card from his or her wallet that corresponds to the virtual payment card selected for use and may communicate (e.g., via a contactless communication channel) payment information from the physical payment card to a processor of the mobile device. Upon verification that the communicated payment information matches at least a portion of payment information stored within a memory of the mobile device, a processor of the mobile device may authorize the purchase transaction using the stored payment information.

[0053] A physical payment card may, for example, be used as a master physical payment card to authorize purchase transactions that are to be completed by the mobile device using stored payment information that does not match payment information received from the physical payment card. For example, a master physical payment card may be associated with a particular issuer and a mobile device may store several virtual cards within a memory of the mobile device having the same

issuer. Upon receipt of payment information from the master physical payment card, a processor of a mobile device may authorize purchase transactions using one or more virtual cards stored within a memory of the mobile device that may share the same issuer as the issuer of the master physical payment card.

[0054] Other devices (e.g., RFID enabled keys) may, for example, communicate security credentials via a contactless communication channel to a processor of a mobile device to authorize other transactions (e.g., non-purchase transactions) that may be conducted by the mobile device. Accordingly, for example, a processor of a mobile device may communicate commands to a wireless device (e.g., a user's car) to perform certain functions (e.g., start the engine of the user's car). In so doing, for example, a user may present an ignition key to the mobile device to communicate security credentials (e.g., a key code matched to the user's car) from the ignition key to the mobile device to authorize the requested function. Upon verification that the key code matches the key code of the user's car, for example, a processor of the mobile device may authorize the requested function and may communicate the associated command to the user's car to execute the requested function.

[0055] Any function may, for example, be authorized to be performed by a processor of a mobile device. Accordingly, for example, any decision to perform a function by a mobile device may be authorized by a processor of the mobile device. In so doing, for example, any function (e.g., checking a balance of a banking account or transitioning from paper bank statements to e-statements) that may be performed by a

processor of a mobile device may be authorized by the processor upon verification that security credentials (e.g., a bank account number) communicated to the processor from a contactless communication device (e.g., a bank card associated with the bank account) matches at least a portion of security credentials (e.g., banking information) that may be stored within a memory of the mobile device.

[0056] Any mobile device, such as a laptop computer, a mobile telephonic device (e.g., a cellular phone), a PDA, an MP3 player, or a positioning device (e.g., a GPS) may be an authorization terminal. Accordingly, for example, any mobile device may accept payment information from any physical payment card, store such payment information within a memory of the mobile device, require that the same (or associated) physical payment card communicate payment information to a processor of the mobile device, and complete a purchase transaction with network entities (e.g., an issuer or a payment server) upon verification that the communicated payment information matches at least a portion of payment information stored within a memory of the mobile device.

[0057] A mobile device may include a contactless communication device. Accordingly, for example, a mobile device may communicate with any card having contactless communication capability. For example, a card (e.g., a non-powered card) may include a near-field communication device (e.g., an RFID tag) that may communicate with a contactless communication device of a mobile device to form a two-way communication channel between the card and the mobile device. In so doing, for example, a non-powered card may communicate one,

two, and/or three tracks of magnetic stripe information to a processor of a mobile device before and/or during a purchase transaction conducted by the mobile device.

[0058] A card (e.g., a powered card) may include a near-field communication device (e.g., an RFID) that may communicate with a contactless communication device of a mobile device. A powered card may, for example, include a battery, a processor, memory, and a manual input interface (e.g., one or more buttons) that may allow a user of the powered card to programmably communicate information to a mobile device. For example, a powered payment card may include a feature associated with a button that allows a user to, for example, pay with credit or pay with debit. Accordingly, for example, a powered payment card may communicate such a payment selection within discretionary data fields of one or more tracks of magnetic stripe data.

[0059] A powered card may, for example, include circuitry to simulate touch (e.g., a capacitance change) in order to form a contactless communication channel with a mobile device. Accordingly, for example, a powered card may be pressed against a touch-sensitive display of a mobile device and information may be communicated by the powered card to the mobile device through a series of card-simulated touches that may be detected by the touch-sensitive display of the mobile device and processed by a processor of the mobile device as data communicated by the powered card.

[0060] A powered card may, for example, include a light sensor to form a contactless communication channel with a mobile device. Accordingly, for example, a powered card may be pressed against a

display of a mobile device and information may be communicated from the mobile device to the powered card through a series of light pulses generated by the display of the mobile device. A frequency, pulse width, and/or a pulse intensity of light pulses may, for example, be detected by a processor of a powered card as data communicated by a mobile device.

[0061] A powered card may, for example, include a light source (e.g., an LED) to form a contactless communication channel with a mobile device. Accordingly, for example, a powered card may emit varying light pulses from an LED that may be detected by a motion-capture device (e.g., a camera) of a mobile device as data communicated by the powered card. A powered card may, for example, include sound emission capabilities that may be detected by a microphone of a mobile device as data communicated by the powered card through a contactless communication channel. A mobile device may, for example, include sound emission capabilities that may be detected by a microphone of a powered card as data communicated by the mobile device through a contactless communication channel.

[0062] A card may include a dynamic magnetic communications device, which may take the form of a magnetic encoder or a magnetic emulator. A magnetic encoder, for example, may be utilized to modify information that is located on a magnetic medium, such that a magnetic stripe reader may then be utilized to read the modified magnetic information from the magnetic medium. A magnetic emulator, for example, may be provided to generate electromagnetic fields that directly communicate data to a read-head of a magnetic stripe reader. A magnetic emulator, for example, may

communicate data serially to a read-head of the magnetic stripe reader. A magnetic emulator, for example, may communicate data in parallel to a read-head of the magnetic stripe reader.

[0063] All, or substantially all, of the front surface, as well as the rear surface, of a card may be implemented as a display (e.g., bi-stable, non bi-stable, LCD, or electrochromic display). Electrodes of a display may be coupled to one or more touch sensors, such that a display may be sensitive to touch (e.g., using a finger or a pointing device) and may be further sensitive to a location of the touch. The display may be sensitive, for example, to objects that come within a proximity of the display without actually touching the display.

[0064] A dynamic magnetic stripe communications device may be implemented on a multiple layer board (e.g., a two-layer flexible printed circuit board). A coil for each track of information that is to be communicated by the dynamic magnetic stripe communications device may then be provided by including wire segments on each layer and interconnecting the wire segments through layer interconnections to create a coil. For example, a dynamic magnetic stripe communications device may include two coils such that two tracks of information may be communicated to two different read-heads included in a read-head housing of a magnetic stripe reader. A dynamic magnetic communications device may include, for example, three coils such that three tracks of information may be communicated to three different read-heads included in a read-head housing of a magnetic stripe reader.

[0065] Input and/or output devices may be included on a card, for example, to facilitate data exchange with the card. For example, an integrated circuit (IC) may be included on a card and exposed from the surface of the card. Such a chip (e.g., an EMV chip) may communicate information to a chip reader (e.g., an EMV chip reader). A contactless device (e.g., one or more RFID antennas and one or more associated RFID chips) may be included in a card, for example, to exchange information with an RFID device.

[0066] One or more detectors may be provided in a card, for example, to sense the presence of an external object, such as a person or device, which in turn, may trigger the initiation of a communication sequence with the external object. The sensed presence of the external object may then be communicated to a processor of the card, which in turn may direct the exchange of information between a card and the external object. Accordingly, timing aspects of the information exchange between an external object and the various I/O devices provided on a card may also be determined by circuitry (e.g., a processor) provided on a card.

[0067] The sensed presence of the external object or device may include the type of object or device that is detected and, therefore, may then determine the type of communication that is to be used with the detected object or device. For example, a detected object may include a determination that the object is a read-head housing of a magnetic stripe reader. Such an identifying detection, for example, may activate a dynamic magnetic stripe communications device so that information may be communicated to the read-head of the magnetic stripe reader. Information may be

communicated by a dynamic magnetic stripe communications device, for example, by re-writing magnetic information on a magnetic medium that is able to be read by a magnetic stripe reader or electromagnetically communicating data to the magnetic stripe reader.

[0068] As per another example, a detected object may include a determination that the object is an RFID enabled device. Such an identifying detection, for example, may cause RFID data to be communicated by a processor of a card to an RFID chip of a card. The RFID data may be temporarily contained within the RFID chip until the RFID data is communicated to a detected RFID device by an RFID antenna on the card. The RFID data may, for example, be erased from the RFID chip after being communicated to the RFID device.

[0069] A card may, for example, be an assembly of multiple printed circuit boards, electronics, one or more RFID antennas, and one or more associated RFID chips. An RFID antenna may, for example, be fabricated on one printed circuit board and an associated RFID chip may, for example, be attached to a separate printed circuit board. Communications (e.g., RFID data transfer between the RFID chip and the RFID antenna) may, for example, be transferred between separate printed circuit boards via conductive paths established between the separate printed circuit boards. An RFID antenna and an associated RFID chip may, for example, reside on the same printed circuit board so as to reduce a number of conductive traces that may be required between separate printed circuit boards.

[0070] A card assembly may, for example, be laminated such that all printed circuit boards,

electronic circuitry and components are covered in a polymer. For example, an electronics package may be provided between two layers of polymer and a liquid polymer may be introduced between these layers and hardened to form a card. A laminated card assembly may, for example, be devoid of electrical contacts on either surface of the laminated card. A laminated card assembly may, for example, provide electrical contacts (e.g., EMV chip contacts) on one or more surfaces of a laminated card assembly.

[0071] A mobile device, such as a laptop computer, a mobile telephonic device (e.g., a cellular phone), a PDA, an MP3 player, or a positioning device (e.g., a GPS) may include one or more RFID antennas and associated RFID chips. Accordingly, for example, any mobile device may establish an RFID communication channel with any other RFID enabled device (e.g., an RFID enabled card). A computing device, such as a desktop computer, may be an RFID enabled device. Accordingly, for example, any RFID enabled device (e.g., an RFID enabled card or an RFID enabled mobile device) may establish an RFID communication channel with any RFID enabled computing device.

Brief Description of the Drawings

[0072] The principles and advantages of the present invention can be more clearly understood from the following detailed description considered in conjunction with the following drawings, in which the same reference numerals denote the same structural elements throughout, and in which:

[0073] FIG. 1 is an illustration of a mobile devices constructed in accordance with the principles of the present invention;

[0074] FIG. 2 is an illustration of a network topology constructed in accordance with the principles of the present invention;

[0075] FIG. 3 is an illustration of a mobile payment system constructed in accordance with the principles of the present invention;

[0076] FIG. 4 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0077] FIG. 5 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0078] FIG. 6 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0079] FIG. 7 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0080] FIG. 8 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0081] FIG. 9 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0082] FIG. 10 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0083] FIG. 11 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0084] FIG. 12 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0085] FIG. 13 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0086] FIG. 14 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0087] FIG. 15 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0088] FIG. 16 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0089] FIG. 17 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0090] FIG. 18 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0091] FIG. 19 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0092] FIG. 20 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0093] FIG. 21 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0094] FIG. 22 is an illustration of a mobile funds transfer system constructed in accordance with the principles of the present invention;

[0095] FIG. 23 is an illustration of a mobile payment system constructed in accordance with the principles of the present invention;

[0096] FIG. 24 is an illustration of a mobile payment system constructed in accordance with the principles of the present invention;

[0097] FIG. 25 is an illustration of a mobile payment system constructed in accordance with the principles of the present invention;

[0098] FIG. 26 is a flow chart of processes constructed in accordance with the principles of the present invention;

[0099] FIG. 27 is an illustration of a mobile devices constructed in accordance with the principles of the present invention;

[0100] FIG. 28 is an illustration of a network topology constructed in accordance with the principles of the present invention;

[0101] FIG. 29 is an illustration of a mobile wallet system constructed in accordance with the principles of the present invention;

[0102] FIG. 30 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0103] FIG. 31 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0104] FIG. 32 is an illustration of a mobile wallet system constructed in accordance with the principles of the present invention;

[0105] FIG. 33 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0106] FIG. 34 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0107] FIG. 35 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0108] FIG. 36 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0109] FIG. 37 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0110] FIG. 38 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0111] FIG. 39 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0112] FIG. 40 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0113] FIG. 41 is an illustration of a mobile wallet system constructed in accordance with the principles of the present invention;

[0114] FIG. 42 is an illustration of a mobile wallet system constructed in accordance with the principles of the present invention;

[0115] FIG. 43 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0116] FIG. 44 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0117] FIG. 45 is an illustration of a mobile wallet system constructed in accordance with the principles of the present invention;

[0118] FIG. 46 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0119] FIG. 47 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0120] FIG. 48 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0121] FIG. 49 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0122] FIG. 50 is an illustration of a mobile application constructed in accordance with the principles of the present invention;

[0123] FIG. 51 is a flow chart of processes constructed in accordance with the principles of the present invention;

[0124] FIG. 52 is an illustration of mobile devices constructed in accordance with the principles of the present invention;

[0125] FIG. 53 is an illustration of a network topology constructed in accordance with the principles of the present invention;

[0126] FIG. 54 is an illustration of a mobile authorization system constructed in accordance with the principles of the present invention;

[0127] FIG. 55 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0128] FIG. 56 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0129] FIG. 57 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0130] FIG. 58 is an illustration of a mobile authorization system constructed in accordance with the principles of the present invention;

[0131] FIG. 59 is an illustration of a mobile authorization system constructed in accordance with the principles of the present invention;

[0132] FIG. 60 is an illustration of a display screen constructed in accordance with the principles of the present invention;

[0133] FIG. 61 is a flow chart of processes constructed in accordance with the principles of the present invention;

[0134] FIG. 62 is an illustration of cards constructed in accordance with the principles of the present invention;

[0135] FIG. 63 is an illustration of a network topology constructed in accordance with the principles of the present invention;

[0136] FIG. 64 is an illustration of mobile devices constructed in accordance with the principles of the present invention;

[0137] FIG. 65 is an illustration of a card constructed in accordance with the principles of the present invention;

[0138] FIG. 66 is an illustration of a card constructed in accordance with the principles of the present invention;

[0139] FIG. 67 is an illustration of a card constructed in accordance with the principles of the present invention;

[0140] FIG. 68 is an illustration of a card constructed in accordance with the principles of the present invention;

[0141] FIG. 69 is an illustration of a card constructed in accordance with the principles of the present invention;

[0142] FIG. 70 is an illustration of a card constructed in accordance with the principles of the present invention;

[0143] FIG. 71 is an illustration of a system constructed in accordance with the principles of the present invention;

[0144] FIG. 72 is an illustration of a system constructed in accordance with the principles of the present invention; and

[0145] FIG. 73 is an illustration of process flow charts constructed in accordance with the principles of the present invention.

Detailed Description of the Invention

[0146] FIG. 1 shows mobile device 100. Mobile device 100 may be any mobile device, such as a mobile telephonic device (e.g., cell phone), a PDA, an electronic tablet, an MP3 player, or a locating device (e.g., a GPS device). Accordingly, mobile device 100 may be operated in a mobile environment while a user of mobile device 100 goes about his or her daily activities (e.g., driving, shopping, walking, dining, and exercising). In addition, for example, mobile device 100 may perform multiple functions

simultaneously (e.g., a person may carry on a conversation while at the same time browsing and purchasing products on the internet).

[0147] Mobile device 100 may include audio processing devices (e.g., microphone 108 and speaker 110). Accordingly, for example, mobile device 100 may receive voice commands from a user via microphone 108 and may process such commands to perform a function. For example, a user may place mobile device 100 into a desired operational mode by speaking a command into microphone 108 that is associated with the desired operational mode. In so doing, for example, mobile device 100 may engage in hands-free operation by receiving voice commands via microphone 108 and performing functions associated with the received voice commands.

[0148] Mobile device 100 may receive data input via microphone 108. For example, a voice-band modem may generate signals in a voice-band frequency range that may be received by microphone 108. A processor of mobile device 100 may interpret the received audible information as data signals and may process the data signals as, for example, data values and/or control data input.

[0149] Mobile device 100 may include camera 102. Camera 102 may capture one or more frames of video data and store the video data within a memory of mobile device 100. Accordingly, for example, a processor of mobile device 100 may receive one or more frames of video information via camera 102 and may process the video information as data values and/or control data input. In so doing, for example, mobile device 100 may receive optical information that is sensed by camera

102 during a series of one or more video capture events that produce one or more frames of video information. The one or more frames of video information may contain one or more data elements (e.g., pixels) having properties (e.g., color, intensity, or contrast) that may be interpreted by a processor of mobile device 100 as data values and/or control data.

[0150] Mobile device 100 may include manual input interface 112. Manual input interface 112 may, for example, include keys and/or buttons that may be sensitive to manual input, such as a touch or an application of pressure. Accordingly, for example, a user of mobile device 100 may enter information into mobile device 100 via manual interface 112 to cause a processor of mobile device 100 to enter a particular mode of operation. Manual interface 112 may, for example, be used for data entry (e.g., dialing a phone number or entering data as may be requested by mobile device 100) during a particular mode of operation of mobile device 100.

[0151] Mobile device 100 may include display 104. Display 104 may provide visible information that may be utilized by a user during interaction with mobile device 100. A portion or all of display 104 may be touch sensitive such that objects making contact with display 104 or objects coming within a proximity of display 104 may be detected by a processor of mobile device 100. Accordingly, for example, mobile payment graphical user interface 106 may be provided by display 104 so that graphical information may be displayed to solicit and/or receive data entry from a user. In so doing, for example, touch-sensitive graphical user interface devices such as radio buttons, textual input

boxes, virtual buttons, pull-down menus, and navigational tools may be used for data entry to initiate, change, and/or support functions performed by mobile device 100.

[0152] FIG. 1 shows architecture 150. User interface 152 may, for example, be included within architecture 150 to allow user interaction with architecture 150. For example, a dedicated key pad or keyboard may be included within user interface 152 to allow alphanumeric data entry into architecture 150.

[0153] Architecture 150 may include one or more displays 154. Display 154 may, for example, be touch-sensitive. Accordingly, for example, display 154 may be utilized for alphanumeric data entry using virtual buttons that may be rendered onto touch-sensitive portions of display 154. In so doing, for example, touching virtual buttons that may be associated with alphabetic and numeric characters of display 154 may be detected by processor 158 as alphanumeric data entry.

[0154] Alphanumeric entry boxes may, for example, be rendered onto display 154. A user may, for example, activate a cursor within such an alphanumeric entry box by touching an area within the alphanumeric entry box. A user may utilize user interface 152 and/or a virtual keypad rendered onto display 154 to select alphanumeric characters to be placed within the alphanumeric entry box in accordance with a character position identified by an activated cursor within the alphanumeric entry box. In so doing, for example, processor 158 may receive alphanumeric characters as typed into a alphanumeric entry box of display 154 and may use such alphanumeric characters as data input.

[0155] Display 154 may, for example, provide data output from architecture 150. For example, display 154 may communicate data using a series of light pulses. Accordingly, for example, processor 158 may cause one or more portions of display 154 to produce light pulses having varying characteristics (e.g., duration, intensity, and frequency) that may communicate information via such light pulses. In so doing, for example, a device that may be sensitive to light pulses may receive information communicated by display 154 via light pulses having varying characteristics. Display 154 may, for example, communicate data using visual information that may be substantially static (e.g., a barcode).

[0156] Architecture 150 may include one or more transceivers 156. Transceiver 156 may communicate information to and/or may receive information from one or more devices. Transceiver 156 may, for example, communicate via a wireless interface with one or more cellular stations of a mobile network. Accordingly, for example, transceiver 156 may allow a mobile device (e.g., mobile device 100 of FIG. 1) to establish a communications channel with an associated cellular station. In so doing, for example, a mobile device (e.g., mobile device 100 of FIG. 1) may exchange information (e.g., voice, text, data, or multimedia) with one or more terrestrial networks (e.g., the internet or a payment network) via an associated cellular station. As per another example, transceiver 156 may exchange information with one or more other mobile devices via one or more associated cellular stations.

[0157] Transceiver 156 may, for example, communicate via a wireless interface with one or more mobile devices directly. Accordingly, for example, transceiver 156 may communicate with another mobile device without first accessing a mobile network via a cellular station of the mobile network. As per another example, transceiver 156 may, for example, communicate via a wireless interface with one or more network devices (e.g., a wireless access point) directly. Accordingly, for example, a mobile device (e.g., mobile device 100 of FIG. 1) may directly connect to a wired and/or a wireless network via any one or more wireless standards (e.g., Bluetooth or Wi-Fi) to exchange information with other devices that may be connected to the wired and/or wireless network. In so doing, for example, a wired and/or wireless network may be accessed by a mobile device without first accessing a mobile network via a cellular station of a mobile network.

[0158] Architecture 150 may include contactless communication device 162, which may communicate via any one or more contactless communication methodologies, such as for example, near field communications (e.g., RFID), Bluetooth, touch simulation, light pulsing (e.g., via an LED), and electromagnetic data communication (e.g., via a dynamic magnetic stripe communications device). Accordingly, for example, contactless communication device 162 may be compatible with any contactless device, such as for example, an RFID enabled payment card and a contactless reader (e.g., a magnetic stripe reader or an NFC reader).

[0159] A non-powered card may, for example, communicate with contactless communications device 162.

Contactless communication device 162 may, for example, establish a carrier field (e.g., an RF field) that may be modulated by a device (e.g., an RFID tag) of a non-powered payment card. In so doing, for example, an RFID tag of a non-powered payment card may derive operational power from an RF field provided by contactless communications device 162 and may communicate information (e.g., one, two, and/or three tracks of magnetic stripe data) to contactless communication device 162 by modulating the RF field produced by contactless communications device 162.

[0160] A powered card may, for example, communicate with contactless communication device 162. A powered card may, for example, include a processor, a battery, a memory, wireless communications devices (e.g., a dynamic magnetic stripe communications device or RFID) and other electronics (e.g., buttons) that may allow a user to interact with the powered card to perform one or more functions. Accordingly, for example, a powered card may be used to communicate specific information to contactless communication device 162 by selective interaction with the buttons of the powered card. In so doing, for example, a powered card may be used to interactively communicate magnetic stripe information (e.g., one, two, and/or three tracks of magnetic stripe data) to contactless communication device 162 by sending a signal to a processor of a powered card (e.g., by pressing a button on the powered card) to initiate such communications.

[0161] Contactless communication device 162 may receive variable data sets from a powered card based upon, for example, manual input provided to a powered card. For example, a button associated with an on-line

purchase may be pressed on the powered card that causes a variable data set (e.g., account number and expiration date) to be communicated from the powered card to contactless communication device 162.

[0162] Discretionary data may, for example, be communicated by a powered card based upon which button was pressed on the powered card. In so doing, for example, a security code (e.g., "111") may be communicated within a discretionary data field when a button associated with a particular feature (e.g., pay with credit) is pressed on the powered card. As per another example, a different security code (e.g., "222") may be communicated within a discretionary data field when a button associated with a different feature (e.g., pay with debit) is pressed on the powered card. Accordingly, for example, processor 158 may identify what type of device may be in communication with contactless communication device 162 by analyzing the data communicated to contactless communication device 162.

[0163] Architecture 150 may include memory 160 and/or processor 158 may include internal memory. Accordingly, for example, application code may be stored within memory 160 and/or processor 158 and executed by processor 158 in support of functions performed by architecture 150. For example, an application (e.g., a graphical user interface) may be executed by architecture 150 and displayed onto display 154, which may be used to interact with a user of a mobile device (e.g., mobile device 100 of FIG. 1). Persons skilled in the art will appreciate that executable application code may be communicated to architecture 150 via any one or more interfaces of

architecture 150 (e.g., user interface 152, display 154, transceiver 156, and/or contactless communication device 162).

[0164] Application data (e.g., payment card data) may be stored within memory 160 and accessed by processor 158 during operation. For example, payment card data may be stored within memory 160 and recalled by processor 158 during a financial transaction being conducted by a mobile device (e.g., mobile device 100 of FIG. 1). Once recalled, processor 158 may communicate the payment card data via transceiver 156 and/or contactless communication device 162 to complete a financial transaction.

[0165] FIG. 2 shows network topology 200 that may include, for example, mobile device 202 (e.g., a mobile telephonic device, a PDA, an electronic tablet, a laptop, a GPS unit, or an MP3 player). Mobile device 202 may, for example, include a contactless interface that may initiate, sustain, and/or terminate communication channel 226 between contactless device 204 and mobile device 202. Contactless device 204 and mobile device 202 may communicate via channel 226 using any number of contactless mediums, which may include for example, visible, audible, capacitive, electromagnetic, magnetic, and/or RF mediums.

[0166] Mobile device 202 may provide one or more transceivers that may communicate with one or more wired networks (e.g., IP network 212 and/or payment network 214) and/or one or more wireless networks (e.g., mobile network 210). Mobile device 202 may, for example, communicate with a cellular station over a wireless radio interface (e.g., a GSM air interface) that may be used by mobile device 202 to communicate

information (e.g., voice and data) to cellular network access infrastructure 206 (e.g., one or more GSM base transceiver stations, base station controllers, and mobile switching centers). Persons skilled in the art will appreciate that cellular network access infrastructure 206 may utilize any multiple access architecture, such as for example, a code-division multiple access architecture and/or a time-division multiple access architecture.

[0167] Mobile device 202 may, for example, communicate with wireless access point 208 over a wireless interface (e.g., a Bluetooth interface or a Wi-Fi interface). Accordingly, for example, mobile device 202 may access one or more wired networks (e.g., IP network 212 and/or payment network 214) and/or one or more wireless networks (e.g., mobile network 210) without the need to first gain access to cellular network access infrastructure 206.

[0168] Contactless device 204 may, for example, be a powered card or a non-powered card (e.g., a powered payment card or a non-powered payment card). Accordingly, for example, payment information (e.g., a payment account number and a card expiration date) may be communicated from contactless device 204 to mobile device 202 in support of a financial transaction being conducted by mobile device 202. In so doing, for example, items for purchase on IP network 212 (e.g., the internet) may be accessed by a browser of mobile device 202 via an access point (e.g., wireless access point 208 or cellular network access infrastructure 206). Mobile device 202 may, for example, complete a purchase transaction by first obtaining required payment information from contactless device 204 and

then communicating such payment information to network entities (e.g., payment server 216 and/or issuer 220).

[0169] Payment server 216 may, for example, contact issuer 220 via a network (e.g., payment network 214) with payment information received from mobile device 202 for authorization of a purchase. Once authorized, payment transaction information may be recorded onto a receipt that may be delivered to mobile device 202 via any one or more delivery options (e.g., via a short messaging service of mobile network 210 or an email delivery service of IP network 212).

[0170] A payment receipt may, for example, be provided to mobile device 202 as a proof-of-purchase object (e.g., a barcode) that may be provided to a display of mobile device 202 and read by other computing equipment (e.g., a barcode scanner) for proof-of-purchase confirmation.

[0171] A mobile device (e.g., mobile device 224) may, for example, include a contactless communication device (e.g., an RFID) that may initiate, sustain, and/or terminate contactless communication channel 228 with merchant terminal 218. Accordingly, for example, mobile device 224 may communicate payment information to merchant terminal 218 to complete a financial transaction. In so doing, for example, mobile device 224 may first receive payment information via contactless communication channel 230 from contactless device 222 (e.g., a non-powered card), temporarily store the received payment information within a memory of mobile device 224, and forward the payment information onto merchant terminal 218 to complete a financial transaction. As per another example, mobile device 224 may provide previously stored financial

information associated with one or more payment cards (e.g., one or more non-powered payment cards). Accordingly, for example, payment information may be recalled from a memory of mobile device 224 and communicated to merchant terminal 218 via contactless communication channel 228 to complete a financial transaction using merchant terminal 218.

[0172] FIG. 3 shows system 300, which may include mobile device 302 and payment card 304. Mobile device 302 may, for example, be a laptop computer, a PDA, a mobile telephonic device (e.g., a smartphone), an MP3 player, a GPS, or any other mobile device. Display 308 may be a touch-sensitive display (e.g., sensitive to a change in capacitance). Payment card 304 may, for example, be a powered payment card or a non-powered payment card.

[0173] Mobile device 302 and payment card 304 may each include a contactless communication device (e.g., RFID) that may communicate via a contactless communication channel that may be formed between mobile device 302 and payment card 304 after coming into proximity to one another. Payment card 304 may, for example, be tapped onto display 308 of mobile device 302 to establish a proximity relationship that forms a communication channel between payment card 304 and mobile device 302. As per another example, payment card 304 may be brought within a proximity distance (e.g., up to two inches) of mobile device 302 to establish a contactless communication channel between mobile device 302 and payment card 304.

[0174] A processor of mobile device 302 may, for example, execute application code that may generate a graphical user interface (GUI) onto display 308 of

mobile device 302. Message 306 of a GUI may invite a user of mobile device 302 to begin a mobile payment by tapping a payment card against display 308. As per another example, by tapping payment card 304 against mobile device 302, mobile device 302 may autonomously determine that a mobile payment is desired and then generate a mobile payment GUI onto display 302.

[0175] Mobile device 302 may, for example, autonomously determine a type of card that may be tapped against it. For example, a processor of mobile device 302 may receive payment card data that may be indicative of a non-powered payment card (e.g., payment card data received from a non-powered card may not provide a security code associated with the card). As per another example, a processor of mobile device 302 may receive data that may be indicative of a powered card (e.g., payment card data received may contain a dynamically generated security code). Payment card data received from a powered card may, for example, include a dynamic security code that may change depending upon a type of transaction being conducted (e.g., debit or credit transaction).

[0176] As per another example, payment card 304 may be a powered payment card that may include electronics to simulate a human touch (e.g., payment card 304 may generate a change in capacitance that may be sensed by display 308). Through a series of simulated touches, payment card 304 may communicate a series of data bits to display 308, which may then be processed by a processor of mobile device 302. In so doing, for example, a contactless communication channel may be established where data is transferred from payment card

304 to mobile device 302 via a series of simulated touches.

[0177] Payment card 304 may, for example, include a light sensor. Accordingly, for example, payment card 304 may be sensitive to light pulses generated within a region of display 308. The light sensor of payment card 304 may receive a series of light pulses, which may be construed by a processor of payment card 304 as data generated by mobile device 302. In so doing, for example, payment card 304 may receive an optical data stream represented by a series of light pulses generated by display 308. As such, a two-way communication channel may be formed, where simulated touches may generate a data stream from payment card 304 to mobile device 302 and light pulses may generate a data stream from mobile device 302 to payment card 304.

[0178] FIG. 4 shows GUI 400, that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 400 may, for example, generate results of a card detection operation that may be performed by a processor of a mobile device. For example, card information may be exchanged between a card and a mobile device via a contactless communication channel that may identify a type of card that is being presented to the mobile device. Any type of card may be detected by a processor of a mobile device, such as for example, an airline card, a travel card, a bank card, a healthcare card, an identification card, and a loyalty rewards card. A card number communicated to a mobile device may, for example, be indicative of a card type (e.g., bank card 404) that is presented to a mobile device. Accordingly, for

example, a processor of a mobile device may identify a card type presented to the mobile device by analyzing a card number received from the card and may indicate the identified card type via GUI 400 (e.g., the identified card type may be generated onto GUI 400 having a different graphical presentation than the other card types listed).

[0179] A GUI may, for example, provide navigation aids. A GUI may, for example, provide navigation aids that may be touch sensitive. For example, GUI 400 may include navigation aids 406 and 408 to enable a user to revert to a previous GUI or advance to a subsequent GUI. Accordingly, for example, a user may touch an area on a display of a mobile device that displays a navigation aid to activate the touched navigation aid. In so doing, for example, a user may touch navigation aid 406 to revert to the previous GUI or a user may touch navigation aid 408 to advance to the next GUI.

[0180] FIG. 5 shows GUI 500, that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 500 may, for example, generate results of a payment card detection operation that may be performed by a processor of a mobile device. A non-powered payment card may, for example, communicate a single payment card number that may be associated with a number of payment options (e.g., debit, credit, or points). Accordingly, for example, GUI 500 may be generated to allow a user an opportunity to select which payment option (e.g., credit option 502) from a number of payment options is to be used to settle a payment transaction. Once identified, a payment option selection (e.g., credit option 502) may be communicated by a mobile device to

an issuer of the payment card to settle the transaction using the selected payment option.

[0181] As per another example, a powered payment card may include a user interface to allow a user to select from a number of payment options. A button on a powered payment card may, for example, be associated with one payment method (e.g., pay with credit) and another button may, for example, be associated with another payment method (e.g., pay with points). Data associated with the selected payment method may be communicated from a powered payment card to a mobile device. Accordingly, for example, a processor of a mobile device may detect the payment method communicated by a powered payment card (e.g., as communicated within a discretionary data field) and may autonomously generate a graphical representation of the payment method selected (e.g., GUI 500 may autonomously generate a graphical representation that credit method 502 was selected).

[0182] FIG. 6 shows GUI 600 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 600 may, for example, include a bank card validation screen as may be generated by a processor of a mobile device. A mobile device may, for example, challenge a user of the mobile device to enter a PIN that may be associated with a payment card (e.g., VISA credit 602) that was previously presented to the mobile device for payment. GUI 600 may, for example, generate virtual pin pad 606 that may include touch-sensitive buttons having alphanumeric indicia associated with each button. A user may touch one or more buttons of pin pad 606 that may correspond to respective characters of a PIN and an

indication of the user's selection may appear within area 604. Characters displayed within area 604 may, for example, be hidden for security purposes.

[0183] Activation of virtual button 608 may, for example, cause a processor of a mobile device to compare a PIN entered by a user of the mobile device to a PIN that may be associated with the payment card presented to the mobile device for payment. The PIN may, for example, be stored within protected memory of the mobile device, so that a processor of the mobile device may locally determine the validity of the PIN entered. Alternately, for example, the mobile device may communicate the PIN to the issuing bank for a remote validation of the PIN entered. Persons skilled in the art will appreciate that a user interface (e.g., a keypad or keyboard) of a mobile device may be used instead of virtual pin pad 606 to enter the one or more characters of a PIN.

[0184] FIG. 7 shows GUI 700 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 700 may, for example, include a bank card validation screen as may be generated by a processor of a mobile device. A mobile device may, for example, challenge a user of the mobile device to enter a security code that may be associated with a payment card (e.g., VISA credit 702) that was previously presented to the mobile device for payment. Such a security code (e.g., a CVV code) may, for example, be printed on the back of the payment card.

[0185] GUI 700 may, for example, generate virtual pin pad 706 that may include touch-sensitive buttons having alphanumeric indicia associated with each

button. A user may touch one or more buttons of pin pad 706 that may correspond to respective characters of a security code and an indication of the user's selection may appear within area 704. Characters displayed within area 704 may, for example, be hidden for security purposes.

[0186] Activation of virtual button 708 may, for example, cause a processor of a mobile device to compare a security code entered by a user of the mobile device to a security code that may be associated with the payment card presented to the mobile device for payment. The security code may, for example, be stored within protected memory of the mobile device, so that a processor of the mobile device may locally determine the validity of the security code entered. Alternately, for example, the mobile device may communicate the security code to the issuing bank for a remote validation of the security code entered. Persons skilled in the art will appreciate that a user interface (e.g., a keypad or keyboard) of a mobile device may be used instead of virtual pin pad 706 to enter the one or more characters of a security code.

[0187] FIG. 8 shows GUI 800 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 800 may, for example, include a bank card validation screen as may be generated by a processor of a mobile device. A mobile device may, for example, maintain memory of one or more payment cards previously presented to the mobile device for payment. A mobile device may, for example, allow a user to store payment information within the mobile device that may be associated with a payment card to be used at some point in the future.

[0188] Accordingly, for example, a user may recall payment information previously stored in memory of a mobile device in order to complete a purchase transaction using the mobile device. In order to validate that a user of a mobile device is actually the owner of payment information recalled from memory of the mobile device, GUI 800 may challenge the user to present the physical payment card whose associated payment information was recalled from memory. In so doing, for example, GUI 800 may prevent a fraudulent user of a mobile device from authorizing a purchase using payment information stored in memory of the mobile device that is not owned by the fraudulent user.

[0189] A user may, for example, be required to present a physical payment card to GUI 800 by placing (or tapping) the physical payment card within a proximity of a display of a mobile device that is generating GUI 800. In so doing, for example, a contactless communication channel (e.g., an RFID communication channel) may be established between the physical payment card and the mobile device, such that payment information may be communicated from the physical payment card to the mobile device. Upon verification that the communicated payment information matches payment information stored in memory of the mobile device, the payment information may be validated and authorized to be communicated from the mobile device to a network entity (e.g., a payment server or the issuer of the payment card) for settlement of the purchase transaction.

[0190] FIG. 9 shows GUI 900 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 900 may, for

example, include validation area 902 as generated by a processor of a mobile device. Validation area 902 may, for example, include one or more data exchange areas (e.g., data exchange areas 904 and 906). Icon 904 may, for example, be generated by GUI 900 within an area of a display of a mobile device that may be sensitive to touch (e.g., an area that may be sensitive to a capacitance change). Area 906 may, for example, be generated by GUI 900 within an area of a display of a mobile device that may generate pulses of light.

[0191] A powered payment card may be validated for use by a mobile device through an exchange data with the powered payment card via data exchange areas 904 and 906. For example, a powered payment card may be pressed against validation area 902 so that a touch simulation device of the powered payment card aligns with data exchange area 904 and a light sensing device aligns with data exchange area 906. Accordingly, for example, the powered payment card may communicate information to a processor of a mobile device by simulating a series of touches in data exchange area 904 and data may be communicated to the powered payment card by a processor of the mobile device by generating a series of light pulses in data exchange area 906. In so doing, for example, a mobile device and a powered payment card may exchange validation information so that payment card information stored within the mobile device may be validated for use.

[0192] A mobile device may, for example, include a motion capture device (e.g., a camera) and a powered payment card may, for example, include a light source (e.g., an LED). Accordingly, for example, information (e.g., validation information) may be exchanged between

a mobile device and a powered payment card such that information communicated by the powered payment card may be communicated as a series of light pulses while the camera of the mobile device captures the series of light pulses. A processor of the mobile device may construe the series of light pulses as information that may be used, for example, as validation information.

[0193] FIG. 10 shows GUI 1000 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 1000 may be generated, for example, after payment card information has been communicated by either of a non-powered payment card or a powered payment card to a mobile device. A user of a mobile device may, for example, elect whether to store such payment card information within a memory location of the mobile device. If a user chooses not to store payment information received from a payment card (e.g., as elected by selection of radio button 1004), a mobile device may delete all payment information previously received from a payment card after the payment information is used to complete a purchase transaction. Accordingly, a user wishing to use the same payment card to complete a payment transaction in the future is required to present the payment card to the mobile device so that the payment card may communicate payment card information to the mobile device in order to complete the payment transaction. If a user chooses to store payment information received from a payment card (e.g., as elected by selection of radio button 1002), a mobile device may store a portion of, or all, payment information previously received from a payment card in accordance with a user's preference.

[0194] FIG. 11 shows GUI 1100 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 1100 may, for example, offer storage options to a user of a mobile device that has elected to store a portion of, or all, payment card information previously communicated to the mobile device by a non-powered card or a powered card. A data storage option may, for example, be selected by a user of a mobile device (e.g., by touching a portion of text box 1102) that stores only a portion (e.g., an expiration date and payment card account number) of the payment card information into a memory of the mobile device. Accordingly, for example, a payment card may communicate one, two, and/or three tracks of magnetic stripe data to a mobile device, but the only payment information stored within a memory of the mobile device upon selection of text box 1102 is the expiration date and the payment card account number. All remaining information that may have been communicated by the payment card to the mobile device may be deleted by the mobile device.

[0195] Selection of text box 1104 may, for example, cause all payment information communicated by a payment card to a mobile device to be stored within a memory of the mobile device. Accordingly, for example, a mobile device may use a portion or all of the payment information stored within its memory to complete a purchase transaction. However, payment card validation information (e.g., a PIN or security code) may still be required to be entered by a user of the mobile device before the mobile device may complete a purchase transaction with the stored payment information.

[0196] Selection of box 1106 may, for example, cause all payment information communicated by a payment card to a mobile device to be stored within a memory of the mobile device. All validation information (e.g., a PIN or security code) that may be entered by a user of the mobile device to validate payment information received from a payment card may also be stored within a memory of the mobile device. Accordingly, for example, a mobile device may use a portion or all of the payment information, including validation information, stored within its memory to complete a purchase transaction.

[0197] Selection of box 1108 may, for example, cause all payment information, including discretionary data fields, communicated by a payment card to a mobile device to be stored within a memory of the mobile device. A powered payment card may, for example, allow a user of the powered payment card to select one or more options that may be associated with the powered payment card. A powered payment card may, for example, communicate indicia associated with the one or more selected options within discretionary data fields of magnetic stripe data that may be communicated to a mobile device.

[0198] For example, a user of a powered payment card may elect to pay for a purchase using rewards points by pressing a button on the powered payment card that is associated with a rewards points payment option. Accordingly, for example, a powered payment card may insert a rewards points payment code within a discretionary data field of a first, a second and/or a third track of magnetic stripe data and may communicate all track data, including the discretionary data field, to a mobile device. In so doing, for example, a

processor of a mobile device may detect such a payment code within a discretionary data field and may store payment information within a memory of the mobile device that is indicative of the rewards points payment code contained within the discretionary data field.

[0199] FIG. 12 shows GUI 1200 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 1200 may, for example, offer a split-payment option to a user of a mobile device, such that the user may elect to split payment for a selected purchase between two or more payment accounts. The mobile device may, for example, communicate payment information for each of the selected split-payment accounts to respective network entities (e.g., issuer and payment servers) of the selected split-payment accounts in order to settle the amounts owing on each of the selected split-payment accounts.

[0200] A user may, for example, select option 1202 (e.g., by tapping a payment card against a display of a mobile device or by presenting a payment card within proximity to the mobile device). In so doing, for example, a contactless communication channel (e.g., an RFID communication channel) may be established between the payment card and the mobile device so that payment information associated with the payment card may be communicated by the payment card to the mobile device and used as a split-payment account for a selected purchase.

[0201] An alternate contactless communication channel may be established, for example, by pressing a payment card against portion 1208. Accordingly, for example, a payment card may communicate payment

information associated with the payment card to a processor of a mobile device by simulating a series of touches at a location within portion 1208 (e.g., at icon 1210) and the processor of the mobile device may communicate information to the payment card by generating a series of light pulses at a location within portion 1208 (e.g., at location 1212). In so doing, for example, payment information associated with the payment card may be received by a processor of a mobile device and used as a split-payment account to partially cover the purchase price of a selected purchase.

[0202] Other contactless communication channels may be established. For example, a processor of a payment card may communicate payment information to a mobile device by generating a series of light pulses (e.g., via an LED of the payment card), which may be captured by a camera of the mobile device and construed by a processor of the mobile device as payment information. As per another example, a payment card may communicate payment information using audible sounds that may be received by a microphone of a mobile device and construed by a processor of the mobile device as payment information.

[0203] A payment account may, for example, be selected from a memory of the mobile device (e.g., by selecting radio button 1204). Associated payment information may, for example, be selectively retrieved from a memory of the mobile device and used by the mobile device as a split-payment account in partial payment for a selected purchase. Alternately, for example, a split-payment option may be declined by a

user of a mobile device (e.g., by selecting radio button 1206).

[0204] FIG. 13 shows GUI 1300 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 1300 may, for example, provide a summary of split-payment methods that may have been selected by a user of a mobile device. Portion 1302, for example, may display an amount owing for a particular selected purchase. Portions 1304-1308 may, for example, include an alphanumeric entry box to allow a user of a mobile device to input payment amounts (e.g., currency or points) that he or she wishes to apply towards a total amount owing as may be displayed in portion 1302. Portions 1304-1308 may, for example, include those payment accounts that a user of a mobile device previously selected as split-payment accounts.

[0205] Accordingly, for example, a user may elect to charge $10 against a VISA credit account, $35 against a M/C debit account, and 500 rewards points earned by the VISA credit account towards full payment of a $50 amount owing for a particular selected purchase. In so doing, for example, a mobile device may communicate with selected network entities (e.g., issuer and payment servers) to provide transaction information associated with each split-payment account selected, so that each amount owing may be settled.

[0206] Portions 1310-1314 may, for example, include alphanumeric entry boxes to allow a user of a mobile device to make comments on each account selected as a split-payment account. Accordingly, for example, a mobile device may communicate notes that may be entered by a user within portions 1310-1314 to, for example, a

payment server. In so doing, for example, receipts and/or account statements that may be generated by a network entity (e.g., an issuer or a payment server) may include such notes so that a user of a mobile device, upon receipt of such receipts and/or account statements, may be reminded of his or her thought process when such a split-payment was transacted.

[0207] FIG. 14 shows GUI 1400 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 1400 may, for example, offer checkout options to a user of a mobile device to allow a level of integration between the user and one or more issuers of associated payment accounts used by the mobile device in settlement of a selected purchase.

[0208] For example, a user may utilize billing tag list 1402 to categorize a selected purchase into one of many purchase categories. A user's physical presence may, for example, be at a fast-food establishment where the user may select a food purchase from the fast-food establishment's website using a browser of the user's mobile device. Payment information used to settle a transaction associated with the selected food purchase may be collected and/or generated by the mobile device and forwarded onto a payment server and/or an associated issuer for settlement. In addition, the mobile device may forward a billing tag selected from billing tag list 1402 to the associated issuer, so that the associated issuer may label the selected transaction on a billing statement using the selected billing tag. In so doing, for example, a user may customize an accounting of the issuer's billing statement by using a mobile device to communicate

payment information and billing tags associated with selected purchases to track expenditures within the various purchase categories of billing tag list 1402.

[0209] A user of a mobile device may select receipt delivery options for each purchase that may be transacted using a mobile device. For example, a receipt delivery list may be generated by a processor of a mobile device so that a user of the mobile device may select a receipt delivery option. Accordingly, for example, the selected receipt delivery option along with payment information may be communicated by a mobile device to a payment server and the payment server (or other entity) may direct a delivery of the receipt based upon the receipt delivery option received.

[0210] A user may, for example, request delivery of a purchase receipt via text messaging (e.g., by selecting receipt delivery option 1406). In so doing, for example, a mobile device may complete a purchase transaction with an entity of a payment network (e.g., a payment server) and may further request that the payment server deliver a receipt to the mobile device in a text message format. Accordingly, for example, in addition to providing payment information to the payment server, a mobile device may also provide a text message address (e.g., an SMS text message address) to the payment server. In so doing, for example, the mobile device may receive a receipt of the completed purchase transaction from the payment server via a text message at the text message address provided by the mobile device.

[0211] As per another example, a multimedia message (e.g., an MMS message containing rich content) may be

received by a mobile device from a payment server in the form of, for example, a graphical image (e.g., barcode), such that the barcode may be used as a proof-of-purchase (e.g., proof-of-purchase of an airline ticket and an associated barcode that gains access by the user of the mobile device to a particular seating assignment on the airplane.)

[0212] A receipt (e.g., a receipt received via multimedia messaging) may, for example, provide rewards to a user of the mobile device for completing payment transactions via a mobile device. For example, a mobile device may communicate indicia to a payment server that identifies a payment transaction as a mobile payment transaction. The communicated mobile payment indicia may, for example, trigger a payment server to not only provide a receipt for the purchase transaction to the mobile device, but also to provide a multimedia game that may be executed by the mobile device. As per an example, an animated trivia question may be communicated to a mobile device via an MMS message upon completion of a mobile payment transaction. Upon successfully answering the animated trivia question, a user of the mobile device may receive another MMS message that contains a coupon for free merchandise from the merchant whose goods were just purchased. As per another example, a receipt received from a payment server may itself contain coupons for discounted or free merchandise without requiring that a user of the mobile device perform any further actions beyond completing a mobile payment purchase with a mobile device.

[0213] A user may, for example, request delivery of a purchase receipt via email (e.g., by selecting

receipt delivery option 1408). In so doing, for example, an email address associated with the user may be provided by the mobile device to a payment server in addition to any required payment information that may be required to complete a purchase transaction. Accordingly, for example, a payment server may address a receipt to an email address received from a mobile device during a mobile payment transaction.

[0214] A user may, for example, request delivery of a purchase receipt (e.g., by selecting receipt delivery option 1410) via a format that may be compatible with an accounting software package (e.g., QuickBooks). For example, a mobile device may allow a user to categorize a particular purchase within a particular expense account (e.g., an office supply expense account) during a purchase transaction. Once the purchase transaction is completed, an electronic receipt may be communicated to the mobile device that may be tagged with the categorized expense account (e.g., the accounting software package may have its own address that receipts may be delivered to). In so doing, for example, an accounting software package that may be executing on the mobile device may autonomously access the electronic receipt from its own address and may autonomously enter the expense in the correct category so that all purchases made by the mobile device may be correctly accounted for within the accounting software package.

[0215] A user may, for example, request delivery of a purchase receipt (e.g., by selecting receipt delivery option 1412) via a format that may be compatible with the bank that issued the selected payment account. Accordingly, for example, a payment server may forward

a receipt of the purchase transaction to the issuing bank and the issuing bank may format the receipt for delivery with the user's month-end account statement.

[0216] A user may, for example, enter comments about a purchase transaction that may be included within a receipt. For example, a user may enter comments 1404 that may remind the user to include the receipt within his or her tax records because the purchase may be deemed as tax deductible. Accordingly, for example, comments 1404 may accompany payment information communicated by a mobile device to a payment server. In so doing, for example, a payment server may add comments 1404 to a receipt generated by the payment server and may forward the receipt with the added comments to the user of the mobile device as dictated by the receipt delivery options requested by the user of the mobile device.

[0217] FIG. 15 shows GUI 1500 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 1500 may, for example, offer a check-out option to a user of a mobile device, such that the user may elect to apply a rewards card to a selected purchase in order for the rewards card to accrue points for the purchase. The mobile device may, for example, submit rewards card information and transaction information to respective issuers of the rewards account so that the respective issuers may credit the rewards account accordingly.

[0218] A user may, for example, select option 1502 (e.g., by tapping a rewards card against a display of a mobile device or by presenting a rewards card within proximity to the mobile device). In so doing, for example, a contactless communication channel (e.g., an

RFID communication channel) may be established between the rewards card and the mobile device so that information associated with the rewards card may be communicated by the rewards card to the mobile device.

[0219] An alternate contactless communication channel may be established, for example, by pressing a rewards card against portion 1508. Accordingly, for example, a rewards card may communicate information associated with the rewards card to a processor of a mobile device by simulating a series of touches within portion 1508 (e.g., at icon 1510) and the processor of the mobile device may communicate information to the rewards card by generating a series of light pulses within portion 1508 (e.g., at location 1512). In so doing, for example, rewards information associated with the rewards card may be received by a mobile device and communicated to an issuer of the rewards card so that the rewards account may be updated with the purchase transaction information.

[0220] Other contactless communication channels may be established. For example, a processor of a rewards card may communicate rewards information to a mobile device by generating a series of light pulses (e.g., via an LED of the rewards card), which may be captured by a camera of the mobile device and construed by a processor of the mobile device as rewards information. As per another example, a payment card may communicate payment information using audible sounds that may be received by a microphone of a mobile device and construed by a processor of the mobile device as payment information.

[0221] A rewards account may, for example, be selected from a memory of the mobile device (e.g., by

selecting radio button 1504). Associated rewards information may, for example, be selectively retrieved from a memory of the mobile device and communicated by the mobile device to an issuer of the rewards account so that the rewards account may be credited with the selected purchase.

[0222] A user of a mobile device may, for example, place an order for a rewards card by selecting radio button 1506. Accordingly, for example, a mobile device may communicate payment information to a payment server to complete a purchase transaction and may also communicate a request that a rewards account be created. A payment server may, for example, forward the rewards account creation request to an issuer of a rewards account along with details of the purchase transaction, so that the issuer may first create the rewards account and may then credit the account according to the purchase transaction. Accordingly, for example, an electronic version of a newly created rewards card (e.g., a graphical representation of a newly created rewards card) may, for example, be communicated to a mobile device which may, for example, include a barcode representation of the rewards account information. In addition, rewards card information may, for example, be added to a memory of a mobile device for future access.

[0223] FIG. 16 shows GUI 1600 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 1600 may, for example, challenge a user of a mobile device to enter an access code that may be required to authenticate a purchase transaction. GUI 1600 may, for example, include virtual keyboard 1604 to allow a user of a

mobile device to enter such an access code. Alternately, for example, a manual input interface of a mobile device (e.g., a keyboard or a keypad) may be used to enter such an access code.

[0224] As a user of a mobile device enters each character of an access code, portion 1602 may reflect such entry. Such entries may, for example, be reflected within portion 1602 as protected characters (e.g., the actual value of each character may be blocked out) to protect the security and safety of the entered access code. Once an entered access code is verified and authenticated by a mobile device, the mobile device may complete the requested purchase transaction.

[0225] FIG. 17 shows GUI 1700 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 1700 may, for example, include portion 1702 that may display a graphical representation of a proof-of-purchase (e.g., a barcode). Such a proof-of-purchase may be communicated to a mobile device via a network entity (e.g., a payment server) upon completion of a purchase transaction by the mobile device.

[0226] Accordingly, for example, portion 1702 may graphically display a proof-of-purchase that may be recognized by a reader (e.g., a barcode reader). In so doing, for example, a system that may include a barcode reader may verify the validity of a proof-of-purchase barcode, which may then allow a user of a mobile device displaying such a barcode to enjoy the goods and/or services purchased by the user via the mobile device as acknowledged by the verified barcode. As per one example, such a verified barcode may allow entry onto

an airplane having a seat assignment that is encoded within the barcode. As per another example, a user may have made an on-line purchase of an appliance using his or her mobile device and may have requested pick-up of the purchased appliance at an appliance inventory warehouse. Upon arrival at the appliance inventory warehouse, a user may retrieve an electronic proof-of-purchase (e.g., a barcode) from a memory of the mobile device that was received by the user's mobile device upon completion of the appliance purchase transaction. A reader (e.g., a barcode reader) at the appliance inventory warehouse may read the user's barcode directly from a display of the user's mobile device, verify that a purchase was completed by the user's mobile device, and may authorize the appliance for pickup by the user.

[0227] FIG. 18 shows GUI 1800 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 1800 may, for example, enable a funds transfer to one or more financial accounts. GUI 1800 may, for example, enable a transfer of funds (e.g., by selecting radio button 1802) directly from one or more financial accounts into one or more financial accounts. GUI 1800 may, for example, generate a communication channel with a recipient of a funds transfer (e.g., by selecting radio button 1804) and may allow the recipient to interactively determine the financial account that is to receive the transferred funds.

[0228] FIG. 19 shows GUI 1900 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 1900 may, for example, enable a funds transfer to one or more

accounts. GUI 1900 may, for example, allow a user of a mobile device to select an object (e.g., by selecting an entry within menu list 1902) that may be associated with the funds transfer. GUI 1900 may, for example, allow a user to select an account (e.g., by selecting an entry within menu list 1904) that may be associated with the object selected within menu list 1902.

[0229] Accordingly, for example, a mobile device may include a memory within which a user may enter one or more potential recipients of a funds transfer. A processor of a mobile device may, for example, list each potential recipient of a funds transfer within menu list 1902. A user of a mobile device may, for example, select a recipient of a funds transfer by activating (e.g., touching) an entry within menu list 1902 that corresponds to the selected recipient. As per an example, a user's funds transfer recipient list, as may be reflected by menu list 1902, may include persons, financial accounts, inanimate objects, or any other type of object.

[0230] Once a selected funds transfer recipient is selected within menu list 1902, menu list 1904 may be populated. Accordingly, for example, a mobile device may include a memory within which a user may enter one or more accounts that may be associated with one or more potential recipients of a funds transfer. A processor of a mobile device may, for example, list each account in menu list 1904 that may be associated with the selected recipient of menu list 1902. A user of a mobile device may, for example, select an account for a funds transfer by activating (e.g., touching) an entry within menu list 1904 that corresponds to the selected account. As per an example, a user's funds

transfer account list, as may be reflected by menu list 1904, may include any account that may be associated with the selected recipient of menu list 1902.

[0231] FIG. 20 shows GUI 2000 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 2000 may, for example, enable a funds transfer from a source account (e.g., an account associated with a payment card that is tapped against a display of a mobile device) to a target account (e.g., a car loan account). Portion 2002 may, for example, list account details that may be associated with a target account (e.g., an account number associated with a car loan, the payoff amount, and the amount due). Portion 2002 may, for example, include details that may be associated with a target account that a mobile device has collected from a network entity (e.g., a bank) via a network connection between the mobile device and the network entity.

[0232] Portion 2004 (e.g., an alphanumeric entry box) may, for example, allow a user of a mobile device to enter an amount to be transferred (e.g., an amount that is equal to the minimum amount due on an installment payment agreement). GUI 2000 may, for example, request an identification of a source account from which the amount will be transferred. As per an example, a user of a mobile device may tap a payment card against a display of the mobile device to establish a contactless communication channel between the payment card and the mobile device within which payment information may be communicated from the payment card to the mobile device. As per another example, a payment card may communicate payment information to a mobile device via a series of touch

simulations (e.g., changes in capacitance generated by a payment card that may be detected by a touch-sensitive display of a mobile device). A series of light pulses, or audible information, for example, may be communicated by the payment card to the mobile device in order to communicate payment information.

[0233] GUI 2000 may, for example, display a summary of payment information that may have been received by a mobile device from a payment card via a contactless communication channel. For example, portion 2006 may be displayed by GUI 2000 to allow a user of a mobile device to confirm the identity of a payment account from which an amount of money will be transferred. Once confirmed, the mobile device may communicate with network entities (e.g., an issuer of the source account and a bank associated with the target account) to complete the money transfer.

[0234] FIG. 21 shows GUI 2100 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 2100 may, for example, enable a funds transfer to an account associated with a person. A recipient may, for example, interactively select an account into which the funds will be transferred. Accordingly, for example, contact list 2102 may be displayed by GUI 2100 as a list of potential recipients of a money transfer. Contact method list 2104 may, for example, by displayed by GUI 2100 as a list of methods that may be used to contact the recipient as selected within contact list 2102. In so doing, for example, a person within contact list 2102 (e.g., Trace) may be selected by a user of a mobile device to be the recipient of a funds transfer and the recipient may be contacted, for

example, in accordance with a method selected in contact method list 2104 (e.g., transfer alert).

[0235] FIG. 22 shows system 2200, which may include mobile device 2202, receiving device 2204, and network 2210. Mobile device 2202 may be a device used to coordinate a money transfer and receiving device 2204 may be a device used to coordinate receipt of a money transfer. Receiving device may, for example, be a mobile device. Receiving device, for example, may not be a mobile device (e.g., a desktop computer). Devices 2202-2204 may communicate via network 2210, which may include any combination of cellular network resources, wireless network resources, and/or wired network resources.

[0236] Mobile device 2202 may, for example, include a processor that may render money transfer GUI 2206 onto a display of mobile device 2202. GUI 2206 may, for example, pause while a user of mobile device 2202 selects a payment account from which a money transfer may be withdrawn. Accordingly, for example, mobile device 2202 may wait until a payment card is brought within a proximity to, or a touch relationship with, mobile device 2202 (e.g., a payment card may be tapped onto a display of mobile device 2202). Alternately, for example, a payment card may communicate with mobile device 2202 using any number of contactless methods (e.g., using light, sound, capacitive, magnetic or electromagnetic communication). In so doing, for example, mobile device 2202 may establish a contactless communication channel with a payment card in which payment information is communicated from the payment card to mobile device 2202 and is summarized onto GUI 2206 for review by a user of mobile device 2202. A

user of mobile device 2202 may enter an amount of money for transfer, may verify a money amount for transfer, and may enter a message to be communicated to receiving device 2204.

[0237] Mobile device 2202 may communicate payment information received from a payment card along with information received from a user of mobile device 2202 to a network entity (e.g., an issuer) where, for example, authorization of the transfer amount from the account selected is performed. Once authorized, mobile device 2202 may communicate a transfer alert along with a transfer alert message to receiving device 2204. Receiving device 2204 may, for example, present a transfer alert along with the associated transfer alert message onto GUI 2208. A user of receiving device 2204 may respond to the transfer alert message received from mobile device 2202 by sending an acknowledgment message to mobile device 2202 via network 2210.

[0238] A user of receiving device 2204 may, for example, be asked to enter account information that is to be used as the receiving account for the money transfer. Accordingly, for example, a user of receiving device 2204 may provide such account information any number of ways. For example, a payment card associated with a receiving account may be brought within a proximity, or a touching, relationship to receiving device 2204. In so doing, for example, a contactless communication channel (e.g., an RFID channel) may be formed to communicate such information. Alternately, a payment card may communicate with receiving device 2204 using any number of contactless methods (e.g., using light, sound, capacitive, magnetic or electromagnetic communication). A user of receiving

device 2204 may verify the receive account information as it may be displayed onto GUI 2208.

[0239] Receiving device 2204 may, for example, communicate information associated with a receiving account to mobile device 2202 via network 2210. Accordingly, for example, mobile device 2202 may coordinate the money transfer via network 2210 with network entities (e.g., an issuer of the account used to provide money to transfer and an issuer of the account used to receive money for transfer). Once the money transfer is completed, an acknowledgment message may be displayed onto GUI 2206 by a processor of mobile device 2202 and an acknowledgment message may be communicated by mobile device 2202 to receiving device 2204 and then displayed onto GUI 2208 by a processor of receiving device 2204.

[0240] FIG. 23 shows system 2300, which may include a mobile device 2302, a powered or non-powered payment card 2304, a remote application 2308 and network 2306. Mobile device 2302 may, for example, access remote application 2308 via network 2306 in order to complete a purchase transaction. Accordingly, for example, payment card 2304 may communicate payment information to mobile device 2302 via contactless communication channel 2312 and mobile device 2302 may communicate the payment information to remote application 2308 via communication channel 2310 to complete the purchase transaction.

[0241] Contactless communication channel 2312 may be any type of contactless communication channel, such as for example, an RF, capacitive, audible, visible, electromagnetic, or magnetic communication channel. Contactless communication channel 2312 may be a two-way

communication channel, where mobile device 2302 may communicate with payment card 2304 in order to, for example, enhance data communication between mobile device 2302 and payment card 2304.

[0242] As per one example, payment card 2304 may communicate payment information (e.g., one, two, and/or three tracks of magnetic stripe data) to mobile device 2302 after payment card 2304 is tapped against mobile device 2302. Remote application 2308 may, for example, be an on-line payment application that does not require a fully populated magnetic stripe message to complete a purchase transaction, but may only require a subset of a fully populated magnetic stripe message (e.g., account number and expiration date). Accordingly, for example, mobile device 2302 may filter payment information received from payment card 2304 to only include the subset of information that may be required by remote application 2308 and may communicate only the filtered payment information to remote application 2308 to complete the purchase transaction.

[0243] In general, for example, mobile device 2302 may filter payment information received from payment card 2304 into a filtered subset of payment data that may be required by remote application 2308 to complete a purchase transaction. In so doing, for example, mobile device 2302 may customize a payment message to remote application 2308 that includes only the filtered subset of data that is needed by remote application 2308 to complete the purchase transaction.

[0244] As per another example, mobile device 2302 may query payment card 2304 via contactless communication channel 2312 for only a subset of payment information that may be required by remote application

2308 to complete a purchase transaction. Accordingly, for example, a processor of payment card 2304 may receive the request and may only supply the requested payment information via contactless communication channel 2312 instead of communicating a complete magnetic stripe message.

[0245] FIG. 24 shows system 2400, which may include a mobile device 2402, a payment card 2404, a rewards card 2416, and items to be purchased 2410-2414. Mobile device 2402 may, for example, include a scanning device (e.g., a camera) that may be used to capture images (e.g., barcode images). Accordingly, for example, a user of mobile device 2402 may activate an application within mobile device 2402 that generates GUI 2408 and that activates a camera to capture barcode images. A processor of mobile device 2402 may, for example, analyze captured barcode images to extract information from the barcode images and construe the extracted information as data input. Accordingly, for example, a camera of mobile device 2402 may be used to scan barcodes of items that the user wishes to purchase and a processor of mobile device 2402 may analyze the scanned information to keep a running total of items selected for purchase. In so doing, for example, a user of mobile device 2402 may wander through a shopping market while scanning barcode labels of items for purchase (e.g., items 2410-2414).

[0246] Mobile device 2402 may access a network (e.g., a local Wi-Fi hotspot) within a shopping market to determine those items that may be offered at a discount to rewards members of the shopping market. Accordingly, for example, a user may scan barcode image 2418 of rewards card 2416 to obtain an instant credit

for discounted items for purchase. As per another example, rewards card 2416 may establish a contactless communication channel with mobile device 2402 so that rewards card 2416 may communicate rewards account information to mobile device 2402 via any one of a number of contactless communication mediums (e.g., RF, capacitive, audible, visible, electromagnetic, or magnetic communication mediums).

[0247] Once a user of mobile device 2402 finishes shopping, the user may present payment card 2404 to mobile device 2402 for payment. Accordingly, for example, contactless communication channel 2406 (e.g., an RF, capacitive, audible, visible, electromagnetic, or magnetic communication channel) may be created and payment information may be communicated from payment card 2404 to mobile device 2402 so that mobile device 2402 may complete the purchase transaction with a network entity (e.g., an issuer of payment card 2404).

[0248] FIG. 25 shows system 2500, which may include mobile device 2502 and payment card 2504. Mobile device 2502 may interact with a merchant establishment (e.g., a restaurant) to gain entry into a user's tab at the merchant's establishment (e.g., a food and alcohol bill generated by the restaurant). Accordingly, for example, a user may monitor each item on the bill, enter an additional amount into the bill (e.g., a tip), and then pay the bill all from the convenience of the user's mobile device 2502.

[0249] Interaction with a merchant establishment may be accomplished any number of ways. For example, mobile device 2502 may access a local Wi-Fi hotspot and may communicate information (e.g., an email address or text messaging address) to the merchant that identifies

a user of mobile device 2502. Accordingly, for example, a merchant may send a message (e.g., an email or text message) to the user-supplied address that may contain a link to the user's bill. A user may, for example, click on the link, enter a pass code to gain entry to the user's bill, and then monitor the bill being generated onto a display of mobile device 2502 via GUI 2508.

[0250] As per another example, mobile device 2502 may place a phone call to a merchant's phone number to establish a communication channel (e.g., a data call) between the merchant server and mobile device 2502. The merchant server may, for example, render GUI 2508 onto a display of mobile device 2502 so that a user of mobile device 2502 may directly interact with the merchant server.

[0251] GUI 2508 may be rendered onto a display of mobile device 2502 to allow a user to remotely interact with his or her bill. For example, a user's meal tab at a restaurant may be itemized by GUI 2508 and an alphanumeric entry box (e.g., box 2510) may allow the user to enter additional data (e.g., add a tip to the bill). A user may, for example, review a total to be charged, verify such a total, and then present payment card 2504 to mobile device 2502 to settle the total amount. In so doing, for example, contactless communication channel 2506 may receive payment information from payment card 2504 via any number of contactless communication mediums (e.g., RF, capacitive, audible, visible, electromagnetic, or magnetic communication mediums) and may communicate such payment information to a network entity (e.g., an

issuer of payment card 2504) to complete a purchase transaction for the total amount of the user's bill.

[0252] FIG. 26 shows flow charts for process sequences 2610-2650. Process sequence 2610 may, for example, execute a payment application on a mobile device (e.g., as in step 2611) to request a user of the mobile device to present a payment card to the mobile device. In step 2612, a user may present a payment card (e.g., tap a payment card onto a display of a mobile device) to begin a payment transaction. In step 2613, a contactless communication channel (e.g., an RF, capacitive, audible, visible, electromagnetic, or magnetic communication channel) may be generated between a payment card and a mobile device to communicate payment information from the payment card to the mobile device. In step 2614, a purchase may be completed by a mobile device by communicating received payment information to network entities to settle a payment transaction.

[0253] Process sequence 2620 may, for example, autonomously detect that a payment card is in a touching or a proximity relationship to a mobile device (e.g., as in step 2621). In step 2622, a contactless communication channel (e.g., an RF, capacitive, audible, visible, electromagnetic, or magnetic communication channel) may be generated between a payment card and a mobile device to communicate payment information from the payment card to the mobile device. In step 2623, a purchase may be completed by a mobile device by communicating received payment information to network entities to settle a payment transaction.

[0254] Step 2631 of sequence 2630 may include presenting a card to a mobile device. A card may, for

example, be a powered card or a non-powered card. In steps 2632 and 2633, a contactless communication channel may be established between a card and a mobile device and information may be exchanged between the card and the mobile device.

[0255] A card may, for example, include a near-field communication device (e.g., an RFID) that may communicate with a contactless communication device of a mobile device to form a two-way communication channel between the card and the mobile device. A card may, for example, include circuitry to simulate touch (e.g., a capacitance change) in order to form a contactless communication channel with a mobile device. Accordingly, for example, a card may be pressed against a touch-sensitive display of a mobile device and information may be communicated by the card to the mobile device through a series of card-simulated touches that may be detected by the touch-sensitive display of the mobile device.

[0256] A card may, for example, include a light sensor to form a contactless communication channel with a mobile device. Accordingly, for example, a card may be pressed against a display of a mobile device and information may be communicated from the mobile device to the card through a series of light pulses generated by the display of the mobile device. A frequency, pulse width, and/or a pulse intensity of light pulses may, for example, be detected by a processor of a card as data communicated by a mobile device.

[0257] A card may, for example, include a light source (e.g., an LED) to form a contactless communication channel. Accordingly, for example, a card may emit varying light pulses from an LED that may

be detected by a motion-capture device (e.g., a camera) of a mobile device as data communicated by the card. A card may, for example, include sound emission capabilities that may be detected by a microphone of a mobile device as data communicated by the card through a contactless communication channel. A mobile device may, for example, include sound emission capabilities that may be detected by a microphone of a card as data communicated by the mobile device through a contactless communication channel.

[0258] Step 2641 of sequence 2640 may include selecting items for purchase using a mobile device. A mobile device may, for example, include a scanning device (e.g., a camera) that may be used by a mobile device to capture images of barcodes that may be associated with items for purchase (e.g., grocery items in a grocery store). Accordingly, for example, a mobile device may collect images of barcodes and a processor of the mobile device may analyze the images to retrieve information (e.g., item description and cost) of each item scanned. Each item's description, cost and other information may, for example, be displayed on a GUI that may be generated by a processor and presented to a display of the mobile device as in step 2642. A payment card may, for example, be presented to the mobile device (e.g., as in step 2643) and payment information may be exchanged between the payment card and the mobile device (e.g., as in step 2644) via a contactless communication channel (e.g., an RF, capacitive, audible, visible, electromagnetic, or magnetic communication channel). In step 2645, a mobile device may communicate received payment

information to network entities (e.g., a payment server and/or an issuer) to complete the transaction.

[0259] In step 2651 of sequence 2650, for example, a mobile device may remotely access an electronic bill. For example, a merchant (e.g., a restaurant) may provide access to a bill (e.g., a restaurant tab for food and beverages) to a patron of the merchant via that patron's mobile device. As per one example, a merchant may provide a link to a bill via a message (e.g., an email message or a text message) that may be sent by the merchant to the patron's mobile device or that may be sent by the patron's mobile device to the merchant. The patron may click on the link and may be taken to a website that may provide access to the patron's tab via a browser that may be executing on the patron's mobile device. As per another example, a data call between a patron's mobile device and a merchant may execute an application (e.g., locally on the patron's mobile device and/or remotely on a merchant's server) to allow a patron to review his or her bill.

[0260] Each item on the patron's bill may, for example, include a description, cost and other information and may be displayed on a GUI that may be generated by a processor and presented to a display of the mobile device as in step 2652. A payment card may, for example, be presented to the mobile device (e.g., as in step 2653) and payment information may be exchanged between the payment card and the mobile device (e.g., as in step 2654) via a contactless communication channel (e.g., an RF, capacitive, audible, visible, electromagnetic, or magnetic communication channel). In step 2655, a mobile device may communicate received payment information to network

entities (e.g., a payment server and/or an issuer) to complete the transaction.

[0261] FIG. 27 shows mobile device 2700. Mobile device 2700 may be any mobile device, such as a mobile telephonic device (e.g., cell phone), a PDA, an electronic tablet, an MP3 player, or a locating device (e.g., a GPS device). Accordingly, for example, mobile device 2700 may be operated in a mobile environment while a user of mobile device 2700 goes about his or her daily activities (e.g., driving, shopping, walking, dining, and exercising). In addition, for example, mobile device 2700 may perform multiple functions simultaneously (e.g., a person may carry on a conversation while at the same time browsing and purchasing products on the internet).

[0262] Mobile device 2700 may include audio processing devices (e.g., microphone 2708 and speaker 2710). Accordingly, for example, mobile device 2700 may receive voice commands from a user via microphone 2708 and may process such commands to perform a function. For example, a user may place mobile device 2700 into a desired operational mode by speaking a command into microphone 2708 that is associated with the desired operational mode. In so doing, for example, mobile device 2700 may engage in hands-free operation by receiving voice commands via microphone 108 and performing functions associated with the received voice commands.

[0263] Mobile device 2700 may receive data input via microphone 2708. For example, a voice-band modem may generate signals in a voice-band frequency range that may be received by microphone 2708. A processor of mobile device 2700 may interpret the received audible

information as data signals and may process the data signals as, for example, data values and/or control data input.

[0264] Mobile device 2700 may include camera 2702. Camera 2702 may capture one or more frames of video data and store the video data within a memory of mobile device 2700. Accordingly, for example, a processor of mobile device 2700 may receive one or more frames of video information via camera 2702 and may process the video information as data values and/or control data input. In so doing, for example, mobile device 2700 may receive optical information that is sensed by camera 2702 during a series of one or more video capture events that produce one or more frames of video information. The one or more frames of video information may contain one or more data elements (e.g., pixels) having properties (e.g., color, intensity, or contrast) that may be interpreted by a processor of mobile device 2700 as data values and/or control data.

[0265] Mobile device 2700 may include manual input interface 2712. Manual input interface 2712 may, for example, include keys and/or buttons that may be sensitive to manual input, such as a touch or an application of pressure. Accordingly, for example, a user of mobile device 2700 may enter information into mobile device 2700 via manual interface 2712 to cause a processor of mobile device 2700 to enter a particular mode of operation. Manual interface 2712 may, for example, be used for data entry (e.g., dialing a phone number or entering data as may be requested by mobile device 2700) during a particular mode of operation of mobile device 2700.

[0266] Mobile device 2700 may include display 2704. Display 2704 may provide visible information that may be utilized by a user during interaction with mobile device 2700. A portion or all of display 2704 may be touch sensitive such that objects making contact with display 2704 or objects coming within a proximity of display 2704 may be detected by a processor of mobile device 2700. Accordingly, for example, mobile wallet graphical user interface 2706 may be provided by display 2704 so that graphical information may be displayed to solicit and/or receive data entry from a user. In so doing, for example, touch-sensitive graphical user interface devices such as radio buttons, textual input boxes, virtual buttons, pull-down menus, and navigational tools may be used for data entry to initiate, change, and/or support functions performed by mobile device 2700.

[0267] Display 2704 may, for example, display graphical objects that may interact with a user of mobile device 2700. Accordingly, for example, a virtual card (e.g., a virtual payment card) may be rendered onto display 2704 having interactive components associated with such a virtual payment card. In so doing, for example, a virtual payment card displayed by display 2704 may itself include a virtual user interface (e.g., one or more virtual buttons) that may be sensitive to touch or proximity. Such virtual buttons may be associated with a feature (e.g., one or more tracks of magnetic stripe information may be communicated by the mobile device when a button is activated). In so doing, for example, a feature activated on a virtual payment card displayed by display 2704 may cause mobile device 2700 to behave

like a payment card (e.g., one or more tracks of magnetic stripe information may be communicated by mobile device 2700 when a virtual button of a virtual payment card of display 2704 is activated).

[0268] FIG. 27 shows architecture 2750. User interface 2752 may, for example, be included within architecture 2750 to allow user interaction with architecture 2750. For example, a dedicated key pad or keyboard may be included within user interface 2752 to allow alphanumeric data entry into architecture 2750.

[0269] Architecture 2750 may include one or more displays 2754. Display 2754 may, for example, be touch-sensitive. Accordingly, for example, display 2754 may be utilized for alphanumeric data entry using virtual buttons that may be rendered onto touch-sensitive portions of display 2754. In so doing, for example, touching virtual buttons that may be associated with alphabetic and numeric characters of display 2754 may be detected by processor 2758 as alphanumeric data entry.

[0270] Alphanumeric entry boxes may, for example, be rendered onto display 2754. A user may, for example, activate a cursor within such an alphanumeric entry box by touching an area within the alphanumeric entry box. A user may utilize user interface 2752 and/or a virtual keypad rendered onto display 2754 to select alphanumeric characters to be placed within the alphanumeric entry box having a character position identified, for example, by an activated cursor within the alphanumeric entry box. In so doing, for example, processor 2758 may receive alphanumeric characters as typed into a alphanumeric entry box of display 2754 and may use such alphanumeric characters as data input.

[0271] Display 2754 may, for example, render a virtual representation of a card (e.g., one or more virtual payment cards stored within memory 2760). Accordingly, for example, information (e.g., payment card number, cardholder name, bank logos and issuer identification) may be stored within memory 2760 and rendered onto display 2754 as a virtual representation of a card. In so doing, for example, virtual interactive objects (e.g., buttons, displays, light sources and light sensors) that may be associated with a virtual card on display 2754 may be utilized through interaction with display 2754 just as if the virtual card were physically present.

[0272] Display 2754 may, for example, provide data output from architecture 2750. For example, display 2754 may communicate data using a series of light pulses. Accordingly, for example, processor 2758 may cause one or more portions of display 2754 to produce light pulses having varying characteristics (e.g., duration, intensity, and frequency) that may communicate information via such light pulses. In so doing, for example, a device that may be sensitive to light pulses may receive information communicated by display 2754 via light pulses having varying characteristics. Display 2754 may, for example, communicate data using visual information that may be substantially static (e.g., a barcode).

[0273] Architecture 2750 may include one or more transceivers 2756. Transceiver 2756 may communicate information to and/or may receive information from one or more devices. Transceiver 2756 may, for example, communicate via a wireless interface with one or more cellular stations of a mobile network. Accordingly,

for example, transceiver 2756 may allow a mobile device (e.g., mobile device 2700 of FIG. 27) to establish a communications channel with an associated cellular station. In so doing, for example, a mobile device (e.g., mobile device 2700 of FIG. 27) may exchange information (e.g., voice, text, data, or multimedia) with one or more terrestrial networks (e.g., the internet or a payment network) via an associated cellular station. As per another example, transceiver 2756 may exchange information with one or more other mobile devices via one or more associated cellular stations.

[0274] Transceiver 2756 may, for example, communicate via a wireless interface with one or more mobile devices directly. Accordingly, for example, transceiver 2756 may communicate with another mobile device without first accessing a mobile network via a cellular station of the mobile network. As per another example, transceiver 2756 may, for example, communicate via a wireless interface with one or more network devices (e.g., a wireless access point) directly. Accordingly, for example, a mobile device (e.g., mobile device 2700 of FIG. 27) may directly connect to a wired and/or a wireless network via any one or more wireless standards (e.g., Bluetooth or Wi-Fi) to exchange information with other devices that may be connected to the wired and/or wireless network. In so doing, for example, a wired and/or wireless network may be accessed by a mobile device without first accessing a mobile network via a cellular station of a mobile network.

[0275] Architecture 2750 may include contactless communication device 2762, which may communicate via

any one or more contactless communication methodologies, such as for example, near field communications (e.g., RFID), Bluetooth, touch simulation, light pulsing (e.g., via an LED), and electromagnetic data communication (e.g., via a dynamic magnetic stripe communications device). Accordingly, for example, contactless communication device 2762 may be compatible with any contactless device, such as for example, an RFID enabled payment card and a contactless reader (e.g., a magnetic stripe reader or an NFC reader).

[0276] A non-powered card may, for example, communicate with contactless communications device 2762. Contactless communication device 2762 may, for example, establish a carrier field (e.g., an RF field) that may be modulated by a device (e.g., an RFID tag) of a non-powered payment card. In so doing, for example, an RFID tag of a non-powered payment card may derive operational power from an RF field provided by contactless communications device 2762 and may communicate information (e.g., one, two, and/or three tracks of magnetic stripe data) to contactless communication device 2762 by modulating the RF field produced by contactless communications device 2762.

[0277] A powered card may, for example, communicate with contactless communication device 2762. A powered card may, for example, include a processor, a battery, a memory, wireless communications devices (e.g., a dynamic magnetic stripe communications device or RFID) and other electronics (e.g., buttons, displays, light sources and light sensors) that may allow a user to interact with the powered card to perform one or more functions. Accordingly, for example, a powered card

may be used to communicate specific information to contactless communication device 2762 by selective interaction with the buttons of the powered card. In so doing, for example, a powered card may be used to interactively communicate magnetic stripe information (e.g., one, two, and/or three tracks of magnetic stripe data) to contactless communication device 2762 by sending a signal to a processor of a powered card (e.g., by pressing a button on the powered card) to initiate such communications.

[0278] Contactless communication device 2762 may receive variable data sets from a powered card based upon, for example, manual input provided to a powered card. For example, a button associated with an on-line purchase may be pressed on the powered card that causes a variable data set (e.g., account number and expiration date) to be communicated from the powered card to contactless communication device 2762.

[0279] Discretionary data may, for example, be communicated by a powered card based upon which button was pressed on the powered card. In so doing, for example, a security code (e.g., "111") may be communicated within a discretionary data field when a button associated with a particular feature (e.g., pay with credit) is pressed on the powered card. As per another example, a different security code (e.g., "222") may be communicated within a discretionary data field when a button associated with a different feature (e.g., pay with debit) is pressed on the powered card. Accordingly, for example, processor 2758 may identify what type of device may be in communication with contactless communication device 2762 by analyzing the

data communicated to contactless communication device 2762.

[0280] Architecture 2750 may include memory 2760 and/or processor 2758 may include internal memory. Accordingly, for example, application code may be stored within memory 2760 and/or processor 2758 and executed by processor 2758 in support of functions performed by architecture 2750. For example, an application (e.g., a mobile wallet graphical user interface) may be executed by architecture 2750 and displayed onto display 2754, which may be used to interact with a user of a mobile device (e.g., mobile device 2700 of FIG. 27). Persons skilled in the art will appreciate that executable application code may be communicated to architecture 2750 via any one or more interfaces of architecture 2750 (e.g., user interface 2752, display 2754, transceiver 2756, and/or contactless communication device 2762).

[0281] Application data (e.g., virtual payment card data) may be stored within memory 2760 and accessed by processor 2758 during operation. For example, payment card data may be stored within memory 2760 and recalled by processor 2758 during a financial transaction being conducted by a mobile device (e.g., mobile device 2700 of FIG. 27). Once recalled, processor 2758 may communicate the payment card data via transceiver 2756 and/or contactless communication device 2762 to complete a financial transaction.

[0282] FIG. 28 shows network topology 2800 that may include, for example, mobile wallet 2802 (e.g., a mobile telephonic device, a PDA, an electronic tablet, a laptop, a GPS unit, or an MP3 player). Mobile wallet 2802 may, for example, include a contactless interface

that may initiate, sustain, and/or terminate a communication channel between a contactless device (e.g., an RFID enabled payment card) and mobile wallet 2802. A contactless device and mobile wallet 2802 may communicate using any number of contactless mediums, which may include for example, visible, audible, capacitive, electromagnetic, magnetic, and/or RF mediums.

[0283] Mobile wallet 2802 may provide one or more transceivers that may communicate with one or more wired networks (e.g., IP network 2812 and/or payment network 2814) and/or one or more wireless networks (e.g., mobile network 2810). Mobile wallet 2802 may, for example, communicate with a cellular station over a wireless radio interface (e.g., a GSM air interface) that may be used by mobile wallet 2802 to communicate information (e.g., voice and data) to cellular network access infrastructure 2806 (e.g., one or more GSM base transceiver stations, base station controllers, and mobile switching centers). Persons skilled in the art will appreciate that cellular network access infrastructure 2806 may utilize any multiple access architecture, such as for example, a code-division multiple access architecture and/or a time-division multiple access architecture.

[0284] Mobile wallet 2802 may, for example, communicate with wireless access point 2808 over a wireless interface (e.g., a Bluetooth interface or a Wi-Fi interface). Accordingly, for example, mobile wallet 2802 may access one or more wired networks (e.g., IP network 2812 and/or payment network 2814) and/or one or more wireless networks (e.g., mobile

network 2810) without the need to first gain access to cellular network access infrastructure 2806.

[0285] Any contactless device (e.g., a powered payment card or a non-powered payment card) may, for example, communicate with mobile wallet 2802 via a contactless medium. Accordingly, for example, payment information (e.g., a payment account number and a card expiration date) may be communicated from a contactless device to mobile wallet 2802. In so doing, for example, items for purchase on IP network 2812 (e.g., the internet) may be accessed by a browser of mobile wallet 2802 via an access point (e.g., wireless access point 2808 or cellular network access infrastructure 2806). Mobile wallet 2802 may, for example, complete a purchase transaction by first obtaining required payment information from a contactless device, storing such payment information and communicating such payment information to network entities (e.g., payment server 2816 and/or issuer 2820).

[0286] Payment server 2816 may, for example, contact issuer 2820 via a network (e.g., payment network 2814) with payment information received from mobile wallet 2802 for authorization of a purchase. Once authorized, payment transaction information may be recorded onto a receipt that may be delivered to mobile wallet 2802 via any one or more delivery options (e.g., via a short messaging service of mobile network 2810 or an email delivery service of IP network 2812). Mobile wallet 2802 may allow a user to associate purchase categories (e.g., groceries, auto repair, or entertainment) to purchases transacted by the mobile wallet so that the user may receive a more detailed accounting of his or her expenditures on his or her receipt. Accordingly,