



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.
13/017,823	06/05/2012	8195576	4508US1.014033.1145	7401

69603 7590 05/16/2012
Bank of America
c/o Moore and Van Allen, PLLC
430 DAVIS DRIVE, SUITE 500
POST OFFICE BOX 13706
RESEARCH TRIANGLE PARK, NC 27709

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 Data Management (ODM) at (571)-272-4200.

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

DAVID M. GRIGG, Rock Hill, SC;
Patrick B. Kelly, Charlotte, NC;
Alicia C. Jones, Fort Mill, SC;
Marc B. Keller, Charlotte, NC;

Change(s) applied
to document,
/D.H.P./
4/16/2012

[0054] In some embodiments, the input provided by the user is in the form of a hotkey, application, voice command, or movement of the mobile device. In these embodiments, the input automatically indicates that the transaction is authorized without needing to authenticate the user's identity further. U.S. Patent Application Serial No. 13/017835 to Grigg *et al.*, entitled "Transaction Authorization System for a Mobile Commerce Device," and filed concurrently herewith, describes such a device, system, and method in greater detail and is hereby incorporated by reference in its entirety.

[0055] The system receives security features for use with the authentication module, in some embodiments. For example, the security feature may be a username and password provided by the user and stored in the mobile device memory or on a server. Other examples of security features include facial images for use with facial recognition software, voice recordings for use with voice recognition software, iris images for use with iris scanning software, a bank of challenge questions and answers, a scanned fingerprint for use with fingerprint scanning software, or other features that are capable of authenticating the user's identity in conjunction with input from the user.

[0056] In an embodiment, the system compares the input with the security feature for the user **308**. For example, the system can compare the username and password entered by the user with a username and password previously stored by the user in the system to determine if the system is able to authenticate the user's identity. Similarly, the system could compare the facial scan with the saved image of the user's face, the voice sample with the saved voice recording, the response to the challenge question with the bank of challenge questions and answers previously saved by the user, the iris scan with the previously stored image of the user's iris, the fingerprint scan with the previously stored image of the user's fingerprint, or any other security feature capable of authenticating the user's identity.

[0057] In some embodiments, the system determines whether the user's identity is authenticated based on the comparison **310**. For example, if the input username and password match the saved username and password then the user's identity is authenticated. If, however, the user's identity is not authenticated based on the comparison of the input with the security feature the system can determine whether the user should have another opportunity to authenticate his identity **312**. For example, the

PART B - FEE(S) TRANSMITTAL

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

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

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

69603 7590 04/05/2012
 Bank of America
 c/o Moore and Van Allen, PLLC
 430 DAVIS DRIVE, SUITE 500
 POST OFFICE BOX 13706
 RESEARCH TRIANGLE PARK, NC 27709

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

Certificate of Mailing or Transmission

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

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/017,823	01/31/2011	DAVID M. GRIGG	4508US1.014033.1145	7401

TITLE OF INVENTION: MOBILE TRANSACTION DEVICE SECURITY SYSTEM

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	\$1740	\$300	\$0	\$2040	07/05/2012

EXAMINER	ART UNIT	CLASS-SUBCLASS
REAGAN, JAMES A	3621	705-067000

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

- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. Use of a Customer Number is required.

2. For printing on the patent front page, list

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

- 1 Michael A. Springs
 2 Moore & Van Allen PLLC
 3 Andrew D. Gerschütz

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

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

(A) NAME OF ASSIGNEE

Bank of America Corporation

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Charlotte, NC

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

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

- ☒ Issue Fee
- ☒ Publication Fee (No small entity discount permitted)
- ☒ Advance Order - # of Copies _____

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

- ☐ A check is enclosed.
- ☒ Payment by electronic funds transfer.
- ☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number 13-4365 (enclose an extra copy of this form).

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

- ☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.
- ☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

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

Authorized Signature

Andrew D. Gerschütz

Date May 4, 2012

Typed or printed name

Andrew D. Gerschütz

Registration No. 65,529

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

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

Electronic Patent Application Fee Transmittal				
Application Number:		13017823		
Filing Date:		31-Jan-2011		
Title of Invention:		MOBILE TRANSACTION DEVICE SECURITY SYSTEM		
First Named Inventor/Applicant Name:		DAVID M. GRIGG		
Filer:		Andrew D. Gerschutz/LaKeisha Preddie		
Attorney Docket Number:		4508US1.014033.1145		
Filed as Large Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl issue fee	1501	1	1740	1740
Publ. Fee- early, voluntary, or normal	1504	1	300	300

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				2040

Electronic Acknowledgement Receipt	
EFS ID:	12707199
Application Number:	13017823
International Application Number:	
Confirmation Number:	7401
Title of Invention:	MOBILE TRANSACTION DEVICE SECURITY SYSTEM
First Named Inventor/Applicant Name:	DAVID M. GRIGG
Customer Number:	69603
Filer:	Andrew D. Gerschutz
Filer Authorized By:	
Attorney Docket Number:	4508US1.014033.1145
Receipt Date:	04-MAY-2012
Filing Date:	31-JAN-2011
Time Stamp:	15:48:15
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Electronic Funds Transfer
Payment was successfully received in RAM	\$ 2040
RAM confirmation Number	2351
Deposit Account	
Authorized User	

File Listing:

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

1	Issue Fee Payment (PTO-85B)	Issue_Fee.pdf	89996 dc61b6c0cc8acb04219f04217b01607f25f4cde5	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	32143 3a6a322e4482d0e20bc14b0c141675da4ff55052	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			122139		
<p>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.</p> <p><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.</p> <p><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.</p> <p><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.</p>					



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

69603 7590 04/05/2012
Bank of America
c/o Moore and Van Allen, PLLC
430 DAVIS DRIVE, SUITE 500
POST OFFICE BOX 13706
RESEARCH TRIANGLE PARK, NC 27709

EXAMINER

REAGAN, JAMES A

ART UNIT

PAPER NUMBER

3621

DATE MAILED: 04/05/2012

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/017,823	01/31/2011	DAVID M. GRIGG	4508US1.014033.1145	7401

TITLE OF INVENTION: MOBILE TRANSACTION DEVICE SECURITY SYSTEM

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	\$1740	\$300	\$0	\$2040	07/05/2012

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

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

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

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

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

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

If the SMALL ENTITY is shown as NO:

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

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

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

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

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

PART B - FEE(S) TRANSMITTAL

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

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

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

69603 7590 04/05/2012
Bank of America
c/o Moore and Van Allen, PLLC
430 DAVIS DRIVE, SUITE 500
POST OFFICE BOX 13706
RESEARCH TRIANGLE PARK, NC 27709

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

Certificate of Mailing or Transmission

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

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/017,823	01/31/2011	DAVID M. GRIGG	4508US1.014033.1145	7401

TITLE OF INVENTION: MOBILE TRANSACTION DEVICE SECURITY SYSTEM

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	\$1740	\$300	\$0	\$2040	07/05/2012

EXAMINER	ART UNIT	CLASS-SUBCLASS
REAGAN, JAMES A	3621	705-067000

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

- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

- (1) the names of up to 3 registered patent attorneys or agents OR, alternatively, 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 has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

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

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

- ☐ Issue Fee
- ☐ Publication Fee (No small entity discount permitted)
- ☐ Advance Order - # of Copies _____

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

- ☐ A check is enclosed.
- ☐ Payment by credit card. Form PTO-2038 is attached.
- ☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

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

- ☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27. ☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

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

Authorized Signature _____

Date _____

Typed or printed name _____

Registration No. _____

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

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



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/017,823	01/31/2011	DAVID M. GRIGG	4508US1.014033.1145	7401
69603	7590	04/05/2012	EXAMINER	
Bank of America c/o Moore and Van Allen, PLLC 430 DAVIS DRIVE, SUITE 500 POST OFFICE BOX 13706 RESEARCH TRIANGLE PARK, NC 27709			REAGAN, JAMES A	
			ART UNIT	PAPER NUMBER
			3621	
DATE MAILED: 04/05/2012				

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

The Patent Term Adjustment to date is 0 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 0 day(s).

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

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

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

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.	Applicant(s)	
	13/017,823	GRIGG ET AL.	
	Examiner	Art Unit	
	JAMES A. REAGAN	3621	

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

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

1. ☒ This communication is responsive to the amendment and response filed on 03/16/2012.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on ____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are 1,4-7,11,12,14-16,18-23,25 and 27-39.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. ____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: ____.

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

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date ____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date ____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. ☐ 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)

<ol style="list-style-type: none"> 1. ☒ Notice of References Cited (PTO-892) 2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948) 3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date ____ 4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material 	<ol style="list-style-type: none"> 5. ☐ Notice of Informal Patent Application 6. ☐ Interview Summary (PTO-413), Paper No./Mail Date ____. 7. ☐ Examiner's Amendment/Comment 8. ☒ Examiner's Statement of Reasons for Allowance 9. ☐ Other ____.
--	--

--	--

DETAILED ACTION

Status of Claims

- 1.** This action is in reply to the amendment and response filed on **03/16/2012**.
- 2.** Claims 1, 5, 6, 11, 12, 14, 16, 18, 20, 25, and 27 have been amended.
- 3.** Claims 2, 3, 8-10, 13, 17, 24, and 26 have been canceled.
- 4.** Claims 1, 4-7, 11, 12, 14-16, 18-23, 25, and 27-39 are currently pending and have been examined.

Art Unit: 3621

Allowable Subject Matter

5. Claims 1, 4-7, 11, 12, 14-16, 18-23, 25, and 27-39 are allowed. See Reasons for Allowance under separate heading.

Reasons For Allowance

6. The following is an Examiner's statement of reasons for allowance:

None of the art of record, taken individually or combination, disclose at least the method step or system components of:

Claim 1:

A mobile transaction device security system comprising:

- *a memory device;*
- *a communication device; and*
- *a processing device coupled to the memory device, wherein the processing device is configured to:*
 - *receive a security protocol from a user, the security protocol comprising a permission module and an authentication module,*
 - *wherein the permission module comprises instructions on when the user must authenticate an identity of the user to perform a transaction,*
 - *wherein the instructions are provided by the user and stored in a database;*
 - *determine that the user is conducting a the transaction;*
 - *compare at least one characteristic of the transaction with the instructions provided by the user; and*
 - *determine a process for authenticating the user by:*
 - *determining if the user must authenticate the user's identity based on the comparison of the transaction with the instructions provided by the user,*
 - *allowing the transaction if the user is not required to authenticate the user's identity based on the comparison, and*

Art Unit: 3621

- *requiring authentication of the user through the authentication module if the comparison of the transaction to the instructions provided by the user indicates that the transaction cannot proceed without authentication,*
- *wherein requiring authentication comprises requesting authentication of the user's identity, receiving input from the user, comparing the input to the authentication module, and allowing the transaction if the user is authorized to perform the transaction based on the comparison of the input with the authentication module.*

Claim 12:

A computer-implemented method of providing financial transaction security, the method comprising:

- *receiving a security protocol from a user, the security protocol comprising a permission module and an authentication module,*
- *wherein the permission module comprises instructions on when the user must authenticate an identity of the user to perform a transaction,*
- *wherein the instructions are provided by the user and stored in a database;*
- *determining that the user is conducting a transaction;*
- *comparing at least one characteristic of the transaction with the instructions provided by the user;*
- *determining if the user must authenticate the user's identity based on the comparison of the transaction with the instructions provided by the user;*
- *allowing the transaction if the user does not need to authenticate the user's identity based on the comparison; and*

Art Unit: 3621

- *requiring authentication of the user through the authentication module if the comparison of the transaction to the instructions provided by the user indicates that the transaction cannot proceed without authentication,*
- *wherein requiring authentication comprises:*
- *requesting authentication of the user's identity,*
- *receiving input from the user,*
- *comparing the input to the authentication module, and allowing the transaction if the user is authorized to perform the transaction based on the comparison of the input with the authentication module.*

Claim 25:

A computer program product for providing a financial transaction security product, the computer program product comprising:

- *a non-transitory computer-readable medium comprising:*
- *an executable portion for causing a computer to receive a security protocol from a user, the security protocol comprising a permission module and an authentication module:*
- *wherein the permission module comprises instructions on when the user must authenticate an identity of the user to perform a transaction,*
- *wherein the instructions are provided by the user and stored in a database;*
- *an executable portion for causing a computer to determine that the user is conducting a transaction;*
- *an executable portion for causing a computer to compare at least one characteristic of the transaction with the instructions provided by the user;*
- *an executable portion for causing a computer to determine if the user must authenticate the user's identity an based on the comparison of the transaction with the instructions provided by the user; and*

Art Unit: 3621

- *an executable portion for causing a computer to allow the transaction if the user does not need to authenticate the user's identity based on the comparison; and*
- *an executable portion for requiring authentication of the user through the authentication module if the comparison of the transaction to the instructions provided by the user indicates that the transaction cannot proceed without authentication,*
- *wherein requiring authentication comprises:*
- *requesting authentication of the user's identity,*
- *receiving input from the user,*
- *comparing the input to the authentication module, and*
- *allowing the transaction if the user is authorized to perform the transaction based on the comparison of the input with the authentication module.*

The Examiner has carefully reviewed the Applicants arguments and assertions filed on **03/16/2012**. Based upon the Applicants arguments and assertions the Examiner is persuaded by and agrees with the Applicant. Fisher does not teach that the processing device is configured to determine the process for authenticating the user by determining if the user must authenticate an identity of the user based on the comparison of the transaction with the permission module, and wherein the processing device is further configured to allow the transaction if the user does not need to authenticate the user's identity. Ziegler is directed to biometric authentication of a customer's identity prior to allowing a transaction. Ziegler does not sufficiently disclose that a transaction can proceed without authentication based on comparison of the transaction to instructions provided by the user. Ziegler tends to teach away from allowing a transaction to proceed without authentication. Ziegler recites: "In any financial transaction, it may be important that the identity of both parties be authenticated in a manner which positively establishes the identities of the parties." See, paragraph [0003] of Ziegler.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Meyer, Roger. Secure Authentication on the Internet (04 April 2007) discloses, "This paper covers current Internet authentication mechanisms and possible attacks. It helps the reader to understand today's issues with authentication mechanisms. To understand the attack vectors, one has to know the current attack trends. Authentication systems can be classified according to their resistance against common attacks. Ten different authentication systems will be introduced and classified accordingly."
- CHEN et al. (GB 002401015A) discloses, "A security method and apparatus is provided in which a trusted authority (40) is arranged to receive data of an individual and to use it both as a biometric reference for comparison with biometric characteristics of a present individual (70A) in order to determine (44) whether the latter is the individual (70) represented by the data, and to generate a decryption key using the data and private data of the trusted authority (40). This decryption key is apt to decrypt data encrypted using both public data of the trusted authority and an encryption key string comprising the biometric data (50). The decryption key therefore may be generated in accordance with identifier-based cryptography (IBE) utilising quadratic residuosity (QR) or Weil or Tate pairings. The method/system may have application in password data storage and/or retrieval."

Art Unit: 3621

8. Any inquiry of a general nature or relating to the status of this application or concerning this communication or earlier communications from the Examiner should be directed to **James A. Reagan** (james.reagan@uspto.gov) whose telephone number is **571.272.6710**. The Examiner can normally be reached on Monday-Friday, 9:30am-5:00pm. If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, **ANDREW J. FISCHER** can be reached at **571.272.6779**.
9. Should Applicant desire in the future to receive formal or informal email communications from the Examiner (e.g. acknowledgments, references, courtesy copies of documents, etc.), the electronic file must contain written authorization to conduct email communications. See MPEP §502.03 III. For Applicant's benefit, exemplary language for written authorization is in MPEP §502.03 III. ¶4. The exemplary language is:

Recognizing that Internet communications are not secure, I hereby authorize the USPTO to communicate with me concerning any subject matter of this application by electronic mail. I understand that a copy of these communications will be made of record in the application file.

10. In the situation where Applicant desires to receive email communications from the Examiner, the Examiner suggests placing the above exemplary language in Applicant's next correspondence.
11. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://portal.uspto.gov/external/portal/pair> . Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at **866.217.9197** (toll-free).

Art Unit: 3621

12. Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

Washington, D.C. 20231

or faxed to **571-273-8300**.

13. Hand delivered responses should be brought to the **United States Patent and Trademark**

Office Customer Service Window:

Randolph Building

401 Dulany Street

Alexandria, VA 22314.

/James A. Reagan/
Primary Examiner, Art Unit 3621
james.reagan@uspto.gov
571.272.6710 (Office)
571.273.6710 (Desktop Fax)

Notice of References Cited	Application/Control No. 13/017,823	Applicant(s)/Patent Under Reexamination GRIGG ET AL.	
	Examiner JAMES A. REAGAN	Art Unit 3621	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2006/0021003 A1	01-2006	Fisher et al.	726/001
*	B	US-2006/0123465 A1	06-2006	Ziegler, Robert	726/002
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N	GB 2401015 A	10-2004	United Kingdom	CHEN et al.	G06F 01/00
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Meyer, Roger. Secure Authentication on the Internet (04 April 2007). Retrieved online 27 March 2012. http://www.sans.org/reading_room/whitepapers/securecode/secure-authentication-internet_2084 . 36 pps.
	V	
	W	
	X	

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

(21) Application No: **0408908.2**
 (22) Date of Filing: **22.04.2004**
 (30) Priority Data:
 (31) **0309182** (32) **23.04.2003** (33) **GB**
 (31) **0311724** (32) **22.05.2003**

(71) Applicant(s):
Hewlett-Packard Development Company L.P.
20555 S.H. 249, Houston, Texas 77070,
United States of America

(72) Inventor(s):
Liqun Chen
Keith Alexander Harrison

(74) Agent and/or Address for Service:
Hewlett-Packard Limited
Intellectual Property Section, Building 3,
Filton Road, Stoke Gifford, BRISTOL,
BS34 8QZ, United Kingdom

(51) INT CL⁷:
G06F 1/00 , G06K 9/00 , H04L 9/00 9/32

(52) UK CL (Edition W):
H4P PPEB
G4A AAP A23C
G4H HTG H1A H14A H2B H2P

(56) Documents Cited:
GB 2370471 A **WO 2003/017559 A2**
WO 2002/073877 A2 **US 4993068 A**
[http://www.hpl.hp.com/techreports/2002/HPL 2002 185.pdf](http://www.hpl.hp.com/techreports/2002/HPL%2020185.pdf), **AA trusted biometric system@**, **Chen et al.**, **HP Labs**, last modified 30 July 2002

(58) Field of Search:
 UK CL (Edition W) **G4A, H4P**
 INT CL⁷ **G06F, G06K, G07F, H04L**
 Other: **WPI, EPODOC, PAJ, INSPEC and selected internet sites**

(54) Abstract Title: **Security method and apparatus using biometric data**

(57) A security method and apparatus is provided in which a trusted authority (40) is arranged to receive biometric data of an individual and to use it both as a biometric reference for comparison with biometric characteristics of a present individual (70A) in order to determine (44) whether the latter is the individual (70) represented by the biometric data, and to generate a decryption key using the biometric data and private data of the trusted authority (40). This decryption key is apt to decrypt data encrypted using both public data of the trusted authority and an encryption key string comprising the biometric data (50). The decryption key therefore may be generated in accordance with identifier-based cryptography (IBE) utilising quadratic residuosity (QR) or Weil or Tate pairings. The method/system may have application in password data storage and/or retrieval.

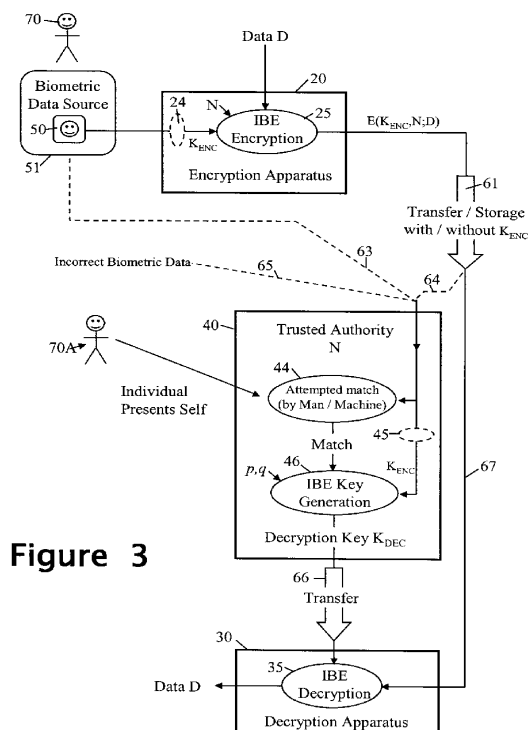


Figure 3

Original Printed on Recycled Paper

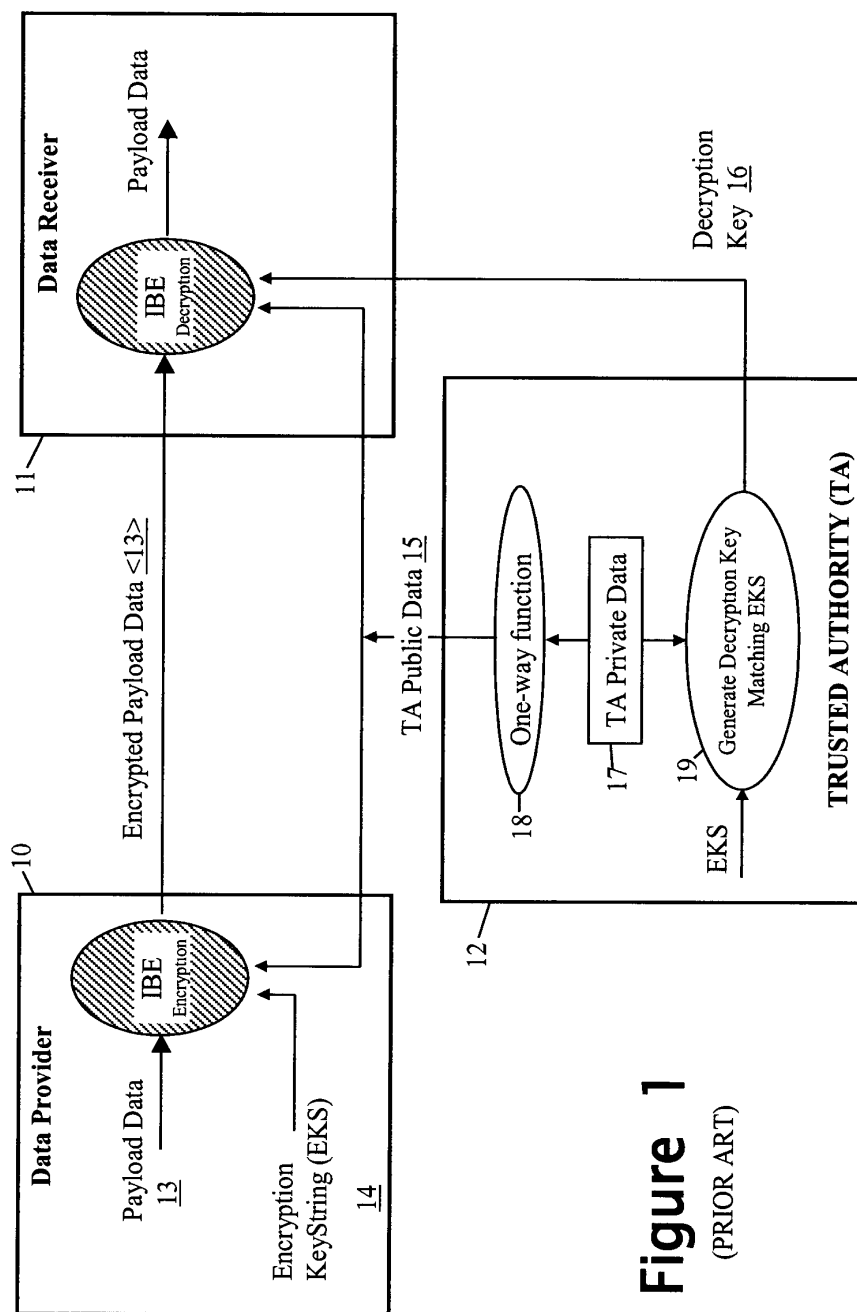
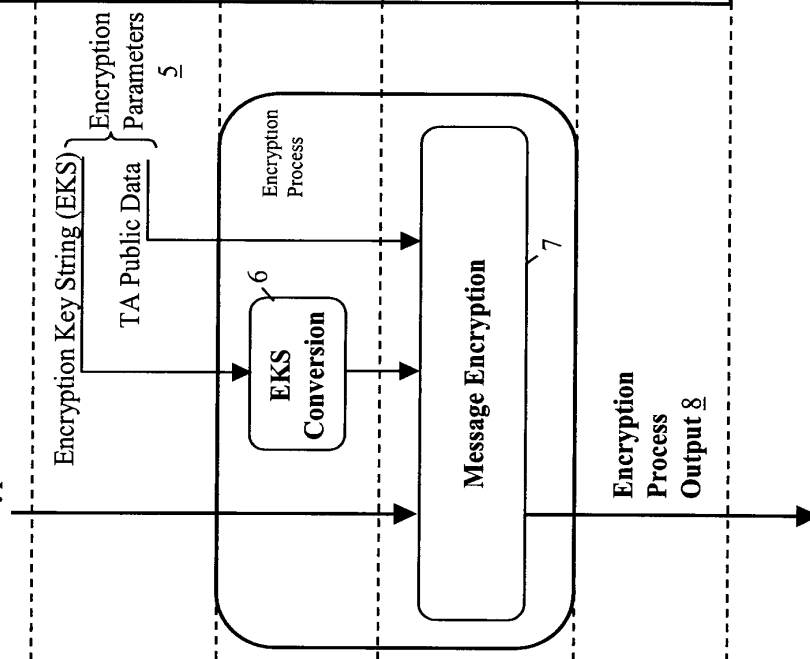


Figure 1
(PRIOR ART)

Figure 2

Message data m
for encryption

(PRIOR ART)



Identifier-Based Method		
Quadratic Residuosity	Bilinear Mappings $p: G_1 \times G_1 \rightarrow G_2$	RSA Based
EKS Modulus N	EKS (P, sP) where P is in G_1 s is secret of TA	EKS Modulus n
$K = \#(\text{EKS})$	“Map-to-point” hash $Q_{\text{ID}} = H_1(\text{EKS})$ where $H_1: \{0,1\}^* \rightarrow G_1$	$e = \#(\text{EKS}) \bmod n$
For each bit: $s_+ \equiv (t_+ + K/t_+) \bmod N$ $s_- \equiv (t_- - K/t_-) \bmod N$	$V = m \oplus H_2(t(sP, rQ_{\text{ID}}))$ where: $H_2: G_2 \rightarrow \{0,1\}^*$ r is a random number	$m^e \bmod n$
For each bit: s_+, s_- (knowledge of EKS and TA concerned also needs to be available)	$V, U (= rP)$	$m^e \bmod n$

3/4

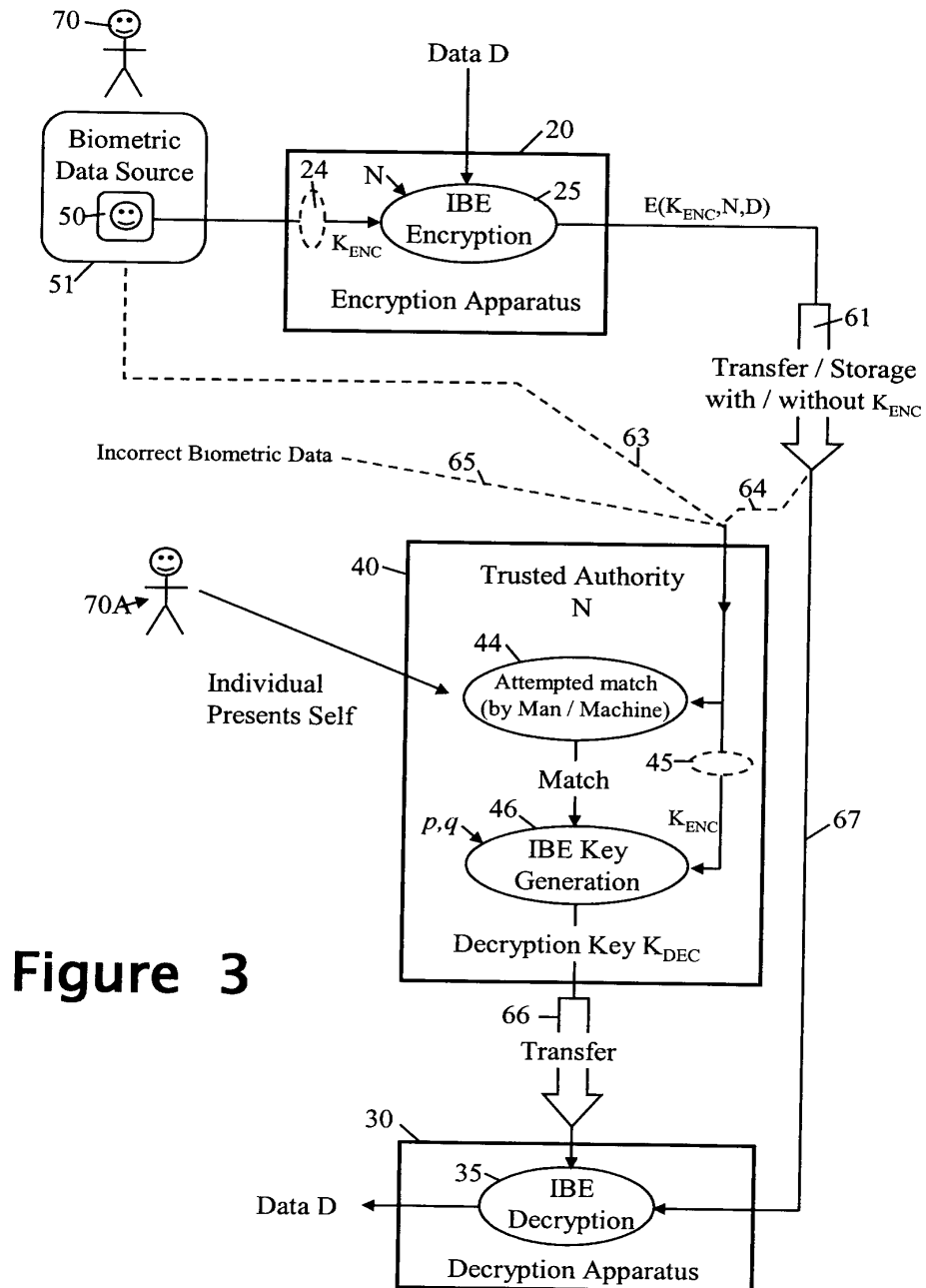


Figure 3

4 / 4

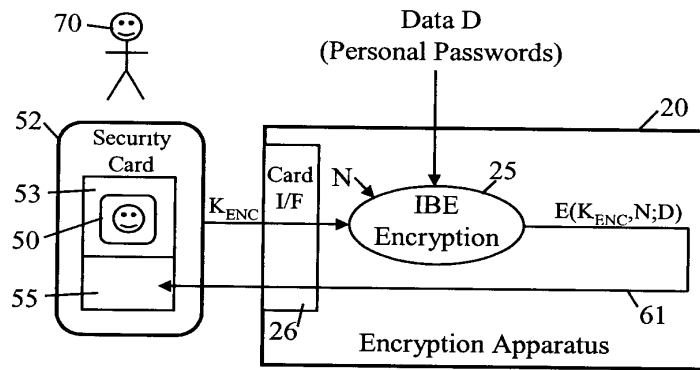


Figure 4A

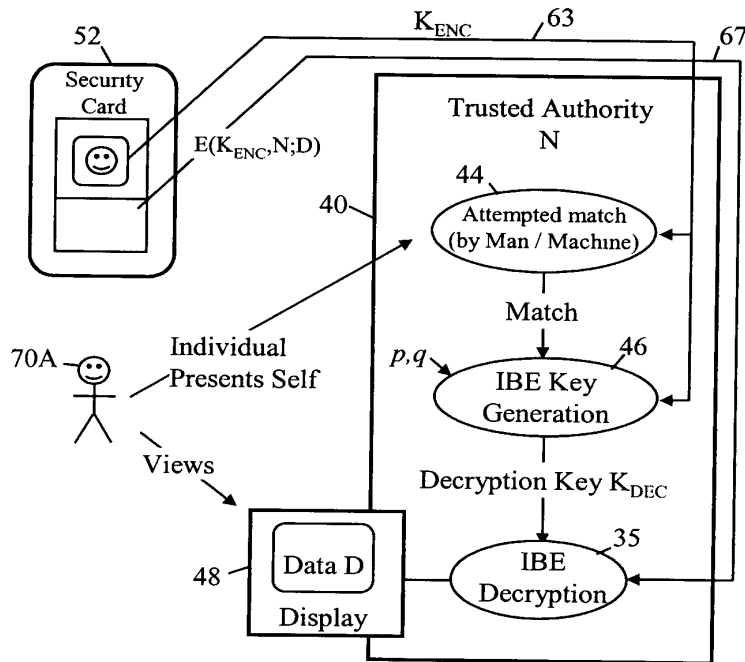


Figure 4B

Security Method and Apparatus Using Biometric Data**Field of the Invention**

- 5 The present invention relates to security methods and apparatuses using biometric data; in particular, the present invention relates to such methods and apparatuses that utilise identifier-based encryption/decryption and analogous techniques.

As used herein, the term “biometric data” means any digital data, however measured or
10 recorded, that represents characteristics of a biological individual intended to be unique to that individual. Thus, both digital image data of a human face and digital fingerprint data are examples of biometric data.

Background of the Invention

- 15 The use of biometric data for authenticating individuals is well known. It is also known to use biometric authentication techniques in relation to memory-based identity cards – for example, such a card can carry fingerprint data concerning the card owner, this data being used to check whether a person presenting the card is the card owner by comparing the data from the card with that generated by a local fingerprint reader. Of course, the biometric
20 data on such a card has to be trustable; more particularly, the card should have the properties of trustworthiness and unforgeability. Trustworthiness means that any information stored in the card must be issued by a trusted authority (that is, an authority trusted by the party relying on the authenticity of the stored biometric data). Unforgeability means that any information stored in the card cannot be modified by an unauthorized entity
25 without being detected (a typical, but not the only, example of a suitable form of card would be one using a write-once memory chip).

It is also known to provide memory-based cards with cryptographic functions. For example, data may be stored in encrypted form on the card and only accessible after the
30 card owner has entered a decryption key which the card uses to decrypt the stored data before it is output from the card.

It is an object of the present invention to provide improved security methods based on biometric data, such methods being usable, without limitation, in relation to memory-based security cards.

- 5 The present invention is in part based on the appreciation that Identifier-Based Encryption (IBE) has certain properties than can be adapted for use in memory-card based security systems and other applications.

Identifier-Based Encryption (IBE) is an emerging cryptographic schema. In this schema
10 (see Figure 1 of the accompanying drawings), a data provider 10 encrypts payload data 13 using both an encryption key string 14, and public data 15 provided by a trusted authority 12. This public data 15 is derived by the trusted authority 12 using private data 17 and a one-way function 18. The data provider 10 then provides the encrypted payload data <13> to a recipient 11 who decrypts it, or has it decrypted, using a decryption key
15 computed by the trusted authority 12 in dependence on the encryption key string and its own private data.

A feature of identifier-based encryption is that because the decryption key is generated from the encryption key string, its generation can be postponed until needed for decryption.
20

Another feature of identifier-based encryption is that the encryption key string is cryptographically unconstrained and can be any kind of string, that is, any ordered series of bits whether derived from a character string, a serialized image bit map, a digitized sound signal, or any other data source. The string may be made up of more than one component
25 and may be formed by data already subject to upstream processing. In order to avoid cryptographic attacks based on judicious selection of a key string to reveal information about the encryption process, as part of the encryption process the encryption key string is passed through a one-way function (typically some sort of hash function) thereby making it impossible to choose a cryptographically-prejudicial encryption key string. In applications
30 where defence against such attacks is not important, it would be possible to omit this processing of the string.

Frequently, the encryption key string serves to “identify” the intended message recipient and the trusted authority is arranged to provide the decryption key only to this identified intended recipient. This has given rise to the use of the label “identifier-based” or “identity-based” generally for cryptographic methods of the type under discussion. However, depending on the application to which such a cryptographic method is put, the string may serve a different purpose to that of identifying the intended recipient and may be used to convey other information to the trusted authority or, indeed, may be an arbitrary string having no other purpose than to form the basis of the cryptographic processes. Accordingly, the use of the term “identifier-based” or “IBE” herein in relation to cryptographic methods and systems is to be understood simply as implying that the methods and systems are based on the use of a cryptographically unconstrained string whether or not the string serves to identify the intended recipient. Generally, in the present specification, the term “encryption key string” or “EKS” is used rather than “identity string” or “identifier string”; the term “encryption key string” is also used in the shortened form “encryption key” for reasons of brevity.

A number of IBE algorithms are known and Figure 2 indicates, for three such algorithms, the following features, namely:

- the form of the encryption parameters 5 used, that is, the encryption key string and the public data of the trusted authority (TA);
- the conversion process 6 applied to the encryption key string to prevent attacks based on judicious selection of this string;
- the primary encryption computation 7 effected;
- the form of the encrypted output 8.

The three prior art IBE algorithms to which Figure 2 relates are:

- **Quadratic Residuosity (QR) method** as described in the paper: C. Cocks, “An identity based encryption scheme based on quadratic residues”, Proceedings of the 8th IMA International Conference on Cryptography and Coding, LNCS 2260, pp 360-363, Springer-Verlag, 2001. A brief description of this form of IBE is given hereinafter.
- **Bilinear Mappings** p using, for example, a modified Tate pairing t or modified Weil pairing e for which:

$$p: G_1 \times G_1 \longrightarrow G_2$$

where G_1 and G_2 denote two algebraic groups of prime order q and G_2 is a subgroup of a multiplicative group of a finite field. For the Tate pairing an asymmetric form is also possible:

$$p: G_1 \times G_0 \longrightarrow G_2$$

5 where G_0 is a further algebraic group the elements of which are not restricted to being of order q . Generally, the elements of the groups G_0 and G_1 are points on an elliptic curve though this is not necessarily the case. A description of this form of IBE method, using modified Weil pairings is given in the paper: D. Boneh, M. Franklin – “Identity-based Encryption from the Weil Pairing” in *Advances in Cryptology - CRYPTO 2001*,
10 LNCS 2139, pp. 213-229, Springer-Verlag, 2001.

- **RSA-Based methods** The RSA public key cryptographic method is well known and in its basic form is a two-party method in which a first party generates a public/private key pair and a second party uses the first party’s public key to encrypt messages for sending to the first party, the latter then using its private key to decrypt the messages. A
15 variant of the basic RSA method, known as “mediated RSA”, requires the involvement of a security mediator in order for a message recipient to be able to decrypt an encrypted message. An IBE method based on mediated RSA is described in the paper “Identity based encryption using mediated RSA”, D. Boneh, X. Ding and G. Tsudik, 3rd Workshop on Information Security Application, Jeju Island, Korea, Aug, 2002.

20 A more detailed description of the QR method is given below with reference to the entities depicted in Figure 1 and using the same notation as given for this method in Figure 2. In the QR method, the trust authority’s public data 15 comprises a value N that is a product of two random prime numbers p and q , where the values of p and q are the private data 17 of
25 the trust authority 12. The values of p and q should ideally be in the range of 2^{511} and 2^{512} and should both satisfy the equation: $p, q \equiv 3 \pmod{4}$. However, p and q must not have the same value. Also provided is a hash function $\#$ which when applied to a string returns a value in the range 0 to $N-1$.

30 Each bit of the user’s payload data 13 is then encrypted as follows:

- The data provider 10 generates random numbers t_+ (where t_+ is an integer in the range $[0, 2^N]$) until a value of t_+ is found that satisfies the equation $\text{jacobi}(t_+, N) = m'$, where m' has a value of -1 or 1 depending on whether the corresponding bit of the user's data is 0 or 1 respectively. (As is well known, the *jacobi* function is such that where $x^2 \equiv \# \pmod N$ the *jacobi* ($\#, N$) = -1 if x does not exist, and = 1 if x does exist). The data provider 10 then computes the value:

$$s_+ \equiv (t_+ + K/t_+) \pmod N$$

where: s_+ corresponds to the encrypted value of the bit m' concerned, and

$$K = \#(\text{encryption key string})$$

10

- Since K may be non-square, the data provider additionally generates additional random numbers t_- (integers in the range $[0, 2^N]$) until one is found that satisfies the equation $\text{jacobi}(t_-, N) = m'$. The data provider 10 then computes the value:

$$s_- \equiv (t_- - K/t_-) \pmod N$$

15 as the encrypted value of the bit m concerned.

The encrypted values s_+ and s_- for each bit m' of the user's data are then made available to the intended recipient 11, for example via e-mail or by being placed in a electronic public area; the identity of the trust authority 12 and the encryption key string 14 will generally also be made available in the same way.

The encryption key string 14 is passed to the trust authority 12 by any suitable means; for example, the recipient 11 may pass it to the trust authority or some other route is used - indeed, the trust authority may have initially provided the encryption key string. The trust authority 12 determines the associated private key B by solving the equation :

$$B^2 \equiv K \pmod N \quad (\text{"positive" solution})$$

If a value of B does not exist, then there is a value of B that is satisfied by the equation:

$$B^2 \equiv -K \pmod N \quad (\text{"negative" solution})$$

As N is a product of two prime numbers p, q it would be extremely difficult for any one to calculate the decryption key B with only knowledge of the encryption key string and N .

However, as the trust authority 12 has knowledge of p and q (i.e. two prime numbers) it is relatively straightforward for the trust authority 12 to calculate B .

Any change to the encryption key string 14 will result in a decryption key 16 that will not
 5 decrypt the payload data 13 correctly. Therefore, the intended recipient 11 cannot alter the encryption key string before supplying it to the trust authority 12.

The trust authority 12 sends the decryption key to the data recipient 11 along with an indication of whether this is the “positive” or “negative” solution for B .

10

If the “positive” solution for the decryption key has been provided, the recipient 11 can now recover each bit m' of the payload data 13 using:

$$m' = \text{jacobi}(s_+ + 2B, N)$$

If the “negative” solution for the decryption key B has been provided, the recipient 11
 15 recovers each bit m' using:

$$m' = \text{jacobi}(s_- + 2B, N)$$

Summary of the Invention

According to one aspect of the present invention, there is provided a security method,
 20 carried out by a trusted authority, comprising receiving biometric data of a specific individual, and using the biometric data both:

as a biometric reference for comparison with biometric characteristics of a subject individual to determine whether the latter is said specific individual, and
 to generate a decryption key based on at least the biometric data and private data of the
 25 trusted authority.

The present invention also envisages apparatus and a computer program product corresponding to the foregoing security method of the invention.

30 According to another aspect of the present invention, there is provided a data access control method comprising:

- (a) encrypting first data based on encryption parameters comprising public data of a trusted authority and an encryption key string formed using at least biometric data of a specific individual;
- (b) providing the biometric data of said specific individual to the trusted authority which
5 uses it both:
- as a biometric reference for comparison with biometric characteristics of a subject individual to determine whether the latter is said specific individual, and
to generate a decryption key based on at least the biometric data and private data of
the trusted authority, said public data of the trusted authority being related to its
10 private data;
- (c) using the decryption key to decrypt the encrypted first data.

In one preferred embodiment, in step (a) the biometric data of said specific individual is read from a memory device of the specific individual and the encrypted first data is stored
15 back to the memory device. When the specific individual wishes to retrieve the first data, that individual presents the memory device to the trusted authority which reads off the biometric data of said specific individual, and then if satisfied that the individual is the specific individual, the trusted authority decrypts the first data and makes it available to the specific individual. This embodiment provides a simple way for a person to store password
20 data securely and later retrieve it.

In another preferred embodiment, step (a) is carried out by a data provider with the biometric data of said specific individual being image data derived from a photograph of the said specific individual, the biometric data of the specific individual being sent to a
25 receiving party together with the encrypted first data for use by the trusted authority in step (b).

In a further preferred embodiment, step (a) is carried out by a data provider with said biometric data of the specific individual comprising data that is the same as biometric data
30 stored on a memory device of said specific individual as a result of having been either read from that card or provided from a common source. The aforesaid subject individual seeks to obtain the decryption key from the trusted authority by presenting a memory device to

the trusted authority to enable the latter to read off biometric data stored in the device and use it as said encryption key; the trusted authority only provides the decryption key to the subject individual if the latter is determined in step (b) to be said specific individual.

- 5 The present invention also envisages a system for implementing the foregoing data access control method of the invention.

Brief Description of the Drawings

- 10 Embodiments of the invention will now be described, by way of non-limiting example, with reference to the accompanying diagrammatic drawings, in which:
- . Figure 1 is a diagram illustrating the operation of a prior art encryption schema known as Identifier-Based Encryption;
 - . Figure 2 is a diagram illustrating how certain IBE operations are implemented by
 - 15 three different prior art IBE methods;
 - . Figure 3 is a diagram of a generalized system embodying the present invention;
 - . Figure 4A is a diagram of a data encryption stage of a first specific example of the Figure 3 system; and
 - . Figure 4B is a diagram of key generation and decryption stages of the first specific
 - 20 example of the Figure 3 system.

Best Mode of Carrying Out the Invention

- Figure 3 illustrates a generalised system embodying the present invention, the system
- 25 comprising: a data encryptor entity 20 for encrypting data D using an encryption key string K_{ENC} and public data of a trusted authority; a trusted authority entity 40 for generating a decryption key K_{DEC} based on the encryption key string K_{ENC} and private data of the trusted authority, the public data being data generated by the entity 40 and being computationally related to the trusted authority's private data ; and a data decryptor entity 30 for using the
- 30 decryption key K_{DEC} and the public data to decrypt the encrypted data D. The entities 20, 30 and 40 are typically based around general-purpose processors executing stored programs but may include dedicated cryptographic hardware modules; furthermore, as will be

discussed below, certain functions of the trusted authority may be carried out by human operators. The computing entities 20, 30 and 40 inter-communicate as needed via, for example, the internet or other network, or by the transfer of data using portable storage devices; it is also possible that at least some of the entities actually reside on the same computing platform. Indeed, in certain embodiments the data decryptor entity 30 may be incorporated into the trusted authority entity 40 whilst in other embodiments the data encryptor entity 20 and the data decryptor entity 30 may be associated with the same individual and be provided by the same computing device.

- 10 The system employs Identifier-Based Encryption with the entities 20, 30 and 40 having, in respect of IBE encryption/decryption processes, the roles of the data provider 10, data recipient 11 and trusted authority 12 of the Figure 1 IBE arrangement. The IBE algorithm used is, for example, the QR algorithm described above with respect to Figure 1 with the private data of the trusted authority being random prime numbers p, q and the
15 corresponding public data being number N .

The encryption key string K_{ENC} is based on biometric data 50 of a specific individual 70. This biometric data is represented in Figure 3 by a face icon but can be any type of biometric data and is not limited to a facial image; possible types of biometric data include
20 image data, fingerprint data, retina scan data etc. The biometric data can be compressed in form and can be obscured for privacy reasons, for example, by being subject to a known one-way function.

The biometric data 50 is provided in digital form to the encryptor entity 20 from a
25 biometric data source 51 that may take a variety of forms. For example, the biometric data source 51 may be a capture device (such as a camera or fingerprint reader) for generating the biometric data directly from the individual 70 at the time it is required for use by the entity 20 – in other words, the individual 70 is present at the entity 20 at the time the data D is to be encrypted. Alternatively, the biometric data can be generated from an analogue
30 storage source (such as a photographic print) or retrieved from a digital data storage medium; in particular, in one embodiment, the biometric data 50 is stored in digital form

on a memory card or other storage device 51 that belongs to the individual 70 and that preferably has the aforementioned properties of trustworthiness and unforgeability

The biometric data 50 is used by the entity 20 to form the encryption key string K_{ENC} , the
 5 biometric data either being used directly as the key or after processing (see dashed operation oval 24) such as by concatenation with other data. The encryption key string K_{ENC} is then used to encrypt data D to form encrypted data $E(K_{ENC}, N; D)$ where $E()$ indicates that the elements appearing before the semi-colon inside the brackets are used to
 10 IBE encrypt the element appearing after the semi-colon. The encrypted data is then either stored to a storage medium for eventual transfer to the decryptor entity 30, or sent over a communications link directly or indirectly to the decryptor entity 30 (see arrow 61). Where the biometric data source is a storage device, the encrypted data may, in certain embodiments, be stored to this device as will be more fully described hereinafter. The biometric data 50 per se or as incorporated into the encryption key string K_{ENC} may be
 15 stored or transmitted along with the encrypted data.

When an individual 70A who may or may not be the same as the individual 70, wishes to access the encrypted data $E(K_{ENC}, N; D)$ this individual presents themselves to the trusted authority entity 40 to which is also provided biometric data that may or may not be that
 20 used in the encryption key string K_{ENC} .

Considering first the situation where the biometric data is genuine – that is, it really is the biometric data used in the encryption key string K_{ENC} – this is represented in Figure 3 by the dashed arrows 63 and 64. The arrow 63 represents the case where the biometric data
 25 provided to the encryptor entity 20 and the trusted authority entity 40 is passed to each entity from the same source 51, for example, because the biometric data is provided from off the same memory card to both entities. The arrow 64 represents the case where the biometric data was output by the entity 20 along with the encrypted data (typically, but not necessarily, in its form incorporated into the encryption key string K_{ENC}) and has now been
 30 passed to the trusted authority. Where the biometric data only forms part of the encryption key string K_{ENC} but is provided in this form to the trusted authority, the latter is arranged to extract the biometric data from the key.

The trusted authority entity first uses the biometric data 50 as a biometric reference for comparison with biometric characteristics of the individual 70A to determine whether the latter is the individual 70 (see operation oval 44). As is well known to persons skilled in the art, this comparison and determination may be carried out automatically by comparing features represented in the reference biometric data 50 with features in measurement data produced by measurement of the subject individual 70A using biometric measurement equipment. Where the biometric data 50 is of obscured form (that is, the biometric measurements of individual 70 have been subject to a one-way function, for example, to produce the data 50), the un-obscured biometrics of individual 70 will have first been translated into biometric feature categories; accordingly, the same feature categorisation and obscuring functions must be applied to the biometric characteristics of the individual 70A to produce data for comparison with the biometric data 50. This categorisation is necessary because when the biometric data is in its obscured form, the comparison operation 44 can only be based on an exact match (a near match being meaningless).

Particularly where the biometric data comprises facial image data, an alternative to effecting an automatic biometric comparison, is to have a human operator presented with the biometric reference data (for example, as an image of a face where the biometric data is facial image data), this operator then judging whether the present individual 70A is the same as that represented by the biometric data.

If no match is found between the individual 70A and that represented by the biometric data 50, the trusted authority 40 refuses to proceed with the generation of the decryption key K_{DEC} needed to access the encrypted data. However, if a match is found in operation 44, the trusted authority proceeds. Where biometric data 50 does not constitute the encryption key string K_{ENC} in its entirety, the next operation is to re-form the encryption key string (see dashed operation oval 45) – this may involve the concatenation of the biometric data with other data known to both the entities 20 and 40. For example, this other data may simply be an item of non-confidential data or it may be a shared secret; this other data may vary between encryption operations of the entity 20. Of course, where the encryption key

string K_{ENC} itself was provided to the trusted authority, then this is used directly without needing to reform it.

Once the encryption key string has been obtained, the trusted authority uses it, along with its private data p, q , to generate the decryption key K_{DEC} (see operation oval 46). As can be seen, the same biometric data that was used as the biometric reference data in operation 44 is also used in the process 46 of generating the decryption key K_{DEC} .

The decryption key K_{DEC} is then transferred (see arrow 66) to the data decryptor entity 30 to which the encrypted data $E(K_{ENC}, N; D)$ is also supplied (see arrow 67). The transfer of the decryption key to the entity 30 from the entity 40 may be effected over a communications link or via a data storage device; as already indicated, in certain embodiments, the decryption entity 30 is actually part of the trusted authority so no transfer is required. The decryption key K_{DEC} is thereafter used to decrypt the encrypted data to recover the data D in clear (operation 35). Where the decryption is effected by the trusted party entity 40, the recovered data D is typically then provided to the individual 70A (now known to be the individual 70) either by displaying it or by the transfer of an electronic or paper copy to the individual; however, the trusted authority may decide not to disclose the data D .

It will be appreciated that the trusted authority can carry out the key generation operation 46 in parallel with, or even before, having determined that the individual 70A is the individual 70 – what is important is that the entity 40 does not provide the decryption key (or where it also effects the decryption operation 35, the recovered data D) to the individual 70A until the latter is determined to be the individual 70.

The foregoing description of the operation of the trusted authority entity 40 was for the situation of the biometric data provided to the entity being the genuine biometric data 50 used in the encryption key string K_{ENC} . If the biometric data presented to the trusted authority entity 40 is not that used for the encryption key string (represented by dashed arrow 65 in Figure 3) as may be the case where the individual 70A is not the individual 70 and tries to fool the trusted authority by presenting their own biometric data, then even

though the trusted authority may be fooled into generating a decryption key, this key will not serve to decrypt the encrypted data $E(K_{ENC}, N; D)$. This is because the trusted authority uses the same biometric data for both operations 44 and 46.

- 5 Figures 4A and 4B illustrates a first specific embodiment of the generalized Figure 3. system. In this embodiment, the biometric data of the individual 70 is stored on a memory card 52 that serves as a security card for an organisation such as a commercial enterprise. The card has, for example, a picture of the individual 70 on its front face and an embedded memory chip divided into a write-once first portion 53 holding the biometric data 50 and a
 10 re-writable second portion 55. For simplicity, in the present example it is assumed that the biometric data 50 directly constitutes the encryption key string K_{ENC} to be used by the encryptor entity 20 to encrypt data D.

- Suppose the individual 70 wishes to safely store all the many passwords that he/she has for
 15 accessing various services. In this case, the individual supplies these passwords as the data D to an encryptor entity 20 that includes a card reader 26. The entity 20 reads the biometric data 50 from the card 52 and uses it as the encryption key string K_{ENC} to encrypt the passwords (operation 25); the entity 20 then writes the encrypted data to the rewritable portion 55 of the memory card 52. The individual 70 now has their passwords safely stored
 20 in their memory card 52. The entity 20 can be provided by a computer or other device under the control of the individual or can be provided by the trusted authority – in this example, the trusted authority may be the security office of the enterprise.

- Should the individual 70 forget any of their passwords, he/she goes to the trusted authority
 25 (security office) and presents their memory card 52 (see Figure 4B). The biometric data 50 is read off this card by the trusted authority entity and used in operation 44 to check that the individual presenting the memory card 52 is the owner of the card as indicated by the biometric data on the card. Preferably, the biometric data 50 is a facial image of the individual enabling a security office member to readily check that the individual presenting
 30 the card is the card owner. Assuming that the check 44 is passed, the decryption key K_{DEC} is generated and used by the trusted authority entity to decrypt the password data D held on

the card; this password data is then displayed to the individual 70 on a display 48 in a manner such that the data D is not visible to members of the security office.

5 Rather than the password storage device being an enterprise security card and the trusted authority being a security office, the individual can store their passwords on any storage medium they deem appropriate and select any party as a trusted authority provided the latter can be trusted to keep their private data (p, q) confidential and not to retain copies of the decrypted passwords. Another possible trusted authority would be a trusted computing platform having functionality such as specified, for example, in "TCPA - Trusted
10 Computing Platform Alliance Main Specification v1.1" www.trustedcomputing.org, 2001 and described in the book "trusted computing platforms – tcpa technology in context"; Pearson (editor); Prentice Hall; ISBN 0-13-009220-7".

15 According to a second specific embodiment of the generalized Figure 3. system, the encryptor entity 20 is operated by a data provider that wishes to send data D to the individual 70 in a secure manner. The data provider has a reasonably current photograph of the individual 70 and so the data provider scans in the photograph to produce digital image data which is then used as the biometric data 50 from which an encryption key string K_{ENC} is formed. The data D is then encrypted using this key and the public data of a trusted
20 authority such as a post office local to the individual. The data provider sends the encrypted data and the encryption key string K_{ENC} to the individual 70 who extracts the encryption key string, puts it on a floppy disc (or other storage device) and takes it to their local post office acting as a trusted authority. The post office reads the biometric data and brings up an image which a counter clerk then uses to determine if the individual
25 presenting the biometric data is that represented by the data; if so, the clerk causes the biometric data to be used to generate a decryption key which is then stored to the storage device of the individual. The individual can now take away the decryption key and use it to recover the data D in clear.

30 According to a third specific embodiment of the generalized Figure 3 system, an individual has a memory card holding their biometric data. This individual wishes to store sensitive data D (such as their medical records) from a data provider and accordingly presents the

memory card to the data provider. The data provider reads off the biometric data and first confirms that this data corresponds to the individual present. Assuming this is the case, the data provider encrypts the data D and stores it back to the card. If at any time in the future, access is required to the sensitive data, a trusted authority reads off the biometric data and
5 confirms that the card belongs to the individual concerned before generating the decryption key and decrypting the data D. In this embodiment, one would normally require some consensual act by the card owner (such as presentation of the card to the trusted authority); however, this embodiment also allows the trusted authority to access the data D in an emergency situation - as might be needed where the individual has had a road traffic
10 accident and the attending medical staff need urgently to access the medical record data D recorded on the card (in this case, the trusted authority would be the emergency services).

In the foregoing example, the data provider could in fact have initially obtained the biometric data not from the card but from a common source – for example, the card and the
15 encrypted data may be created simultaneously using the same biometric data.

As already noted, the encryption key string K_{ENC} may comprise data additional to the biometric data 50. This additional data may, for example, be conditions placed by the data
20 provider on the release of the data D, these conditions being checked by the trusted authority before generation of the decryption key and/or release of the decryption key / the decrypted data.

It will be appreciated that instead of the QR IBE method, the above-described
25 embodiments can be implemented using any other suitable IBE algorithm, such as those mentioned above that use of Weil or Tate pairings, or are RSA based; analogous cryptographic algorithms can also be used.

Whilst in the foregoing example the biometric data has concerned human individuals, the
30 biometric data can alternatively be that of another type of biological organism such as a dog or horse.

Furthermore, although in the described examples the individuals have presented themselves to the trusted authority, the trusted authority or a party associated with it may be more pro-active and approach or otherwise select an individual (for example, a customs officer may select a traveller at an airport and ask to see their identity card which is a
5 memory card with biometric data).

The trusted authority may be distributed in nature having, for example, a remote station at which an individual presents themselves for biometric measurement, and a central station where biometric data is compared and decryption key generation is carried out.

10

It is possible to require the involvement of multiple trust-authority entities effectively forming a compound trust authority. This may be desirable where a single authority is not trusted to be entirely reliable. One way of achieving this would be for the data encryptor to recursively encrypt the data D, with each iteration being done using the same encryption
15 key string but the public data of a different trusted authority – the individual must then go to several trust authorities in turn to successively roll back each encryption iteration. An alternative approach is for the data provider to encrypt the data D using a public base key associated with each of the trusted authorities, decryption of the encrypted item only being possible by obtaining a decryption sub-key from the trusted delegate entity acting for each
20 trusted authority in turn. This can be expressed as:

Encryption: $\text{ciphertext} = E(K_{\text{all}}, \text{data})$

Decryption: $\text{data} = D(K_{\text{all}}, \text{ciphertext})$

where K_{all} is encryption key string related to all trusted authorities, K'_{all} is the corresponding decryption key; K'_{all} is retrieved from all decryption sub-keys. Further
25 information about how multiple trusted authorities can be used is given in:

Chen L., K. Harrison, A. Moss, N.P. Smart and D. Soldera. "Certification of public keys within an identity based system" *Proceedings of Information Security Conference 2002*, ed. A. H. Chan and V. Gligor, LNCS 2433, pages 322-333, Springer-Verlag, 2002.

30

CLAIMS

1. A security method, carried out by a trusted authority, comprising receiving biometric data of a specific individual, and using the biometric data both:
 - as a biometric reference for comparison with biometric characteristics of a subject individual to determine whether the latter is said specific individual, and
 - to generate a decryption key based on at least the biometric data and private data of the trusted authority.
2. A method according to claim 1, wherein the decryption key is made available to the subject individual only if the latter is determined by the trusted authority to be said specific individual.
3. A method according to claim 1, wherein the decryption key is used by the trusted authority to decrypt data that has been encrypted based on encryption parameters comprising public data of the trusted authority and an encryption key string formed using at least said biometric data, said public data of the trusted authority being related to its private data.
4. A method according to claim 3, wherein the decrypted data is made available to the subject individual if the latter is determined by the trusted authority to be said specific individual.
5. A method according to claim 1, wherein if the subject individual is determined by the trusted authority to be the specific individual, the decryption key is used by the trusted authority to decrypt data that has been encrypted based on encryption parameters comprising public data of the trusted authority and an encryption key string formed using at least said biometric data, said public data of the trusted authority being related to its private data.

6. A method according to claim 1, wherein the generation of the decryption key is only carried out if said subject individual is determined to be said specific individual.
7. A method according to any one of the preceding claims, wherein the subject individual
5 is a human person that has presented him/herself to the trusted authority and purports to be said specific individual.
8. A method according to any one of the preceding claims, wherein the determination of whether said subject individual is said specific individual is carried out automatically by
10 comparing features represented in the reference biometric data with features in measurement data produced by measurement of the subject individual.
9. A method according to any one of claims 1 to 7, wherein the determination of whether said subject individual is said specific individual is carried out by a human.
15
10. A method according to any one of the preceding claims, wherein the biometric data comprises image data of the face of the specific individual.
11. A method according to any one of the preceding claims, wherein the biometric data is
20 read from a memory device presented by the subject individual.
12. A method according to any one of the preceding claims, wherein the generation of the decryption key is effected in accordance with identifier-based cryptography utilising quadratic residuosity.
25
13. A method according to any one of claims 1 to 11, wherein the generation of the decryption key is effected in accordance with identifier-based cryptography utilising Weil or Tate pairings.
- 30 14. Apparatus for carrying out the method of any one of claims 1 to 13.
15. Apparatus arranged to act as a trusted authority and comprising:

an input arrangement for receiving biometric data of a specific individual;
 a biometric measurement arrangement for measuring biometric characteristics of a
 subject individual to produce biometric measurement data;
 a comparison arrangement for comparing the received biometric data of said specific
 5 individual with the biometric measurement data of said subject individual to
 determine whether the latter is said specific individual;
 a key-generation arrangement for generating a decryption key based on at least the
 biometric data and trusted-authority private data; and
 a control arrangement for ensuring that until the comparison arrangement has
 10 determined that the subject individual is said specific individual, either the key-
 generation arrangement does not generate the decryption key, or the decryption key,
 and any data decrypted using the decryption key, is not made available for use.

16. A computer program product for conditioning programmable apparatus for carrying
 15 out the method of any one of claims 1 to 13.

17. A computer program product for conditioning programmable apparatus provided with
 an input arrangement and a biometric measurement arrangement to act as a trusted
 authority that is arranged:

20 to receive biometric data of a specific individual via said input arrangement;
 to generate biometric measurement data by using said biometric measurement
 arrangement to measure biometric characteristics of a subject individual;
 to determine whether the subject individual is said specific individual by comparing the
 received biometric data of said specific individual with the biometric measurement
 25 data of said subject individual;
 to generate a decryption key based on at least the biometric data and trusted-authority
 private data; and
 to ensure that until the apparatus been determined that the subject individual is said
 specific individual, either the decryption key is not generated, or the decryption key,
 30 and any data decrypted using the decryption key, is not made available for use.

18. A data access control method comprising:

- (a) encrypting first data based on encryption parameters comprising public data of a trusted authority and an encryption key string formed using at least biometric data of a specific individual;
- (b) providing the biometric data of said specific individual to the trusted authority which
5 uses it both:
as a biometric reference for comparison with biometric characteristics of a subject individual to determine whether the latter is said specific individual, and
to generate a decryption key based on at least the biometric data and private data of the trusted authority, said public data of the trusted authority being related to its
10 private data;
- (c) using the decryption key to decrypt the encrypted first data.
19. A method according to claim 18, wherein the decryption key is only generated, or only made available for use in step (c), by the trusted authority if the subject individual is
15 determined by the trusted authority to be the specific individual.
20. A method according to claim 18, wherein in step (a) the biometric data of said specific individual is contemporaneously generated from said specific individual.
- 20 21. A method according to claim 18, wherein in step (a) the biometric data of said specific individual is generated from recorded analogue biometric data of said specific individual.
22. A method according to claim 18, wherein in step (a) biometric data of said specific individual is retrieved from digital storage.
- 25 23. A method according to claim 22, wherein the biometric data of said specific individual is retrieved from a memory device presented by said specific individual.
24. A method according to claim 18 or claim 22, wherein the biometric data of said
30 specific individual is provided to the trusted authority by being read off a memory device presented by said subject individual.

25. A method according to any one of claims 18 to 23, wherein the biometric data of said specific individual is provided to the trusted authority by transfer from an entity carrying out step (a).
- 5 26. A method according to any one of claims 18 to 25, wherein the subject individual is a human person that has presented him/herself to the trusted authority and purports to be said specific individual.
- 10 27. A method according to any one of claims 18 to 26, wherein in step (b) the determination of whether said subject individual is said specific individual is carried out automatically by comparing features represented in the reference biometric data with features in measurement data produced by measurement of the subject individual.
- 15 28. A method according to any one of claims 18 to 26, wherein in step (b) the determination of whether said subject individual is said specific individual is carried out by a human.
- 20 29. A method according to any one of claims 18 to 28, wherein step (c) is carried out by the trusted authority and the decrypted data is made available to the specific individual.
30. A method according to any one of claims 18 to 28, wherein the trusted authority provides the decryption key to said specific individual which then carries out step (c).
- 25 31. A method according to any one of claims 18 to 30, wherein the biometric data of said specific individual comprises image data of the face of the specific individual.
- 30 32. A method according to claim 18, wherein in step (a) the biometric data of said specific individual is read from a memory device of said specific individual and the encrypted first data is stored to said device, the biometric data of said specific individual being provided to the trusted authority in step (b) by being read from said memory device, and step (c) being carried by the trusted authority and only if the subject individual is determined in

step (b) to be said specific individual, the decrypted first data produced in step (c) being made available to said specific individual.

33. A method according to claim 32, wherein the first data comprises password data.

5

34. A method according to claim 18, wherein step (a) is carried out by a data provider with the biometric data of said specific individual being image data derived from a photograph of said specific individual, the biometric data of said specific individual being sent to a receiving party together with the encrypted first data for use by the trusted authority in step

10 (b).

35. A method according to claim 34, wherein the receiving party is the trusted authority.

36. A method according to claim 34, wherein the receiving party is said specific individual.

15

37. A method according to claim 18, wherein step (a) is carried out by a data provider with said biometric data of said specific individual comprising data that is the same as biometric data stored on a memory device of said specific individual as a result of having been either read from that device or provided from a common source, the said subject individual seeking to obtain the decryption key from the trusted authority by presenting a memory device to the trusted authority to enable the latter to read off biometric data stored in the device, the trusted authority providing the decryption key to the subject individual only if the latter is determined in step (b) to be said specific individual.

20
25

38. A method according to claim 37, wherein the encryption key string includes a data element known to the data provider and passed to the trusted authority, this data element being varied between iterations of steps (a) to (c).

30 39. A method according to any one of claims 18 to 38, wherein the cryptographic processes involving the encryption key string and decryption key are effected in accordance with identifier-based cryptography utilising quadratic residuosity.

40. A method according to any one of claims 18 to 38, wherein the cryptographic processes involving the encryption key string and decryption key are effected in accordance with identifier-based cryptography utilising Weil or Tate pairings.

5

41. A system for carrying out the method of any one of claims 18 to 40.

42. A data access control system comprising:

encryption apparatus for encrypting first data based on encryption parameters comprising
10 public data of a trusted authority and an encryption key string formed using at least biometric data of a specific individual;

trusted-authority apparatus comprising:

an input arrangement for receiving the biometric data of said specific individual;

a biometric measurement arrangement for measuring biometric characteristics of a
15 subject individual to produce biometric measurement data;

a comparison arrangement for comparing the received biometric data of said specific individual with the biometric measurement data of said subject individual to determine whether the latter is said specific individual;

a key-generation arrangement for generating a decryption key based on at least the
20 biometric data and trusted-authority private data; and

a control arrangement for ensuring that until the comparison arrangement has determined that the subject individual is said specific individual, either the key-generation arrangement does not generate the decryption key, or the decryption key, and any data decrypted using the decryption key, is not made available for use.

25 decryption apparatus for using the decryption key to decrypt the encrypted first data.

43. A system according to claim 42, wherein the decryption apparatus is part of the trusted-authority apparatus.

30 44. A system according to claim 42, wherein the encryption apparatus comprises an input arrangement for reading the biometric data of said specific individual from a memory device.

45. A system according to claim 42, wherein the input arrangement of the trusted authority apparatus is arranged to read the biometric data of said specific individual from a memory device presented by said subject individual.

5

46. A system according to claim 42, wherein the encryption apparatus comprises an input arrangement for reading the biometric data of said specific individual from a memory device presented by said specific individual, and an output arrangement for storing the encrypted first data in said memory device; the input arrangement of the trusted-authority apparatus being arranged to read the biometric data of said specific individual and the encrypted first data from a memory device presented by said subject individual.

10

47. A system according to claim 44, wherein the trusted-authority apparatus includes the decryption apparatus, and the input arrangement of the trusted-authority apparatus is further arranged to read the encrypted first data from the memory device presented by said subject individual.

15



Application No: GB0408908.2

Examiner: Mr Adam Tucker

Claims searched: 1-47

Date of search: 6 August 2004

Patents Act 1977: Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
A	-	WO02/073877 A2 Brandys, See in particular page 8 lines 4-31 and claims 1 & 9
A	-	US4993068 A Piosenka et al., See in particular the abstract
A	-	GB2370471 A GCHQ, See in particular the abstract
A	-	WO03/017559 A2 Stanford University, See the whole document
A	-	http://www.hpl.hp.com/techreports/2002/HPL 2002 185.pdf , AA trusted biometric system@, Chen et al., HP Labs, last modified 30 July 2002 See in particular sections 5 & 6

Categories:

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

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC^W :

G4A; H4P

Worldwide search of patent documents classified in the following areas of the IPC⁰⁷

G06F; G06K; G07F; H04L

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

WPI, EPODOC, PAJ, INSPEC and selected internet sites



Dialog®

[Home](#)

[Help](#)

[Contact Us](#)

[Logoff](#)

[Search History](#)

Save ☐ Search within these results: ☐

L1 security AND protocol AND "permission module" AND "authentication module" AND identity AND transaction AND characteristic AND compare

Enter Search Terms

[Perform New Search](#)
Choosing this option will erase previous sets.

Core FT1 (17,643) **Core FT2 (19,865)**

Records: 1 to 25 of 17,643 Page 1 [Next >>](#)

[Display Selected](#) ☒ Highlight Selected [Clear All](#) (0 of 100 selected)

☐ **Check All**

☐ [Agent technology application strategies in personal and team software process environment.](#)
Date: June 2011
 1/6,K/1 (Item 1 from file: 9)
 05172474 Supplier Number: 283706153
 Agent technology application strategies in personal and team software process environment.
 June 2011
Word Count: 2564

TEXT:
 ...by Fig. 6.
 (FIGURE 7 OMITTED)
 (FIGURE 8 OMITTED)
 Besides that, we did perform evaluation towards the system based on the functionality (suitability, accuracy and **security**) and

usability (understandability, learn ability and operability) factors.
Respondents were given a period of time to use the system and at the end, they are...

...used during all the interviews. However, separate interviews were used. Before conducting the interviews, the agent technologies were contacted to assign the responsible or grant **permission** to contact the recognized expert in the concerned area or field of activity for the topic in software development activities and described the agent technology...

...University Press, USA., ISBN-10: 9780195092691, pp: 304.

Sushil, R., K. Garg and R. Bhargava, 2008. Design, validation, simulation and parametric evaluation of a novel **protocol** for locating mobile agents in multiregion environment. J. Comput. Sci., 4: 256-271.
DOI: 10.3844/jcssp.2008.256.271

Wooldridge, M., 2009. An Introduction...

View: [HTML](#) | [PDF](#) | [Word](#)

☐ [RFAXIS CMOS RFEIC TURBO-CHARGES CHINA'S FIRST DOMESTIC WI-FI...](#)

Date: March 22, 2012

1/6,K/2 (Item 2 from file: 9)

05171917 Supplier Number: 283809462

RFAXIS CMOS RFEIC TURBO-CHARGES CHINA'S FIRST DOMESTIC WI-FI...

March 22, 2012

Word Count: 852

TEXT:

...solutions to the rapidly growing wireless communications markets. The SCI Wi-Fi chipset (including the S103 RF IC and S901 Baseband IC), and the SWM9001 **module**, are China's first domestic Wi-Fi solutions that have obtained Wi-Fi Alliance certification. SCI also owns IPs based on Chinese **WLAN Authentication** and Privacy Infrastructure (WAPI) encryption standard, and has developed flexible business models including chipset, **module** sales and IP licensing. The SWM9001 USB-based Wi-Fi **module** uses RFAxis' RFX2402 C single-chip front-end IC to achieve best-class performance in terms of operating range, data throughput and receive sensitivity. SCI...

...evaluated, the RFX2402 C stood out by a large margin, due to its simplicity, miniature size, attractive price and uncompromised performance. In fact, our SWM9001 **module** outperformed many of the top-brand Wi-Fi products of the same category available on the market today, based on independent tests at several third...

View: [HTML](#) | [PDF](#) | [Word](#)

☐ [Multilateral environmental agreements versus world trade organization system: a comprehensive study.](#)

Date: September 2009

1/6,K/3 (Item 3 from file: 9)

05163982 Supplier Number: 283456855

Multilateral environmental agreements versus world trade organization system: a comprehensive study.

September 2009

Word Count: 3530

ABSTRACT:

...Settlement Body (DSB) of the WTO. The study would discuss the scope of the core Environmental Conventions and related International Agreements taken like the Kyoto **Protocol**, Montreal **Protocol**, Basel Convention, CITES, ILOCAT and the trade resolutions taken by different states under them, domestically and internationally to regulate and monitor trade practices accordingly. Conclusion...

TEXT:

...of the United Nations, and some are stand-alone agreements. There is no umbrella organization for MEAs.

Some of the major MEAs are: The Montreal **Protocol** requires parties to exercise control over trade by providing for a variety of trade restrictions including voluntary industry agreements, product labeling requirements, requirements for import...

...exported to States not party to the convention unless, the State is a party to any other agreement bilateral, regional or multilateral; and the Kyoto **Protocol** potentially might lead to similar policy measures affecting trade. It lists a wide range of potential areas for action, including energy efficiency, renewable energy resources...

...effective re-regulation of international trade and also provide the easiest way to distinguish between legal and illegal products. MEA notification procedures (basel convention, montreal **protocol**) have also been submitted to committees of WTO for providing greater co-ordination between the WTO rules and MEAs. These trade restrictions also help countries which lack the regulatory or institutional capacity to control the products in question, to ban or restrict trade in products which are not granted **permission** for export or import (3). Finally, the impact of MEAs both in terms of implementation of the plan and the trade forgone as its result...

...in the amount, and type, of trade measures being developed in MEAs which include trade restrictions on specific items, labeling requirements for e.g., Biosafety **Protocol**, and in the possibility of development of rules relating to intellectual property rights in the Convention on Biological Diversity.

Also, there is the evident reluctance of US to join MEAs, including those with trade measures (The US decision to abandon the Kyoto **Protocol** in 2001 to the United Nations Framework Convention on Climate Change encapsulates an alarming trend in American attitude toward the environmental agreements). This unilateralist tendency...

...final and without appeal. In case if one of the states involved fails to comply with it, the other party may have recourse to the **Security** Council of the United Nations. The ICJ has also the advantage of having an environmental chamber with a procedure similar to the general submission procedures...

View: [HTML](#) | [PDF](#) | [Word](#)

- ☐ [F5 Accelerates Its Wireless Push Next Stage Of Growth Acquisition of Traffix is F5's first in wireless gear field; aims at 4G.](#)

Date: March 16, 2012

1/6,K/4 (Item 4 from file: 9)

05163752 Supplier Number: 283087869

F5 Accelerates Its Wireless Push Next Stage Of Growth Acquisition of Traffix is F5's first in wireless gear field; aims at 4G.

March 16, 2012

Word Count: 627

TEXT:

...analyst Troy Jensen. When cellphone users try to access websites or data products, F5's gear sends the user's requests to servers that grant **permission** or block services.

F5 aims to have a big role in "optimizing" the flow of voice and data services over fourth-generation networks using LTE...

...the market."

Deutsche Bank analyst Brian Modoff estimates F5 paid about \$130 million for Traffix. The Tel Aviv, Israel-based company developed an Internet signaling **protocol** that's popular among wireless firms in 4G networks. It helps them operate and manage their networks.

In a report, analyst Modoff says the Traffix...

...one Traffix customer.

Besides technology it gets from Traffix, F5 is developing technology to help wireless firms inspect packets of mobile data for routing and **security**. F5's new "deep packet inspection" technology, which will compete with products from Allot and Procera Networks ((STOCK(PKT))), should be ready for commercial release...

...analysts say there could be more coming.

Yet, Jensen says F5 won't forget about its core data center market, which includes firewall and other **security** products. He suggests F5 could take a run at firewall firm Palo Alto Networks. "Near term, I wouldn't be surprised if they did more **security** acquisitions," Jensen said. "Palo Alto Networks is growing like a weed."

View: [HTML](#) | [PDF](#) | [Word](#)

☐ Obama's political pal is now Inmate No. 40892-424.

Date: March 16, 2012

1/6,K/5 (Item 5 from file: 9)

05163732 Supplier Number: 283205246

Obama's political pal is now Inmate No. 40892-424.

March 16, 2012

Word Count: 743

TEXT:

...come across as a beguiling rogue, good-naturedly absorbing jokes about his mop of hair and always maintaining his innocence.

The feds delayed the minimum **security** imprisonment 90 days so Blago could help prepare an appeal. But early Thursday in his Chicago home the impeached governor said goodbye to his wife...

...Hare Airport and had his last double patty melt in freedom until 2026.
(He didn't finish it.)

At the prison, which may be low **security** but is still surrounded by razor wire, Blagojevich went through a standard four-hour entrance procedure, including a psychiatric evaluation, a body cavity strip search

...

...offenses along with a few murderers and Jeffrey Skilling of Enron CEO infamy doing his 24 years. To avoid trouble, Blagojevich should quickly learn inmate **protocol**: no staring at anyone, lay low, be quiet, ask **permission** before joining other inmates at a cafeteria table.

The former governor will live in a cell the size of a walk-in closet with three...

View: [HTML](#) | [PDF](#) | [Word](#)

☐ TOYOTA MOTOR CORPORATION JOINS TRUSTED COMPUTING GROUP (TCG).

Date: March 16, 2012

1/6,K/6 (Item 6 from file: 9)

05162926 Supplier Number: 283127483

TOYOTA MOTOR CORPORATION JOINS TRUSTED COMPUTING GROUP (TCG).

March 16, 2012

Word Count: 554

TEXT:

...been working to prevent incidental and malicious attacks, as well as prevent unauthorized access to related systems.

TCG's efforts will address: Establishing a secure **authentication** method for accessing the systems Ensuring consistency of data and system Protecting stored information TCG has already developed and published many technologies specifications based on the root-of-trust concept, such as Trusted Platform **Module** (TPM), Self-Encrypting Drives (SEDs) and Trusted Network Connect (TNC).

TCG established the Embedded Systems Work Group in 2011, and the work group is in...

View: [HTML](#) | [PDF](#) | [Word](#)

☐ Good Technology to Deliver Military Grade Secure Android.

Date: February 01, 2012

1/6,K/7 (Item 7 from file: 9)

05157078 Supplier Number: 282370536

Good Technology to Deliver Military Grade Secure Android.

February 01, 2012

Word Count: 1087

TEXT:

...Exchange servers located in DoD data centers via Good's email application to end-point Android devices wirelessly, using a FIPS 140-2

validated cryptographic **module** with AES encryption to ensure data protection for data-at-rest as well as data-in-transit. Good's patented container-based technology prevents data...

...power to do more.

For more information, visit www.dell.com. Biometric Associates, LP
Biometric Associates, LP is a unique developer, manufacturer, and integrator of **authentication** and identity systems. Products include smart card middleware for mobile operating systems and Bluetooth smart card readers and headsets specifically designed to provide military-grade...

View: [HTML](#) | [PDF](#) | [Word](#)

☐ Unbreakable SCADA security essential for pipelines.

Date: February 2012

1/6,K/8 (Item 8 from file: 9)

05150578 Supplier Number: 281461400

Unbreakable SCADA security essential for pipelines.

February 2012

Word Count: 2165

TEXT:

...developed by Innominate Security Technologies. The system was specifically designed for harsh environments and includes small, economical, industrial-rated modules that incorporate router, firewall, encryption, **authentication** and other functions that can be installed without disturbing production.

An FL mGuard creates secure data communication via Virtual Private Network tunnels (VPN). VPN provides...

...S. government and others.

Communication with control devices is only allowed from designated locations via unbreakable software security keys (imagine a password on steroids), and **authentication** via certificates of authority that verify the communication origin is from specific command-and-control individuals at specific workstations. The mGuard device filters all outgoing...

...handshake protocols will be intercepted and discarded. This highly secure method blocks hacking, virus transmission, and unauthorized access to data streams of information because the **module** screens and rejects any unauthorized packets, including malware and hacker probes.

(FIGURE 2 OMITTED)

In "Stealth Mode" these products are completely transparent, invisible while automatically...

...in hacker software. Yet even the best, brand new, fully featured, most expensive PLC on the market does not offer simple source verification and data **authentication**, or encryption of commands or data traffic. If all this does not yet make you nervous, consider the consequences if some disgruntled nutjob deliberately triggers...

View: [HTML](#) | [PDF](#) | [Word](#)

☐ [Regional News - North America.](#)

Date: January 02, 2012

1/6,K/9 (Item 9 from file: 9)

05144210 Supplier Number: 280905540

Regional News - North America.

January 02, 2012

Word Count: 72605

TEXT:

...2011

Bill would require found change to fund nonprofit instead of TSA Rep. Jeff Miller, R-Fla., has proposed legislation that would require the Transportation **Security** Administration to give change left in **security** checkpoint trays by travelers to a nonprofit organization. Under the proposal, the money would go to the USO, a nonprofit, congressionally chartered private organization with...

...in the first 50 weeks of 2011 compared with the same period last year.
Dec 29, 2011

Wi-Fi Protected Setup is said to have **security** flaw The U.S. Computer Emergency Readiness Team is warning that the Wi-Fi Protected Setup **protocol** used in wireless home routers may be exploited by hackers, citing **security** researcher Stefan Viehbock. The **security** flaw is in a program found on most commercially available routers. Dec 29, 2011

More insurers offer coverage for post-breach cleanup More companies are...

...groups are voicing increasing frustration with TSA passenger screening procedures, charging that longer delays, reduced privacy and embarrassing pat-downs have done little to increase **security** for the flying public. "The system is broken, it's extremely flawed and it's absurd that we all sit back and say we can't do anything about it," says Geoff Freeman of the U.S. Travel Association, which fears people will eventually stop flying rather than face the **security** gauntlet. Dec 28, 2011
Recycling is for socialists, say tea party activists. Members of Arizona's tea party have a new post-election target: curbside...

...are "floating test beds." However, Navy officials defend the destroyer as "fully operational worldwide." Dec 28, 2011

TSA gives screeners collective bargaining rights The Transportation **Security** Administration's 40,000 screeners now have the right to vote on collective bargaining rights. The TSA's decision to give the workers the rights...

...and some other employment issues. Strikes are not permitted. "The safety of the traveling public is our top priority, and we will not negotiate on **security**," said TSA Administrator John Pistole. "But morale and employee engagement cannot be separated from achieving superior **security**." Dec 28, 2011

TSA suspends worker who failed to screen checked bags The Transportation **Security** Administration has suspended an employee at Newark

Liberty International Airport for failing to screen checked bags. The bags were sent on to be loaded on...

...called a passive optical diode holds promise for quicker and more secure information processing, according to the researchers developing the technology. The devices could increase **security** and eliminate supercomputer challenges tied to bandwidth. Dec 28, 2011

Water crisis affects 39% of world's businesses. At least 39% of the world's ...

...Israel to the U.S. in 1977. Dec 27, 2011

Some health officials continue to criticize TSA scanners Experts continue to raise questions about Transportation **Security** Administration scanners that use back-scatter technology. Dr. Edward Dauer, head of radiology at Florida Medical Center, said the scanners emit radiation and could pose...

...said. "This is an additional exposure." The scanners are installed at 40 U.S. airports, and the TSA says they are safe. "The safety and **security** of the traveling public is TSA's No. 1 priority, and TSA would not use technology that could jeopardize the health of passengers or our...

...false-alarm rate France and Germany have decided not to order millimeter-wave scanners because the devices have a high false-alarm rate. The Transportation **Security** Administration currently uses the scanners, which some experts consider safer than scanners that emit radiation. However, in Germany, the scanners had a false positive rate of 54%. The TSA says the scanners currently meet its standards. Dec 27, 2011

U.S. should focus **security** strategy on thwarting plots, expert says **Security** expert Bruce Schneier says the only useful aviation **security** measures taken since 9/11 are locking and reinforcing cockpit doors, teaching travelers to fight back and positive bag matching. "The rest is **security** theater," he said. Schneier said the government should focus on terrorists who are planning plots. Dec 27, 2011

TSA adds subways, ferries to **security** scope The Transportation **Security** Administration has expanded its search and screening operations to include subways, ferry terminals, train stations and other mass-transit venues in the U.S. The...could provide a quarter of a million people with clean, cheap energy, according to this article. Free Flow Power of Gloucester, Mass., has won federal **permission** to begin exploratory work that could lead to the installation of tens of thousands of turbines beneath the surface of the Mississippi. There are big...

...officials say they expect the technique to cost 80% less than conventional post-combustion methods of sequestration. Dec 26, 2011

TSA screening increases risk of **security** breaches. A "one-size-fits-all" approach to **security** screening is unlikely to prevent a future terror attack and may even "invite disaster," The Washington Times editorial board writes. The board criticized recent efforts by the Transportation **Security** Administration to boost **security** after the foiled air cargo bomb plot. It also noted that government screening requires more resources and spending than screening conducted by airlines. Dec 26, 2011

Flight attendants criticize TSA screening techniques. A group of flight attendants has joined pilots in criticizing the Transportation **Security** Administration's new **security** techniques and set Nov. 24, one of the busiest travel days of the year, as a "pat-down opt-out day." Some pilots have criticized...

...air carriers have the information needed to hire qualified pilots," the report said. Dec 23, 2011

TSA launches help line for disabled travelers The Transportation **Security** Administration has launched a help line aimed at assisting travelers with disabilities and special medical needs go through the airport-screening process. The TSA recommends...

...9 a.m. to 9 p.m. ET, 72 hours before traveling. The number is (855) 787-2227. Dec 23, 2011

Chattanooga Airport gets new **security** scanner Tennessee's Chattanooga Airport recently received a full-body scanner that displays generic images instead of detailed images of travelers' bodies. The scanner, which...

...that we're looking out for their interest, trying to make it the best experience as we can and at the same time adhering to **security** principles that we should have in place," said Steve Wood, federal **security** director for TSA in East Tennessee. Dec 23, 2011

AAR reports strong gains in traffic, intermodal levels U.S. rail shipments during the week ending...

...expect that," said Mark Bergsrud, senior vice president of marketing at United Continental. Dec 22, 2011

TSA tests scanning equipment at California airport The Transportation **Security** Administration is testing scanning equipment at California's Monterey Regional Airport as part of a plan to speed **security** screening for members of the military. Military members are asked to present their identification for scanning by the machines. "This location will be used in...

...chosen for testing because of the large numbers of military personnel who use it. Dec 22, 2011

Jam, cranberry sauce won't make it through **security**, TSA says Travelers should think twice about trying to carry certain holiday goodies through airport **security**. Earlier this month, TSA agents at Denver International Airport refused to let Kathleen Triou take homemade raspberry jam through a **security** checkpoint. "It was jam. Just homemade jam in a tiny mason jar," said Triou. "They said it has the potential to be bomb material." Jams...

...also will ask airlines to identify diversion airports. The goal is to avoid prolonged weather delays. Dec 21, 2011

Airlines, experts push for streamlining aviation **security** Congress is expected to approve a bill this week to expedite **security** screening for military personnel. "U.S. service members are entrusted to protect citizens with their lives and as such, TSA is recognizing that these members pose very little risk to **security**," said John Pistole, administrator of the Transportation **Security** Administration. A group that represents international airlines predicts that the future of aviation

security will include a tunnel capable of screening travelers for banned items. The Transportation **Security** Administration is moving toward more risk-based projects, such as its PreCheck program, which allows prescreened frequent fliers to move more quickly through **security**. Dec 21, 2011

House GOP targets MACT as part of payroll tax bill Republicans in the U.S. House of Representatives are looking to postpone...

...for the aerospace industry. "The fact that our industry is a leading job creator, a technological innovator and a critical part of our nation's **security** is too important to be taken for granted," said AIA President and CEO Marion C. Blakey. "If this industry stops being Second to None, the...

...in a far less intrusive way," said Cameron Humphres, the airport's director. "I appreciate that. I think passengers appreciate it as well." The Transportation **Security** Administration has installed 540 scanners at more than 100 airports in the U.S. Dec 19, 2011

Column: Order suggests TSA is moving away from X-ray scanners The Transportation **Security** Administration recently ordered more than 300 millimeter-wave body scanners, writes Tony Bizjak in the Sacramento Bee. The order suggests that the TSA is moving...

...about all cancellations or delays of more than 30 minutes. Dec 19, 2011
TSA fires four Charlotte agents for failing to screen bags The Transportation **Security** Administration on Friday terminated four agents at Charlotte/Douglas International Airport in North Carolina for failing to properly screen travelers' luggage. Officials said 12 more...

...80 bags out of 80,000 were not opened and screened by hand. Dec 19, 2011

TSA chief supports expanding passenger-advocate program The Transportation **Security** Administration hopes to expand its advocate program to more airports next year, Administrator John Pistole said. It already has advocates at some large U.S...

Company Names: ...UNITED STATES TRANSPORTATION **SECURITY** ADMINISTRATION...

Industry Names:

View: [HTML](#) | [PDF](#) | [Word](#)

☐ MINIATURE M2M MODULE BY CINTERION ENABLES LINYANG ELECTRONICS...

Date: February 15, 2012

1/6,K/10 (Item 10 from file: 9)

05134348 Supplier Number: 280070152

MINIATURE M2M **MODULE** BY CINTERION ENABLES LINYANG ELECTRONICS...

February 15, 2012

Word Count: 1043

MINIATURE M2M **MODULE** BY CINTERION ENABLES LINYANG ELECTRONICS...

(

TEXT:

(Full text of a statement. Contact details below.)

(BW)(CINTERION)(GTO.BOURSE) Miniature M2M **Module** by Cinterion
Enables Linyang Electronics Smart Meters and Power Management Solutions

High-Tech Writers/Energy Writers

MUNICH--(BUSINESS WIRE) - Feb. 15, 2012-- Cinterion, the global...

Linyang Electronics is a top 100 electronic information enterprise in China and one of the most competitive in the smart metering industry.

Cinterion's **module** provides secure wireless data communications for a range of Linyang products and services including load monitoring and control. These services help power companies and consumers...

...devices, and managed services to wireless operators, banks, enterprises and government agencies.

Gemalto is the world leader for electronic passports and identity cards, two-factor **authentication** devices for online protection, smart credit/debit and contactless payment cards, as well as subscriber identification modules (SIM) and universal integrated circuit cards (UICC) in...

View: [HTML](#) | [PDF](#) | [Word](#)

- ☐ Overview of McAfee real-time database monitoring, auditing, and intrusion prevention: databases are repositories of the most valuable information assets in the enterprise. And yet, in many organizations today, they are poorly protected.

Date: November 2011

1/6,K/11 (Item 11 from file: 9)

05131236 Supplier Number: 279391505

Overview of McAfee real-time database monitoring, auditing, and intrusion prevention: databases are repositories of the most valuable information assets in the enterprise. And yet, in many organizations today, they are poorly protected.

November 2011

Word Count: 1108

TEXT:

...to achieve adequate security. Following is a brief overview of existing categories of tools that can be found in use across enterprises large and small.

Authentication and access control

* Pros--Establishes roles and privileges, the most basic level of security

* Cons--Difficult to enforce properly, over-liberal granting of access, privilege...

...traffic only. Some agents can also monitor IPC communications, but they suffer from being even more intrusive since they must be implemented as a kernel **module**, making them hard to install and maintain. To truly monitor the database, it is not enough to capture network traffic, even if you are able...

View: [HTML](#) | [PDF](#) | [Word](#)

- ☐ NCR Reports 4Q Results.

Date: February 09, 2012

1/6,K/12 (Item 12 from file: 9)
05130256 Supplier Number: 279412723
NCR Reports 4Q Results.

February 09, 2012
Word Count: 2433

TEXT:

...ATMs with one of NCR's SelfServ 32, 34, or 38 models. All of the new NCR SelfServ ATMs will include NCR's Scalable Deposit **Module** (SDM) technology. SDM is the only technology on the market that allows consumers to deposit both cash and checks simultaneously in any orientation through a...

...service mobile website that will allow travelers to reserve and purchase tickets, update reservation details and inquire about flight schedule.

In addition, NCR's Credential **Authentication** Technology - Boarding Pass Scanning System was selected by the U.S. Transportation Security Administration for use in a pilot program that aims to automatically verify...

View: [HTML](#) | [PDF](#) | [Word](#)

☐ CINTERION RECEIVES 2011 SMART GRID EXCELLENCE AWARD.

Date: January 11, 2012

1/6,K/13 (Item 13 from file: 9)
05108753 Supplier Number: 276782821
CINTERION RECEIVES 2011 SMART GRID EXCELLENCE AWARD.

January 11, 2012
Word Count: 1062

TEXT:

(Full text of a statement. Contact details below.)

(BW)(CINTERION)(GTO.BOURSE) Cinterion Receives 2011 Smart Grid Excellence Award

- Innovative M2M **Module** Honored for Exceptional Innovation

High-Tech Editors/Technology Editors

MUNICH--(BUSINESS WIRE) - Jan. 10, 2012-- Cinterion, the global leader in cellular machine-to-machine (M2M) communication and a Gemalto company (Euronext NL0000400653 GTO), today announced that its EU3 M2M **module** won a 2011 Smart Grid Excellence Award from SmartGrid.TMCnet.com.

...challenges and long-life requirements of global smart grid and automatic meter reading (AMR) applications. By enabling UMTS capabilities on the 900 MHz band, the **module** offers increased coverage area for high-speed communications even in very remote locations, which is essential for geographically diverse smart metering applications. In addition, EU3...

...devices, and managed services to wireless operators, banks, enterprises and government agencies.

Gemalto is the world leader for electronic passports and identity cards, two-factor **authentication** devices for online protection, smart credit/debit and contactless payment cards, as well as subscriber identification modules (SIM) and universal integrated circuit cards (UICC) in...

View: [HTML](#) | [PDF](#) | [Word](#)

☐ Where to Start? With the New Year, Regulatory 'To-do Lists' Just Keep on Growing.

Date: January 01, 2012

1/6,K/14 (Item 14 from file: 9)

05104960 Supplier Number: 276204131

Where to Start? With the New Year, Regulatory 'To-do Lists' Just Keep on Growing.

January 01, 2012

Word Count: 5432

TEXT:

...McMillan cites eight discrete security requirements under MU that must be present in a certified EHR. These include audit controls, encryption controls, emergency access provisions, **authentication** provisions, and accounting for disclosure capability. "The Stage 1 meaningful use requirement, that you conduct a risk assessment in accordance with the original HIPAA rule...of electronic order entry. But other areas lagged, such as electronically documenting the problem list, and fewer than 10 percent of physicians even used the **module** .

The stakes were high, as losing its Joint Commission accreditation-which could happen if the facility could not demonstrate improvement- would block the facility from...

View: [HTML](#) | [PDF](#) | [Word](#)

☐ Lessons for Germany's gendiagnostikgesetz from Europe's **protocol** on genetic testing for health purposes.

Date: March 2011

1/6,K/15 (Item 15 from file: 9)

05104803 Supplier Number: 275128853

Lessons for Germany's gendiagnostikgesetz from Europe's **protocol** on genetic testing for health purposes.

March 2011

Word Count: 13554

Lessons for Germany's gendiagnostikgesetz from Europe's **protocol** on genetic testing for health purposes.
(

TEXT:

This Note argues that, in some important respects, the German GenDG and, in fewer respects, the Council of Europe's conceptually similar Additional **Protocol** to the Convention on Human Rights and Biomedicine, Concerning Genetic Testing for Health Purposes, also called the **Protocol** on Genetic Testing for Health Purposes (" **Protocol**"), (9) do not provide the level of understanding and specificity necessary to provide equity to all parties in situations where its edicts apply.

Part I of this Note summarizes and emphasizes major aspects of the GenDG and the **Protocol**. Part II addresses the right to know and home genetic testing kits, issues for which the **Protocol** provides the best alternative with specific exceptions and more flexibility. In Part III, this Note acknowledges that the **Protocol** provides a better alternative on issues of consent, particularly in situations of lack of capacity to consent, improper refusal to consent, and balancing of interests in paternity testing, but examines ways that both laws could better address the issue.

I. THE GENDIAGNOSTIKGESETZ AND THE COUNCIL OF EUROPE'S **PROTOCOL** ON GENETIC TESTING FOR HEALTH PURPOSES

A. The Gendiagnostikgesetz Discrimination, Accreditation, and Test Results
The GenDG prohibits discrimination based on "genetic characteristics." (10) Its rigorous...

...Act. (36) While several groups are represented on the commission's panel, insurer and employer interests are not. (37)

D. The Council of Europe's **Protocol** on Genetic Testing for Health Purposes

In 1996, the Committee of Ministers of the Council of Europe instructed the Steering Committee on Bioethics to draw up a **protocol** (38) to the Convention on Human Rights and Biomedicine. (39) The Convention entered into force on December 1, 1999, (40) and has been signed by thirty-five states, twenty-eight of which have further ratified or acceded to it. (41) Yet the **Protocol** to the Convention, which opened for signatures on November 27, 2008, has not yet obtained the five ratifications--including those of four Council of Europe states--necessary for entry into force. (42) Rather, the **Protocol** has been signed by five states, two of which have ratified it. (43) Germany has not signed or ratified either the Convention or the **Protocol**, (44) although a German doctor chairs the Council of Europe's Working Party on Human Genetics. (45) While the **Protocol** is not binding on Germany as a non-party, this Note examines its importance as an instructive guide for the German Act.

E. Scope of the **Protocol**

The **Protocol** does not apply to genetic tests carried out on the human embryo or fetus, or to genetic tests carried out for research purposes. (46) It...

...50) and it directs that appropriate measures be taken (51) "to prevent stigmatization of persons or groups in relation to genetic characteristics." (52)

Under the **Protocol**, all genetic tests must meet quality assurance requirements in programs, monitoring, and qualifications of persons providing the genetic services. (53) The tests must also have...

...and only subsequent to an independent evaluation of ethical acceptability. (61) Such screenings must also meet further specific conditions. (62) And unlike the GenDG, the **Protocol** requires that governments facilitate public access to "objective general information on genetic tests, including their nature and the potential implications of their results." (63)

II. LESSONS FOR THE GENDIAGNOSTIKGESETZ FROM THE **PROTOCOL**

A. Right Not to Know

Under the GenDG, pre-test consent must be obtained as to "if, and if so to which extent, the examination results may be disclosed." (64) Assumedly, this disclosure would include disclosure to the test subject himself. (65) This stands in contrast to the **Protocol**, which simply states that "(e)veryone undergoing a genetic test is entitled to know any information collected about his or her health derived from this...

...the absence of consent would be opposite in each situation: in Germany, no disclosure to anyone including even the test subject himself, and under the **Protocol**, disclosure to the subject. Thus, the GenDG assumes the subject does not want to know, and the **Protocol** assumes the subject does.

The GenDG sets the right not to know test results above the right to know them. While the right to know...

...not to know is explicitly laid out in Section 9. (67) Furthermore, the right not to know is not qualified in any way. (68) The **Protocol**, in contrast, provides that "(t)he wish of a person not to be informed shall be respected," (69) but also states that, "(i)n exceptional...

...care, stated in Article 4 of the Convention on Human Rights and Biomedicine, might conflict with the patient's right not to know." (71) The **Protocol** then introduces the duty of care as a factor to be balanced, and the doctor must determine in her own expertise whether this duty outweighs the right not to know. (72)

The **Protocol** makes room for situations in which information about preventable diseases is made known to the unwilling subject, while the GenDG makes no such allowance. Yet...

...s interest in avoiding a life-altering of fatal disease (75) should override his uninformed interest in remaining ignorant of information. In this regard, the **Protocol** presents the best approach in its allowance of exceptions to the right not to know. It must also be remembered that because the **Protocol** allows for national laws to prevent the doctor from making such an exception, Germany would still be able to sign on to the **Protocol** and retain its current policy on the right to know. (76)

B. Exception to the Medical Supervision Requirement

Both the GenDG and the **Protocol** contain a general requirement of either supervision or direct administering of genetic testing by a medical doctor. (77) Yet the **Protocol** allows for an exception to this requirement. (78) The **Protocol** somewhat cryptically states: "Exceptions to the general rule ... may be allowed by a Party, subject to appropriate measures being provided, taking into account the way the test will be carried out, to give effect to the other provisions of this **Protocol**," and goes on to state that "such an exception may not be made with regard to genetic tests with important implications for the health of the persons concerned or members of their family or with important implications concerning procreation choices." (79) The "other provisions of this **Protocol**" mentioned are "the provisions concerning the nature and quality of prior information, free and informed consent and genetic counseling" (80) Yet it remains unclear what would qualify as "important implications" of "appropriate measures."

The Explanatory Report to the **Protocol** clarifies that home

genetic test kits, also called direct-to-consumer (DTC) tests, in which the consumer can both administer and analyze the test, are perfectly acceptable. (81) This is true at least in situations as dictated by a state Party to the **Protocol** (82) according to the following factors: the potential implications for the test subject and his family; the ease of interpretation of the results; treatment possibilities...

...ensure that consumers will, in reality, always follow all directions, the severity of the potential problems of misuse and misinterpretation are greatly alleviated by the **Protocol's** requirement that only less significant tests and those which are easy to interpret are allowed in DTC kits. (93) Yet commentators have also objected to the general idea of DTC kits because such kits cannot require informed consent. (94) The **Protocol** also specifically addresses this problem by recognizing the ability of the consumer to make an informed decision as an important concern in determining whether DTC kits should be allowed. (95) Overall, then, the **Protocol** provides specific guidelines that make for a workable system governing direct-to-consumer genetic kits.

III. LESSONS FOR THE GENDIAGNOSTIKGESETZ AND THE **PROTOCOL**

A. Persons Lacking the Capacity to Consent

In the case of a genetic test on a subject lacking capacity to consent, the GenDG provides first...

...regard to a genetically related person," there is no other way to determine whether the offspring will have a genetic illness or condition. (97)

The **Protocol**, on the other hand, deviates from its base treaty, the Convention on Human Rights and Biomedicine, (98) by allowing "a genetic test to be carried...

...as important for their health, or to allow them to make an informed choice with respect to procreation." (99)

As opposed to the GenDG, the **Protocol** allows testing for the benefit of family members, not just their unborn offspring, in the case of a subject lacking capacity to consent. The Explanatory Report to the **Protocol** identifies a situation in which testing for the benefit of living family members would be vital: "(A) person not able to consent (who is) suffering...

...the relatives is not outweighed by an attendant benefit to the test subject. (102)

B. Impossibility of Obtaining Consent from Subject, and Deceased Subjects

The **Protocol** provides:

When it is not possible, with reasonable efforts, (103) to contact a person for a genetic test for the benefit of his or her...

...out in accordance with the principle of proportionality, where the expected benefit cannot be otherwise obtained and where the test cannot be deferred. (104) The **Protocol** also states that provisions shall be made for the subject when he expressly opposes the genetic test. (105)

The GenDG provides no exception to the...

...in the case of a deceased or impossible-to-find subject. (106) This means that in the situation (provided in the Explanatory Report to the **Protocol**) of a family with a history of ovarian cancer where the genetic mutation had not been identified, the use of the subject's genetic information...

...defies reason and is easily avoidable. (109)

Similar to the exception for genetic impossibility of subject contact is the exception for deceased subjects under the **Protocol**. (110) The only major difference here is that the **Protocol** requires, in the case of a deceased subject, that "the consent or authorization required by law has been obtained." (111) The GenDG specifies nothing in...

...situations seem to be left with no recourse to gain access to it if the deceased gave no express, written consent before he passed.

The **Protocol** allows no exception to the consent requirement when fully informed consent is obtainable. (113) Family disclosure over the objections or absent the consent of the...
...wishing to be the bearer of bad news, the unsure nature of the specific genetic test, or even spite. (120) Under both the GenDG and **Protocol**, the test subject with capacity and ability to consent to disclosure of genetic information always has the last word, and no reasons for withholding consent...

...principles of ethics' (that) have significantly influenced much of Western thinking and action, particularly in the medical-legal sphere." (123) While the GenDG and the **Protocol** arguably increase patient autonomy, a family member's autonomy is likely decreased when she is being barred access to genetic information. (124) Beneficence, nonmaleficence, and...

...someone seeking such consent."

C. Secret Paternity Testing

On the subject of consent and descent determination through secret paternity tests, both the GenDG and the **Protocol** take the same stance--all such genetic tests require free and informed consent of the test subject. (125) Yet a previous case from the European...Mikulic's recognition of that interest as an important factor to be balanced against the possible father's privacy interest seems more reasonable than the **Protocol** and the GenDG in their blanket prohibition on paternity testing without consent. (133) Such an identity interest of the possible offspring could be limited and...

...her to remain without knowledge of her father. (134)

CONCLUSION

The strict consent requirement of the GenDG, and even the looser consent requirement of the **Protocol**, could often leave families scrambling to find answers that are easily accessible through other family members' genetic tests, including information about possible future health problems and paternity. In regard to the right not to know and direct-to-consumer genetic tests, the **Protocol** hits the mark by allowing for health interest exceptions in the former case and limited

exceptions creating greater accessibility to non-crucial genetic information in the latter. The difficulties for the GenDG, and sometimes the **Protocol**, come in areas where it seems the legislators did not consider individual situations in which it may be inequitable to the test subject or his...

...GINA U.S. laws affecting genetic information in multiple contexts, such as the Americans with Disabilities Act, the Civil Rights Act, the Employee Retirement Income **Security** Act, the Health Insurance Portability and Accountability Act. See Janneke H. Gerards, Regulation of Genetic Information in the United States, in GENETIC INFORMATION AND GENETIC...

...Genetic Exceptionalism" in Medicine: Clarifying the Differences between Genetic and Nongenetic Tests, 138 ANNALS OF INTERNAL MED. 571, 571 (2003).

(9.) Council of Europe, Additional **Protocol** to the Convention on Human Rights and Biomedicine concerning Genetic Testing for Health Purposes, C.E.T.S. No. 203 (2008), available at <http://conventions.coe.int/treaty/Commun/ChercheSig.asp?NT=203&CM=8&DF=30/10/2009&CL=ENG> (hereinafter "**Protocol**").

(10.) GenDG (section) 4(1). Genetic characteristics are defined as "human genetic information inherited upon fertilisation or otherwise gained before birth." GenDG (section) 3(4...

...and if so to which extent, the examination results may be disclosed of, as the case may be, destroyed." The section then provides that subject **permission** may be revoked at any time, orally or in writing, and such revocation must be immediately documented and reported. GenDG (section) 8(2).

(14.) Id..
...the Genetic Diagnostic Commission created by this Act. Id.

(31.) Id. (section) 18. This context is not specifically mentioned in the Council of Europe's **Protocol** on the subject. In the insurance setting, the law bans third parties from obtaining any kind of genetic information, except in cases where the contract at issue exceeds 300,000 euros. As the implications of the differences between the German law and the **Protocol** are vast and this particular field much-analyzed, this difference will not be discussed in this Note. Id.; see, e.g. Ashley M. Ellis, Genetic...

...and Insurance, 36 TULSA L.J. 703 (2001).

(32.) GenDG (section) 19. This context is also not specifically mentioned in the Council of Europe's **Protocol**. Genetic privacy in employment has been heavily explored in previous works, and therefore will not be discussed in this Note. See, e.g., Ellis, supra...

...int/treaty/Commun/ListeTraites.asp?CM=8&CL=ENG (last visited Sept. 19, 2009).

(41.) Convention on Human Rights and Biomedicine, supra note 39.

(42.) **Protocol**, supra note 9.

(43.) Id.

(44.) Convention on Human Rights and Biomedicine, supra note 41; **Protocol**, supra note 9. While it follows that if a country did

not sign the Convention, it would not sign the **Protocol** to the Convention, it is unclear why Germany has not signed the Convention. The Bundesministerium der Justiz (the Federal Ministry of Justice) simply states on...19y.html (last visited Feb. 8, 2010).

(45.) Additional **Protocol** to the Convention on Human Rights and Biomedicine, concerning Genetic Testing for Health Purposes: Explanatory Report, Introduction art. 8, available at <http://conventions.coe.int/Treaty/EN/Reports/Html/203.htm> (last visited Sept. 23, 2010) (hereinafter "Explanatory Report").

(46.) **Protocol**, supra note 9, art. 2(2). The purpose for the exclusion from the **Protocol** of testing for research or on an embryo or fetus is not clear.

(47.) **Protocol**, supra note 9, art. 3. This requirement remains somewhat nebulous, even in view of its limited discussion in the Explanatory Report. Explanatory Report, supra note 45, (paragraph) (paragraph) 37-38 ("This article affirms the primacy of the human being concerned by genetic tests covered by the **Protocol** over the sole interest of society of science.... The aim of (the **Protocol**) is to protect human rights and dignity.").

(48.) The Explanatory Report specifically states: "Yet not all differences in treatment necessarily amount to discrimination. In particular...

...on account of his or her genetic characteristics or the genetic characteristics of a genetically related person.... " GenDG (section) 4(1) (emphasis added). In the **Protocol**, the emphasis is on discrimination against the person "either as an individual or as a member of a group on grounds of his or her genetic heritage.... "

Protocol, supra note 9, art. 4(1) (emphasis added). The effect of these two statements could be different. For example, a person who is discriminated against because his brother has a genetic condition would be covered under the German law, but might not be covered under the **Protocol** because it is not his "genetic heritage" that is the basis for the discrimination, but rather that of his brother's. See infra note 50 for the definition of "genetic heritage". Yet if this interpretation were correct, it would seem to take away the meaning of the phrase in the **Protocol** "or as a member of a group"--if one can be discriminated against only on the basis of his own chromosomes and genes, discrimination against...

...the sentence. This may be one reason to believe the definition of "genetic heritage" is not meant to be limited to the individual discriminated against. **Protocol**, supra note 9, art. 4(1); see infra note 50.

(50.) **Protocol**, supra note 9, art. 4(1). The term "Genetic Heritage" seems to be unclear on its face, and is not defined in the Explanatory Report...

...paragraph) 42. Paragraph 44 of the Explanatory Report provides that particular attention be paid to stigmatization in the context of screening programs. In neither the **Protocol** itself nor the Explanatory Report is stigmatization outright prohibited (only sought to be prevented), although discrimination clearly is prohibited. Id. (paragraph) (paragraph) 39-44.

(53...

...regular monitoring: (c) persons providing genetic services have appropriate qualifications to enable them to perform their role in accordance with professional obligations and standards.

(a) **Protocol**, supra note 9, art. 5.

(54.) "Clinical utility of a genetic test shall be an essential criterion for deciding to offer this test to a person or a group of persons."

Protocol, supra note 9, art. 6. "Clinical utility" is to be understood by the value of the test results in guiding the person concerned in his...

...to genetic tests with important implications for the health of the persons concerned or members of their family or with important implications concerning procreation choices." **Protocol**, supra note 9, art. 7.

(56.) *Id.* art. 8(1).

(57.) *Id.* art. 8(2). The definition of "genetic counseling" in the **Protocol** is more extensive than the definition in the GenDG:

The notion of "genetic counselling" is to be understood here as a communication and support process...

...must refer to Article 18." *Id.* (paragraph) 84. Article 18 contains the requirement that if there are such implications, the person tested shall be informed. **Protocol**, supra note 9, at Art. 18. Like the GenDG, though, it does not go so far as to require that the family members be informed...

...s consent. *Id.*

(58.) Explanatory Report, supra note 45, (paragraph) 88.

(59.) *Id.* arts. 13, 14.

(60.) *Id.* art. 13.

(61.) *Id.* art. 19.

(62.) **Protocol**, supra note 9, art. 19. Those conditions are:

(a) the programme is recognised for its health relevance for the whole population or section of population...

...about the right not to know, reveals the legislative attitude that the right not to know is more important than the right to know.

(66.) **Protocol**, supra note 9, art. 16(2).

(67.) "Clarification in regard to the right of any subject person to not have to know results, including without...

...not have examination results, either partially or entirely, disclosed but to have them destroyed instead...." GenDG (section) 9(2), 9(5).

(68.) *Id.*

(69.) **Protocol**, supra note 9, art. 16(3).

(70.) *Id.* art. 16(4).

(71.) Explanatory Report, supra note 45, (paragraph) 135. The reference here to Article 4...

View: [HTML](#) | [PDE](#) | [Word](#)

☐ PHILIPPINES PLDT GROUP TO ROLL OUT NEW WIFI SERVICE NEXT YEAR.

Date: December 21, 2011

1/6,K/16 (Item 16 from file: 9)

05096604 Supplier Number: 275385829

PHILIPPINES PLDT GROUP TO ROLL OUT NEW WIFI SERVICE NEXT YEAR.

December 21, 2011

Word Count: 359

TEXT:

...is sign in with a username and password which they can purchase online or in retail stores. In the near future, we would make automatic **authentication** through the use of the subscribers SIM (subscriber identification **module**) card," he said.

As the service uses standard WiFi technology found in most portable devices, the carrier-grade WiFi service can be used by all...

View: [HTML](#) | [PDE](#) | [Word](#)

☐ BUSINESS AND INNOVATION AT THE HEART OF THE TRADE SHOW ...

Date: November 29, 2011

1/6,K/17 (Item 17 from file: 9)

05075968 Supplier Number: 273570375

BUSINESS AND INNOVATION AT THE HEART OF THE TRADE SHOW ...

November 29, 2011

Word Count: 752

TEXT:

...other smart mobile objects.

Many projects in Government Security and in E-health The identity protection sector is booming and the technologies of identification and **authentication** presented by the exhibitors have been applied to many documents (biometrics passports, electronic ID, electronic driver's license, health cards...). E-health has been in...

...IT SECURITY APPLICATION: GEMALTO with Just4YourEyes

* BEST TRANSPORTATION APPLICATION: INSIDE SECURE with VHBR

* BEST BANKING/RETAIL/LOYALTY APPLICATION: SIMARTIS TELECOM with Bubble

* BEST SECURE INTERNET/**AUTHENTICATION** APPLICATION: HID GLOBAL with Next Generation Secure Identity Ecosystem

* BEST MOBILITY APPLICATION: NXP SEMICONDUCTORS with PN65 Secure NFC **module**

* BEST eTRANSACTIONS APPLICATION: VERIFONE with PAYware Mobile Enterprise

* BEST MANUFACTURING & TESTS APPLICATION: OBERTHUR TECHNOLOGIES with ID
One Digital watermark

See you at the 27th CARTES...

View: [HTML](#) | [PDF](#) | [Word](#)

☐ CINTERION ENABLES REMOTE MONITORING OF 100,000 KONICA MINOLTA...

Date: November 18, 2011

1/6,K/18 (Item 18 from file: 9)

05066312 Supplier Number: 272710469

CINTERION ENABLES REMOTE MONITORING OF 100,000 KONICA MINOLTA...

November 18, 2011

Word Count: 1142

TEXT:

Cinterion's award-winning Java™ **module** provides secure wireless data communications and runs application software designed to manage the service and maintenance needs of enterprise-grade office machines anywhere in the...

...other issues before problems arise. The solution's embedded Java client from Inside M2M collect machine data via an attached MCT terminal, and the Cinterion **module** securely communicates back and forth over wireless networks to a dedicated backend server provided by Inside M2M. System administrators can log on from any computer...

...and security expertise as well as its engineering support in local markets around the world," said Derek Uhlig, CEO of Inside M2M. "Cinterion's Java **module** is crucial for simultaneous software hosting and secure communications, allowing cost efficiencies by eliminating the need for additional processors and complexity."

"We were pleased to...

...devices, and managed services to wireless operators, banks, enterprises and government agencies.

Gemalto is the world leader for electronic passports and identity cards, two-factor **authentication** devices for online protection, smart credit/debit and contactless payment cards, as well as subscriber identification modules (SIM) and universal integrated circuit cards (UICC) in...

View: [HTML](#) | [PDF](#) | [Word](#)

☐ CINTERION LAUNCHES NEW HIGH-SPEED AUTOMOTIVE M2M **MODULE**...

Date: November 15, 2011

1/6,K/19 (Item 19 from file: 9)

05065288 Supplier Number: 272557255

CINTERION LAUNCHES NEW HIGH-SPEED AUTOMOTIVE M2M **MODULE**.

November 15, 2011

Word Count: 922

CINTERION LAUNCHES NEW HIGH-SPEED AUTOMOTIVE M2M **MODULE**.

(

TEXT:

(Full text of a statement. Contact details below.)

(BW)(CINTERION)(GTO.BOURSE) Cinterion Launches New High-Speed Automotive M2M **Module**

High-Tech Editors

CARTES & IDentification 2011

PARIS--(BUSINESS WIRE) - Nov. 15, 2011-- Cinterion, the global leader in cellular machine-to-machine (M2M) communication modules and a Gemalto (Euronext NL 0000400653 GTO) company, launches AH3, its new high-speed automotive M2M **module** with a new triple-diversity antenna design. AH3 delivers reliable always-on communications across global 2G and 3G cellular networks for advanced applications such as...

The **module**'s SIM Access Profile enables easy integration of additional wireless devices, connection with smartphones and software applications, while analog audio processing and advanced voice support provide superior hands-free capabilities. AH3's compact, single-sided design shares a common footprint with forthcoming LTE modules.

The ruggedized AH3 **module** features a totally new and improved triple-diversity antenna concept that is based on pogo pads enabling simple and reliable mounting at reduced total cost...

...mobile businesses with greater and richer access to information and remote diagnostics," said Norbert Muhrer, CEO Cinterion. "Cinterion's easy-to-integrate, richly-featured AH3 **module** meets all the demands of advanced automotive applications."

Additional AH3 product information:

AH3 samples and evaluation kits are available with mass production beginning in Q2...

...devices, and managed services to wireless operators, banks, enterprises and government agencies.

Gemalto is the world leader for electronic passports and identity cards, two-factor **authentication** devices for online protection, smart credit/debit and contactless payment cards, as well as subscriber identification modules (SIM) and universal integrated circuit cards (UICC) in...

View: [HTML](#) | [PDF](#) | [Word](#)

☐ Readers can function as intelligent alarm keypads.

Date: October 2011

1/6,K/20 (Item 20 from file: 9)

05058023 Supplier Number: 270732668

Readers can function as intelligent alarm keypads.

October 2011

Word Count: 196

TEXT:

...versions of Symmetry Security Management V6.x or as fully functional, intelligent alarm keypads when used with Symmetry Homeland V7 with the Symmetry Intrusion Management **module** and supported Symmetry M2150 multiNODE controllers. The Javelin 884-KP reads NXP Mifare and Mifare DESFire smart cards, in addition to Personal Identity Verification (PIV), Transportation Worker Identity Credential (TWIC) and First Responder **Authentication** Card (FRAC) cards. The Javelin 880-KP reads 125kHz HID Proximity credentials. Other models will be released over time. The Javelin LCD graphical display verifies...

View: [HTML](#) | [PDF](#) | [Word](#)

☐ CARTES & IDENTIFICATION 2011: 16TH EDITION OF THE SESAMES AWARDS.

Date: October 21, 2011

1/6,K/21 (Item 21 from file: 9)

05040449 Supplier Number: 270335245

CARTES & IDENTIFICATION 2011: 16TH EDITION OF THE SESAMES AWARDS.

October 21, 2011

Word Count: 812

TEXT:

...The finalists are HID Global with Next Generation Secure Identity Ecosystem; Intercede with PIV Credentials on a BlackBerry phone; Smart Packaging Solutions with Embedded Contactless **Module**.

- IT SECURITY SESAME The finalists are Gemalto with One4all; Gemalto with Just4YourEyes; Nets Denmark A/S with PCI OEM **Module**.

- TRANSPORTATION SESAME The finalists are ASK with TicketTac; INSIDE Secure with VHBR; Mastercard with City Card on MasterCard M/Chip Advance.

- BANKING / RETAIL / LOYALTY SESAME...

...finalists are Simartis Telecom SRL with Bubble; Turkcell with Turkcell Mobile Wallet (Turkcell Cep-T Cuzdan); Watchdata System Co. Ltd. with SC-NFC;

- TRUSTED INTERNET / **AUTHENTICATION** SESAME The finalists HID Global with Next Generation Secure Identity Ecosystem; NXP Semiconductors with On-card gesture recognition; Trusted Designer with Certphone.

- MOBILITY SESAME The finalists are GoTrust Technology Inc with SWP microSD; NXP Semiconductors with PN65 Secure NFC **module**; Trusted Logic with Trusted User Interface for Android devices.

- E-TRANSACTIONS SESAME The finalists are BPC Banking Technologies with BeeSmart Card; Buyster with Buyster mobile...

View: [HTML](#) | [PDF](#) | [Word](#)

☐ Improving security of online banking using RFID.

Date: July 2011

1/6,K/22 (Item 22 from file: 9)

05035665 Supplier Number: 263035559

Improving security of online banking using RFID.

July 2011

Word Count: 2206

ABSTRACT:

Banks protect customers' security in three main techniques: passwords, encryption, and firewalls/server security. This study develops a **module** that shall further tighten security of online banking, and improve trust. This study proposed that there is a need for an additional **authentication** due to the fact that trust has new dimensions in financial services. A model using RFID as a second **authentication** layer is proposed and developed. Internet security is assumed to be a major obstacle to the adoption of online banking, which made customers concerned about...

TEXT:

...a user name and password during transmission and uses them to access the account.

This study proposed that there is a need for an additional **authentication** due to the fact that trust has new dimensions in financial services. Several studies have identified trust as an important factor influencing customer participation in...

...OMITTED)

Data security between the customer browser and our Web server is handled through Secure Sockets Layer (SSL) security protocol, which provides data encryption, server **authentication**, message integrity for a Internet connection, and provides a security "handshake" that is used to initiate the connection (Freier et al, 1996). Some banks came up with their own method of enhanced security model. Wool forest National bank in the USA for example, implemented what they call "Intelligent **Authentication**" (IA). The way it works is each time a customer uses online banking, the system will "profile" his/her online banking behavior by tracking each...

...security risks and improving customers' trust. Therefore, in an attempt to help online banks achieve a high level of trust, this study has developed a **module** that shall further tighten security of online banking, and reduce the associated risk (see figure 2), by adding a Radio-Frequency Identification (RFID) reader to...that scanning is done over the air. Sensing the presence of the ATM card, and reading its information shall provide physical evidence for user's **authentication**. The absence of the card shall prevent accessing the account. The bank providing the ATM card shall be responsible for encrypting and securely transmitting data.

DOUBLE AUTHENTICATION

With Double **Authentication**, there are two **authentication**/authorization stages. These two stages occur after a user tries to access the online baking account. This will provide additional **authentication** for online banking services. With Double **Authentication**, you essentially require remote users to pass a second stage of user **authentication** (the magnetic code stored on the back of ATM card) before they can gain network access. The system architecture is illustrated in figure 5.

(FIGURE...

...way that their use will increase trustworthiness in the human-to-technology interaction. There are various means to provide those security services, (e.g., firewalls, **authentication**, intrusion detection,

etc.), but "how can we trust that the system is secured enough to use?" This study has developed and proposed a **module** that shall further tighten security of online banking, and improve trust, by adding an RF ID in the online banking system at the end user...

View: [HTML](#) | [PDF](#) | [Word](#)

☐ CINTERION LAUNCHES THE WORLD'S THINNEST HSPA+ **MODULE**...

Date: October 13, 2011

1/6,K/23 (Item 23 from file: 9)

05031970 Supplier Number: 269505466

CINTERION LAUNCHES THE WORLD'S THINNEST HSPA+ **MODULE**...

October 13, 2011

Word Count: 836

CINTERION LAUNCHES THE WORLD'S THINNEST HSPA+ **MODULE**...

(

TEXT:

(Full text of a statement. Contact details below.)

(BW)(CINTERION)(GTO.BOURSE) Cinterion Launches the World's Thinnest HSPA+ **Module** for Machine-to-Machine Applications

PHS8 Provides Flexible Surface Mounting and a Reliable Path to LTE

Technology Writers/Tradeshaw Writers CTIA Enterprise & Applications
2011 booth...

...Machine (M2M) industry leader for more than 15 years and a Gemalto company (Euronext NL 0000400653 GTO), today launched the world's thinnest HSPA+ M2M **module**. This fully ruggedized, high-bandwidth **module** features flexible Surface Mounting Technology and enables secure, high-speed voice and data communications on global 2G and 3G cellular networks. It also provides a...

"Our new PHS8 **module** enables advanced communications for today's networks and readiness for tomorrow's technology," said Norbert Muhrer, CEO, Cinterion. "Providing a compatible footprint as a bridge...

...integrated GPS and flexible surface mounting PHS8 simplifies integration and streamlines efficient mass manufacturing to deliver lower total cost of ownership for M2M customers. The **module**'s unique thermal design extends the temperature range from -40°C to +85°C for reliable communications in even the most extreme conditions. Integrated voice...

...devices, and managed services to wireless operators, banks, enterprises and government agencies.

Gemalto is the world leader for electronic passports and identity cards, two-factor **authentication** devices for online protection, smart credit/debit and contactless payment cards, as well as subscriber identification modules (SIM) and universal integrated circuit cards (UICC) in...

View: [HTML](#) | [PDF](#) | [Word](#)

☐ Public sector innovation: case study of e-government projects in Pakistan.

Date: December 2009

1/6,K/24 (Item 24 from file: 9)

05026538 Supplier Number: 269029162

Public sector innovation: case study of e-government projects in Pakistan.

December 2009

Word Count: 6355

TEXT:

...Hajj (DGH), Jeddah, Mecca or Medina etc. Updation of status of the pilgrims will be done through a secure, reliable and efficient manner after proper **authentication** and authorisation of the requesting terminal. However, the dissemination of information will be done through a simple and easy-to-use interface provided to pilgrims...developmental budgets, district government plans and its budgets, provincial plans for next 5-10 years, information of budget, furniture, equipments etc. in any office, training **module**, training calendar of each institution, training curriculum for each training course/centres, list of resource persons and their specialisation, basic information of Local government, HMIS...

View: [HTML](#) | [PDE](#) | [Word](#)

☐ PERSONAL ARGENTINA AND GEMALTO DEPLOY SIM-BASED FACEBOOK SERVICE.

Date: October 05, 2011

1/6,K/25 (Item 25 from file: 9)

05024695 Supplier Number: 268763129

PERSONAL ARGENTINA AND GEMALTO DEPLOY SIM-BASED FACEBOOK SERVICE.

October 05, 2011

Word Count: 564

TEXT:

The software application, which is embedded inside the Subscriber Identification **Module** (SIM), allows you to easily access core Facebook features from the phone's main screen, through an intuitive and interactive menu. You can receive notifications...

...devices, and managed services to wireless operators, banks, enterprises and government agencies.

Gemalto is the world leader for electronic passports and identity cards, two-factor **authentication** devices for online protection, smart credit/debit and contactless payment cards, as well as subscriber identification modules (SIM) and universal integrated circuit cards (UICC) in...

View: [HTML](#) | [PDE](#) | [Word](#)

Records: 1 to 25 of 17,643

Page 1 [Next >>](#)

© 2012 Dialog LLC All Rights Reserved.
Version: 3.0

+ You Search Images Maps Play ^{NEW} YouTube News Gmail Documents Calendar More ~





Search

About 487,000 results (0.37 seconds)



Everything

Images

Introduction to EFT Server

help.globalscape.com/help/efits-2/introduction_to_efitsserver.htm

Aug 18, 2011 -- All **module** features are available during the trial period for both "SMB" and ... files transferred over the Internet using **secure protocols** including FTPS (SSL/TLS), ... of completed **transactions**, and digital certificates for proof of **identity**. ... **Authentication** and Authorization - EFT Server supports password, ...

Maps

Videos

News

Shopping

More

RFC 5324 - MIB for Fibre-Channel Security Protocols (FC-SP ...

www.iaggs.org/rfcs/rfc5324.html

The T11-FC-SP-AUTHENTICATION-MIB Module16 4.8.3.
Management **Transaction** of the **Security** Association Management **Protocol** (see below) ... has to be protected by which SA, and what the **characteristics** of the protection are. **Protocols** is to allow a Fibre Channel entity to be assured of the **identity** of each ...

Alexandria, VA

Change location

Glossary

java.sun.com/j2ee/tutorial/1_3-fcs/doc/Glossary.html

A person that combines components and **modules** into deployable application ...
Security identities may be principals or groups in the operational environment.

All results

Related searches

More search tools

Included Authentication Modules

docs.redhat.com/.../6/.../Included_Authentication_Modules.html

The following **authentication modules** are included in the Enterprise ... This login **module** is designed to establish caller **identity** and credentials when the ... or EJB methods that are associated with the unchecked **permission** constraint. ... a single **character** The transport **protocol** to use for **secure** access, such as SSL.

RFC 5592 - Secure Shell Transport Model for the Simple Network ...

tools.ietf.org/html/rfc5592

by D Harrington - 2009

This memo specifies a MIB **module** that is compliant to the SMiv2, which is described in Masquerade - SSH provides for verification of the **identity** of the SSH server and the ... has been properly configured to support authPriv security **characteristics**. ... The **security protocols** used in the Secure Shell **Authentication Protocol** ...

Glossary

msdn.microsoft.com/en-us/library/hh446592.aspx

Security. A Guide to Claims based **Identity** and Access Control (2nd Edition) ... claims provider that does not involve the redirection feature of the HTTP **protocol**. ... **Compare** with passive federation. ... A statement, such as a name, **identity**, key, group, **permission**, or capability WS-Federation **Authentication Module** (FAM).

Security Services

docs.oracle.com / ... > Introduction to WebLogic Enterprise Security

You can use **Secure Sockets Layer (SSL)** or Hyper-Text Transfer **Protocol** (HTTPS) to ... Each of these forms of **authentication** has one common **characteristic**-they all ... When used with an **Authentication** provider Login **Module**, **Identity** Assertion ... Role mapping is the process by which the **security** service **compares** users or ...

User Authentication and Authorization in the Java Platform

www.research.ibm.com/people/k/koved/papers/acsac.pdf

by C.L.L. Gong - Related articles

to decide the granting of individual access **permissions** to running code (according to the code's **characteristics**, e.g., ... tected resources will invoke **security** checks that **compare** ... **identities**. The Java **Authentication** and Authorization Ser- vice (JAAS) is designed vice, or **LoginModule**, that gets plugged in under

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	20740	(password) and biometric	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/03/27 10:32
L2	2361	L1 and authenticat\$3 and permission and transaction and identity	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/03/27 10:32
L3	11	L2 and "permission module"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/03/27 10:32
L4	5	L3 and (mobile or cell or cellular)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/03/27 10:32
L5	133	L2 and ("permission module" or "authentication module")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/03/27 10:32
L6	105	L5 and (mobile or cell or cellular)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/03/27 10:32
L7	60	L6 and (authenticat\$3 WITH (comparison or compar\$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/03/27 10:32
L8	20740	password and biometric	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/03/27 10:32
L9	0	L1 and authenticat\$3 and permission and transaction and identity	EPO; JPO	OR	ON	2012/03/27 10:38
L10	129	(password) and biometric	EPO; JPO	OR	ON	2012/03/27 10:38
L11	1160	705/67.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/03/27 10:48
L12	3022	security protocol permission module authentication module identity transaction characteristic compare	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2012/03/27 10:48
L13	4	security protocol "permission module" "authentication module" identity transaction	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	AND	ON	2012/03/27 10:49

		characteristic compare	IBM_TDB			
S1	20312	(password) and biometric	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/02/09 08:12
S2	2293	S1 and authenticat\$3 and permission and transaction and identity	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/02/09 08:14
S3	11	S2 and "permission module"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/02/09 08:16
S4	5	S3 and (mobile or cell or cellular)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/02/09 08:17
S5	130	S2 and ("permission module" or "authentication module")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/02/09 08:19
S6	102	S5 and (mobile or cell or cellular)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/02/09 08:19
S7	59	S6 and (authenticat\$3 WITH (comparison or compar\$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/02/09 08:55
S8	20312	password and biometric	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/02/09 08:57

3/ 27/ 2012 10:55:09 AM

C:\Users\jreagan\Documents\EAST\Workspaces\13017823.wsp

Issue Classification 	Application/Control No. 13017823	Applicant(s)/Patent Under Reexamination GRIGG ET AL.
	Examiner JAMES A REAGAN	Art Unit 3621

ORIGINAL						INTERNATIONAL CLASSIFICATION														
CLASS		SUBCLASS				CLAIMED					NON-CLAIMED									
705		67				G	0	6	Q	20 / 00 (2012.01.01)										
CROSS REFERENCE(S)																				
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)																			
705	65	64	44																	
380	229																			
713	155	156	157	158	159															
726	2	5	9	10																

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

NONE		Total Claims Allowed:	
		30	
(Assistant Examiner)	(Date)		
/JAMES A REAGAN/ Primary Examiner, Art Unit 3621	03/27/2012	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

Search Notes 	Application/Control No. 13017823	Applicant(s)/Patent Under Reexamination GRIGG ET AL.
	Examiner JAMES A REAGAN	Art Unit 3621

SEARCHED			
Class	Subclass	Date	Examiner
705	67	3/27/2012	JAR

SEARCH NOTES		
Search Notes	Date	Examiner
EAST	2/7/2012	JAR
Updated EAST	3/27/2012	JAR
GOOGLE	3/27/2012	JAR
DIALOG	3/27/2012	JAR

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner
	EAST Interference	3/27/2012	JAR

	/JAMES A REAGAN/ Primary Examiner, Art Unit 3621
--	---

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl No.: 13/017,823 Confirmation No.: 7401
Applicant: David M. Grigg
Filed: January 31, 2011
Group Art Unit: 3621
Examiner: REAGAN, James A.
Title: **MOBILE TRANSACTION DEVICE SECURITY SYSTEM**
Atty Dkt. No. 014033-001145
Customer No. 69603

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT UNDER 37 C.F.R. § 1.111

Examiner Reagan:

In response to the Office Action dated February 13, 2012, please amend the above-identified application as follows:

Amendments to the Drawings are provided on page 2 of this response.

Amendments to the Claims are reflected in the listing of claims beginning on page 3 of this response.

A **Summary of the March 9, 2012 Interview** with the Examiner is provided on page 10 of this response.

Remarks begin on page 11 of this response.

TRII\796160v2

Appl. No.: 13/017,823
Amdt. Dated: March 16, 2012
Reply to Office Action of February 13, 2012
Page 2 of 15

The Drawings

Replacement Sheets

Replacement drawings 5, 6, 8, and 9 are submitted herein in compliance with 37 C.F.R. §1.121(d). The replacement drawings are being submitted to replace fictional names, phone numbers, addresses, and business names with X's.

No new matter is added.

TRI1\796160v2

Amendments to the Claims:

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

1. (Currently Amended) A mobile transaction device security system comprising:
 - a memory device;
 - a communication device; and
 - a processing device coupled to the memory device, wherein the processing device is configured to:
 - receive a security protocol from a user, the security protocol comprising a permission module and an authentication module, wherein the permission module comprises instructions on when the user must authenticate an identity of the user to perform a transaction, wherein the instructions are provided by the user and stored in a database;
 - determine that the user is conducting ~~a~~ the transaction;
 - compare at least one characteristic of the transaction with the instructions provided by the user ~~permission module~~; and
 - determine a process for authenticating the user by:
 - determining if the user must authenticate the user's identity based on the comparison of the transaction with the instructions provided by the user,
 - allowing the transaction if the user is not required to authenticate the user's identity based on the comparison, and
 - requiring authentication of the user through the authentication module if the comparison of the transaction to the instructions provided by the user indicates that the transaction cannot proceed without authentication, wherein requiring authentication comprises requesting authentication of the user's identity,
 - receiving input from the user, comparing the input to the authentication module,
 - and allowing the transaction if the user is authorized to perform the transaction based on the comparison of the input with the authentication module, ~~the~~

determination based on the comparison of the transaction with the permission module.

2. (Cancelled)

3. (Cancelled)

4. (Original) The system of claim 1, wherein the authentication module comprises at least one security feature.

5. (Currently Amended) The system of claim 4 ~~claim 3~~, wherein the at least one security feature is customizable by the user.

6. (Currently Amended) The system of claim 4 ~~claim 3~~, wherein the security feature consists of at least one of a username, a password, a challenge question, a voice recognition test, a facial recognition test, a fingerprint identification test, and an iris scan.

7. (Original) The system of claim 1, wherein the communication device consists of at least one of a keyboard, a scanner, a touchpad, a camera, a speaker, and a microphone.

8. (Cancelled)

9. (Cancelled)

10. (Cancelled)

11. (Currently Amended) The system of claim 1 ~~claim 9~~, wherein the characteristic of the transaction consists of at least one of the dollar amount of the transaction, the identity of the merchant, the category of the expense, the time of the transaction, and the location of the transaction.

12. (Currently Amended) A computer-implemented method of providing financial transaction security, the method comprising:

receiving a security protocol from a user, the security protocol comprising a permission module and an authentication module, wherein the permission module comprises instructions on when the user must authenticate an identity of the user to perform a transaction, wherein the instructions are provided by the user and stored in a database;

determining that the user is conducting the a transaction;

comparing at least one characteristic of the transaction with the instructions provided by the user permission module;

determining if the user must authenticate the user's identity based on the comparison of the transaction with the instructions provided by the user; permission module

allowing the transaction if the user does not need to authenticate the user's identity based on the comparison; and

requiring authentication of the user through the authentication module if the comparison of the transaction to the instructions provided by the user indicates that the transaction cannot proceed without authentication, wherein requiring authentication comprises:

requesting authentication of the user's identity,

receiving input from the user,

comparing the input to the authentication module, and

allowing the transaction if the user is authorized to perform the transaction based on the comparison of the input with the authentication module; and

allowing the transaction if the user does not need to authenticate the user's identity.

13. (Cancelled)

14. (Currently Amended) The method of claim 12, wherein receiving the security protocol from the user comprises ~~receiving instructions for prompting the authentication module and~~ receiving security features for authenticating the user's identity.

15. (Original) The method of claim 12, wherein determining that the user is conducting a transaction comprises receiving a signal from a point-of-sale device indicating that the user is attempting to conduct a transaction.

16. (Currently Amended) The method of claim 12, wherein comparing the transaction with the instructions provided by the user permission module comprises comparing at least one of ~~the~~ a transaction amount, ~~the~~ a transaction time, ~~the~~ a transaction location, ~~the~~ a transaction merchant, and ~~the~~ a transaction category with predetermined instructions in the permission module.

17. (Cancelled)

18. (Currently Amended) The method of claim 12, wherein allowing the transaction comprises transferring ~~the user's~~ account information of the user to a point-of-sale device.

19. (Original) The method of claim 18, wherein the transferring the user's account information to the point-of-sale device comprises wirelessly transferring the account information.

20. (Currently Amended) The method of claim 12 ~~claim 13~~, wherein requesting authentication of the user's identity comprises receiving input of at least one of a username, a password, an answer to a challenge question, a voice recognition scan, a facial scan, a fingerprint scan, and an iris scan.

21. (Original) The method of claim 20, wherein comparing the input from the user with the authentication module comprises comparing the input from the user with a security feature.

22. (Original) The method of claim 21, wherein the security feature is stored in memory associated with a mobile device.

23. (Original) The method of claim 22, wherein the memory is capable of receiving power from a point-of-sale device.

24. (Cancelled)

25. (Currently Amended) A computer program product for providing a financial transaction security product, the computer program product comprising:

 a non-transitory computer-readable medium comprising:

 an executable portion for causing a computer to receive a security protocol from a user, the security protocol comprising a permission module and an authentication module,
 wherein the permission module comprises instructions on when the user must authenticate an identity of the user to perform a transaction, wherein the instructions are provided by the user and stored in a database;

 an executable portion for causing a computer to determine that the user is conducting the a transaction;

 an executable portion for causing a computer to compare at least one characteristic of the transaction with the instructions provided by the user permission module;

 an executable portion for causing a computer to determine if the user must authenticate the user's identity an identity of the user based on the comparison of the transaction with the instructions provided by the user permission module; and

 an executable portion for causing a computer to allow the transaction if the user does not need to authenticate the user's identity based on the comparison; and

an executable portion for requiring authentication of the user through the authentication module if the comparison of the transaction to the instructions provided by the user indicates that the transaction cannot proceed without authentication, wherein requiring authentication comprises:

requesting authentication of the user's identity,

receiving input from the user,

comparing the input to the authentication module, and

allowing the transaction if the user is authorized to perform the transaction based on the comparison of the input with the authentication module.

26. (Cancelled)

27. (Currently Amended) The computer program product of claim 25, further comprising an executable portion for causing a computer to determine ~~the user's~~ a location of the user when the user is conducting the transaction.

28. (Original) The computer program product of claim 25, further comprising memory coupled to the non-transitory computer readable medium.

29. (Original) The computer program product of claim 28, wherein the memory stores at least one of financial account information for the user, instructions associated with the permission module for the user, and security features associated with the authentication module for the user.

30. (Original) The computer program product of claim 29, wherein the user's financial account information consists of information associated with at least one of a checking account, a savings account, a money market account, a credit account, an investment account, and a rewards points account.

31. (Original) The computer program product of claim 25, wherein the permission module requires the user to authenticate the user's identity if a transaction amount is over a predetermined dollar amount.

32. (Original) The computer program product of claim 25, wherein the permission module requires the user to authenticate the user's identity if the transaction is occurring at a non-approved merchant.

33. (Original) The computer program product of claim 32, wherein the non-approved merchant is a merchant that the user has not purchased from previously.

34. (Original) The computer program product of claim 25, wherein the permission module requires the user to authenticate the user's identity if the user has not authenticated the identity within a predetermined time period.

35. (Original) The computer program product of claim 25, wherein the permission module requires the user to authenticate the user's identity if the user is outside of predetermined geographical areas.

36. (Original) The computer program product of claim 25, wherein the permission module requires the user to authenticate the user's identity if a transaction amount would lower a balance in the user's account below a predetermined level.

37. (Original) The computer program product of claim 25, wherein the permission module requires the user to authenticate the user's identity if the user has already conducted a predetermined number of transactions within a predetermined time period.

38. (Original) The computer program product of claim 25, wherein allowing the transaction comprises determining an account from which a payment for the transaction is made.

39. (Original) The computer program product of claim 38, wherein determining the account comprises comparing the transaction to instructions received from the user.

Summary of March 9, 2012 Interview with the Examiner

On March 9, 2012, Examiner Reagan and the undersigned attorney had a brief telephone interview to discuss amendments to the drawings. In the interview, Examiner Reagan indicated that submission of replacement drawings with the Response to the Office Action would be entered as a matter of right after being inspected by the Examiner for new matter and compliance with formatting requirements. Applicants thank the Examiner for the discussion.

REMARKS

This Amendment is filed in response to the Office Action dated February 13, 2012.

Claims 1-39 are pending in the application.

Claims 1-39 stand rejected in the application.

Applicants kindly request amendment to claims 1, 5, 6, 11, 12, 14, 16, 18, 20, 25, and 27.

Applicants kindly request cancellation of claims 2, 3, 8-10, 13, 17, 24, and 26.

Thus, once the proposed amendments have been entered into the record, claims 1, 4-7, 11, 12, 14-16, 18-23, 25, and 27-39 will be pending.

Applicants respectfully submit that the pending claims are patentable and respectfully request reconsideration in light of the following remarks.

I. Replacement Drawings

Applicants submit herewith four drawing sheets in compliance with 37 C.F.R. §1.121(d) to replace Figures 5, 6, 8, and 9. The drawing sheets replace fictional names, businesses, phone numbers, and email addresses with X's. Applicants respectfully request that the Amendments to the drawings be submitted in advance of the Application publishing.

II. Claim Rejections – 35 USC § 112

In the February 13, 2012 Office Action, the Office rejected claims 9 and 10 under 35 U.S.C. §112, second paragraph, as allegedly being indefinite for failing to particularly point out and distinctly claim the subject matter which the Applicants regard as the invention. Specifically, the Office stated that the limitation "instructions" lacks antecedent basis. Applicants have cancelled claims 9 and 10, making this rejection moot. Applicants respectfully request withdrawal of the 35 U.S.C. §112, second paragraph, rejection.

III. Claim Rejections – 35 USC § 103

In the February 13, 2012 Office Action, the Office rejected claims 1-7, 12, 13, 15, 17-26, 28, and 29 under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Patent Application Publication No. 2006/0021003 to Fisher et al. (hereinafter Fisher) in view of U.S. Patent Application Publication No. 2006/0123465 to Ziegler (hereinafter Ziegler). Applicants do not agree with the rejections but in furtherance of prosecution have amended independent claims 1, 12, and 25 with additional recitations from claims 2, 3, 8, 9, and 10. As recognized by the Office, at least claims 8, 9, and 10 are not obvious over Fisher and Ziegler.

Specifically, Applicants have amended the independent claims to recite that the permission module comprises instructions on when the user must authenticate the user's identity to perform a transaction, wherein the instructions are provided by the user. Additionally, the independent claims have been amended to recite that at least one characteristic of a transaction is compared with the instructions provided by the user. The independent claims have been further amended to recite determining if the user must authenticate an identity of the user based on the comparison of the transaction with the instructions provided by the user and allowing the transaction if the user does not need to authenticate the user's identity.

In the February 13, 2012 Office Action, the Office rejected claims 8-11, 14, 16, 27, and 30-39 under 35 U.S.C. §103(a) as allegedly being unpatentable over Fisher and Ziegler and further in view of Official Notice. Applicants respectfully traverse these rejections.

The Office recognized that Fisher does not teach that the processing device is configured to determine the process for authenticating the user by determining if the user must authenticate an identity of the user based on the comparison of the transaction with the permission module, and wherein the processing device is further configured to allow the transaction if the user does not need to authenticate the user's identity. The Office alleged that Ziegler, in at least paragraph 0127, discloses allowing the transaction to proceed if the user is properly authenticated, or

preventing the transaction if the user is not properly authenticated. See, page 6, lines 10-16, of the February 13, 2012 Office Action.

Applicants submit that paragraph 0127 of Ziegler is directed to biometric authentication of a customer's identity prior to allowing a transaction. Nowhere in paragraph 0127 or in all of Ziegler is it disclosed that a transaction can proceed without authentication based on comparison of the transaction to instructions provided by the user. In fact, the portion of Ziegler cited in the Office Action teaches away from allowing a transaction to proceed without authentication. Ziegler recites: "In any financial transaction, it may be important that the identity of both parties be authenticated in a manner which positively establishes the identities of the parties." See, paragraph [0003] of Ziegler.

As recited in MPEP §2145, "A prior art reference that 'teaches away' from the claimed invention is a significant factor to be considered in determining obviousness." Here, Ziegler actively teaches away from allowing a transaction when a the user does not authenticate the user's identity by reciting that it may be important that the identity of both parties by authenticated in a manner which positively establishes the identities of the parties. One skilled in the art would not be directed to a system that allows individuals, in some cases, to perform transactions without authentication after reading in Ziegler that positively establishing the identities of the parties to a transaction is important.

Further, the Office recognized that the combination of Fisher and Ziegler does not specifically disclose that:

- The permission module comprises instructions on when the user must authenticate the user's identity to perform the transaction.
 - The instructions are provided by the user.
 - The instructions are based on a characteristic of the transaction.
- See, page 11, lines 7-11, of the February 13, 2012 Office Action.

To cure this deficiency, the Office took Official Notice and alleged that it is old and well known in the OPSEC arts to set standards for ensuring secure transactions. The Office alleged that:

“In the competitive business climate, there is a profit-driven motive to maximize the profitability of goods and services that are provided or marketed to customers. Enterprises typically use business planning to make decisions in order to maximize profits. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine/modify the method of Fisher/Ziegler with the technique of setting specific authentication instructions because n the competitive business climate, there is a profit-driven motive to maximize the profitability of goods and services that are provided or marketed to customers. Enterprises typically use business planning to make decisions in order to maximize profits. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine/modify the method of Fisher/Ziegler with the security standards technique” See, page 11, line 16 to page 12, line 1, of the February 13, 2012 Office Action.

Applicants respectfully disagree. MPEP §2144.03(A) recites: “Official notice unsupported by documentary evidence should only be taken by the Office where the facts asserted to be well-known, or to be common knowledge in the art are capable of instant and unquestionable demonstration as being well-known.” It is not common knowledge to provide a permission module that receives instructions from a user on when the user must authenticate the user’s identity to perform a transaction, wherein the instructions are based on a characteristic of the transaction. The cited art relied upon by the Office in fact teaches the opposite – that positively establishing the identity of the parties to a transaction is important. The Applicants traverse the Office Action’s Official Notice that providing a permission module comprising instructions received from the user on when the user must authenticate the user’s identity is common knowledge and request that the Office provide documentary evidence in the next Office action if the rejection is to be maintained. (See MPEP §2144.03(C)).

Applicants further submit that the rules for when authentication is required as presented in dependent claims 31-37 are novel and non-obvious over both the cited prior art and are not common knowledge in the art.

In view of the arguments and amended claims, Fisher, Ziegler, and Official Notice, alone or in combination, fail to teach or suggest independent claims 1, 12, and 25, as well as dependent claims 4-7, 11, 14-16, 18-23, and 27-39. The Applicants respectfully request that the Office Action withdraws the rejections of claims 1-39 under §103 and issues a Notice of Allowance.

Conclusion

In view of the amended claims and the remarks presented above, it is respectfully submitted that all of the present claims of the application are in condition for immediate allowance. It is therefore respectfully requested that a Notice of Allowance be issued. The Office is encouraged to contact Applicants' undersigned attorney to resolve any remaining issues in order to expedite examination of the present application.

It is not believed that extensions of time or fees for net addition of claims are required, beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 CFR § 1.136(a), and any fee required therefore (including fees for net addition of claims) is hereby authorized to be charged to Deposit Account No. 13-4365.

Respectfully submitted,

/Andrew D. Gerschutz/

Andrew D. Gerschutz
Registration No. 65,529

CUSTOMER NUMBER 69603
MOORE & VAN ALLEN PLLC
430 Davis Drive, Suite 500
Post Office Box 13706
Research Triangle Park, NC 27709
Tel Triangle Office: (919) 286-8000
Fax Triangle Office: (919) 416-8365

Electronically filed via the EFS-Web Electronic Filing System of the United States Patent and Trademark Office on March 16, 2012.

500 →

503	FINANCIAL TRANSACTION SECURITY SYSTEM				502	✕
504	HOME USER INFORMATION ACCOUNTS PERMITTED TRANSACTIONS USER AUTHENTICATION HELP					
506	CURRENT USER: XXXXX					
508	ACCOUNT INFORMATION: CHECKING ACCOUNT AND CREDIT ACCOUNTS ACTIVE					
510	PERMITTED TRANSACTIONS: CUSTOM BASED ON TRANSACTION AMOUNT, MERCHANT, AND CATEGORY					
512	USER AUTHENTICATION: USERNAME, FACIAL SCANNING, AND VOICE RECOGNITION ACTIVE					
	<u>RECENT TRANSACTIONS</u>					
	<u>PAYEE NAME</u> — 514	<u>AMOUNT</u> — 516	<u>DATE</u> — 518	<u>SECURITY</u> — 520		
	GAS STATION	\$30.00	12/01/2010	AUTOMATIC PAYMENT		
	PAY FROM: CREDIT ACCOUNT					
	PREVIOUS BALANCE: \$140.00					
	GROCERY STORE	\$120.00	12/03/2010	VOICE SCAN CONFIRMED	522	
	PAY FROM: CHECKING ACCOUNT					
	PREVIOUS BALANCE: \$2200					
	COFFEE SHOP	\$3.00	12/04/2010	AUTOMATIC PAYMENT	524	
	PAY FROM: CHECKING ACCOUNT					
	PREVIOUS BALANCE: \$2080					

FIG. 5

600 →

FINANCIAL TRANSACTION SECURITY SYSTEM		502	☒
HOME <u>USER INFORMATION</u> ACCOUNTS PERMITTED TRANSACTIONS USER AUTHENTICATION HELP			
604	CURRENT USER: XXXXX	602	EDIT 608 LOG OUT 610
606	MAILING ADDRESS:		
	STREET: XXXXXXXXX		
	CITY, STATE, ZIP: XXXXXXXXXXXXX		
	PHONE NUMBER: XXX-XXX-XXXX		
	EMAIL ADDRESS: XXXXXXXXXXXXXXX		
612	ADD A USER:		
	MAILING ADDRESS:		
	STREET: _____		
	CITY, STATE, ZIP: _____		
	PHONE NUMBER: _____		
	EMAIL ADDRESS: _____		
614	AUTHORIZE THIS USER FOR CURRENT ACCOUNTS? _____ YES _____ NO _____ CUSTOMIZE 616		

FIG. 6

800 →

804	FINANCIAL TRANSACTION SECURITY SYSTEM	502	802	☒
	HOME USER INFORMATION ACCOUNTS <u>PERMITTED TRANSACTIONS</u> USER AUTHENTICATION HELP			
	INSTRUCTIONS FOR ALLOWING A TRANSACTION WITHOUT AUTHENTICATING IDENTITY			EDIT
806	(A) DOLLAR AMOUNT THAT DOES NOT REQUIRE AUTHENTICATION: \$5.00 836 824 826			
808	(B) TIME SINCE PREVIOUS AUTHENTICATION BEFORE REQUIRING AUTHENTICATION: NOT SELECTED			
810	(C) DISTANCE FROM BILLING ADDRESS BEFORE REQUIRING AUTHENTICATION: NOT SELECTED			
812	(D) MERCHANTS THAT DO NOT REQUIRE AUTHENTICATION: MERCHANTS PURCHASED FROM MORE THAN TEN TIMES IN PREVIOUS YEAR — 828 XXXXXXX — 830 XXXXXXXX AT LOCATION XXXXXXXX — 832			
818	(E) TRANSACTION CATEGORIES THAT DO NOT REQUIRE AUTHENTICATION: GAS STATIONS — 834 COFFEE SHOPS			
820	(F) LOW BALANCE IN ACCOUNT BEFORE REQUIRING AUTHENTICATION: NOT SELECTED			
822	(G) CUSTOM INSTRUCTIONS: NOT SELECTED			

FIG. 8

900

FINANCIAL TRANSACTION SECURITY SYSTEM

502

902

X

HOME | USER INFORMATION | ACCOUNTS | PERMITTED TRANSACTIONS | USER AUTHENTICATION | HELP

904

CURRENT USER: XXXXX

906

CLEAR

908

USERNAME: XXXXX

914

EDIT

PASSWORD: *****

EDIT

916

CHALLENGE QUESTION: NOT SELECTED

920

ADD

910

FACIAL SCAN: IMAGE STORED AND ACTIVE

EDIT

912

VOICE SCAN: VOICE RECORDING STORED AND ACTIVE

EDIT

922

IRIS SCAN: NOT SUPPORTED

928

918

FINGERPRINT SCAN: FINGERPRINT NOT SAVED

ADD

924

CUSTOM DEVICE SECURITY FEATURE: NOT SUPPORTED

926

CHANGE CURRENT USER

FIG. 9

Electronic Acknowledgement Receipt	
EFS ID:	12320733
Application Number:	13017823
International Application Number:	
Confirmation Number:	7401
Title of Invention:	MOBILE TRANSACTION DEVICE SECURITY SYSTEM
First Named Inventor/Applicant Name:	DAVID M. GRIGG
Customer Number:	69603
Filer:	Andrew D. Gerschutz
Filer Authorized By:	
Attorney Docket Number:	4508US1.014033.1145
Receipt Date:	16-MAR-2012
Filing Date:	31-JAN-2011
Time Stamp:	11:14:55
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		BOA_1145_Response_to_OA_d ated_02132012_.pdf	132716 b5efb9d9bc53cb1c553c5c188dac630f490 487e	yes	15

Multipart Description/PDF files in .zip description					
Document Description			Start	End	
Amendment/Req. Reconsideration-After Non-Final Reject			1	1	
Drawings-only black and white line drawings			2	2	
Claims			3	9	
Applicant summary of interview with examiner			10	10	
Applicant Arguments/Remarks Made in an Amendment			11	15	
Warnings:					
Information:					
2	Drawings-only black and white line drawings	BOA_1145_Replacement_Drawings.pdf	73520	no	4
			9667a0c99d271388a75121e70955d1dd631c44ec		
Warnings:					
Information:					
Total Files Size (in bytes):			206236		
<p>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.</p> <p><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.</p> <p><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.</p> <p><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.</p>					

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

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875					Application or Docket Number 13/017,823	Filing Date 01/31/2011	☐ To be Mailed
APPLICATION AS FILED – PART I							
(Column 1)		(Column 2)		SMALL ENTITY ☐ OR		OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	OR	RATE (\$)	FEE (\$)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (j), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X \$ =		OR	X \$ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X \$ =			X \$ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	
APPLICATION AS AMENDED – PART II							
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY OR OTHER THAN SMALL ENTITY	
AMENDMENT	03/16/2012	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	* 30	Minus	** 39	= 0	X \$ =	OR X \$60= 0
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X \$ =	OR X \$250= 0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	OR TOTAL ADD'L FEE
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY OR OTHER THAN SMALL ENTITY	
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X \$ =	OR X \$ =
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X \$ =	OR X \$ =
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	OR TOTAL ADD'L FEE
<p>* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.</p> <p>** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".</p> <p>*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".</p> <p>The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.</p>							

Legal Instrument Examiner:
/BRENDA TURNER/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/017,823	01/31/2011	DAVID M. GRIGG	4508US1.014033.1145	7401
69603 7590 03/14/2012 MOORE & VAN ALLEN, PLLC FOR BOFA 430 DAVIS DRIVE, SUITE 500 POST OFFICE BOX 13706 RESEARCH TRIANGLE PARK, NC 27709			EXAMINER REAGAN, JAMES A	
			ART UNIT 3621	PAPER NUMBER
			MAIL DATE 03/14/2012	DELIVERY MODE PAPER

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

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

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record

A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews

Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.

All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:

- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:

- 1) A brief description of the nature of any exhibit shown or any demonstration conducted,
- 2) an identification of the claims discussed,
- 3) an identification of the specific prior art discussed,
- 4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
- 5) a brief identification of the general thrust of the principal arguments presented to the examiner,
(The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
- 6) a general indication of any other pertinent matters discussed, and
- 7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.



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.
13/017,823	01/31/2011	DAVID M. GRIGG	4508US1.014033.1145	7401
69603 7590 02/13/2012 MOORE & VAN ALLEN, PLLC FOR BOFA 430 DAVIS DRIVE, SUITE 500 POST OFFICE BOX 13706 RESEARCH TRIANGLE PARK, NC 27709			EXAMINER REAGAN, JAMES A	
			ART UNIT 3621	PAPER NUMBER
			MAIL DATE 02/13/2012	DELIVERY MODE PAPER

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

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

Office Action Summary	Application No. 13/017,823	Applicant(s) GRIGG ET AL.	
	Examiner JAMES A. REAGAN	Art Unit 3621	

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

Period for Reply

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

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

Status

1) ☒ Responsive to communication(s) filed on 01/31/2011.

2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.

3) ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on ____; the restriction requirement and election have been incorporated into this action.

4) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5) ☒ Claim(s) 1-39 is/are pending in the application.

5a) Of the above claim(s) ____ is/are withdrawn from consideration.

6) ☐ Claim(s) ____ is/are allowed.

7) ☒ Claim(s) 1-39 is/are rejected.

8) ☐ Claim(s) ____ is/are objected to.

9) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

10) ☐ The specification is objected to by the Examiner.

11) ☒ The drawing(s) filed on 01/31/2011 is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)	4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. ____.
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)	5) ☐ Notice of Informal Patent Application
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date <u>02/18/2011</u> .	6) ☐ Other: ____.

Art Unit: 3621

DETAILED ACTION

Acknowledgments

1. This action is in reply to the application filed on **01/31/2011**.
2. Claims 1-39 are currently pending and have been examined.

Information Disclosure Statement

3. The Information Disclosure Statement filed on **02/18/2011** has been considered. An initialed copy of the Form 1449 is enclosed herewith.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention

5. Claims 9 and 10 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

6. Claims 9 and 10 recites the limitation *instructions*. There is insufficient antecedent basis for this limitation in the claim.

Art Unit: 3621

Claim Rejections - 35 USC § 103

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

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

8. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

9. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Art Unit: 3621

10. Claims 1-7, 12, 13, 15, 17-26, 28 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fisher et al. (USPGP 2006/0021003 A1), hereinafter **FISHER**, in view of Ziegler (USPGP 2006/0123465 A1), hereinafter **ZEIGLER**.

Claim 1:

FISHER as shown below discloses the following limitations:

- *a memory device;* (see at least paragraphs 0008, 0010, 0011)
- *a communication device;* (see at least paragraphs 0008, 0010, 0011)
- *a processing device coupled to the memory device, wherein the processing device is configured to:* (see at least paragraphs 0008, 0010, 0011)
- *receive a security protocol from a user, the security protocol comprising a permission module and an authentication module;* (see at least paragraphs 0010, 0011, 0012, 0015, 0018)

FISHER does not disclose the following limitations, but **ZEIGLER** as shown does:

- *determine that the user is conducting a transaction;* (see at least paragraphs 0003, 0008, 0010, 0127)
- *compare the transaction with the permission module;* (see at least paragraphs 0003, 0008, 0010, 0127)
- *determine a process for authenticating the user, the determination based on the comparison of the transaction with the permission module.* (see at least paragraphs 0003, 0008, 0010, 0127)

In the competitive business climate, there is a profit-driven motive to maximize the profitability of goods and services that are provided or marketed to customers. Enterprises typically use business planning to make decisions in order to maximize profits. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine/modify the method of **FISHER** with the technique of **ZEIGLER** because, "In any financial transaction, it may be important that the identity of both parties be authenticated in a manner

Art Unit: 3621

which positively establishes the identities of the parties. It may also be important that the transaction be non-reputable, so that neither party can deny their involvement in the transaction at a later date. Traditionally, the authentication of transactions were established principally by face-to-face meetings and handwritten signatures. People could identify each other and experts could attest to the authenticity of handwriting. Authentication was not impervious to fraud, but was strong enough to provide reasonable levels of transactional security.” (ZEIGLER: paragraph 0003)

Claim 2:

The combination of **FISHER/ZEIGLER** discloses the limitations as shown in the rejections above. **FISHER** does not specifically disclose *the processing device is configured to determine the process for authenticating the user by determining if the user must authenticate an identity of the user based on the comparison of the transaction with the permission module, and wherein the processing device is further configured to allow the transaction if the user does not need to authenticate the user's identity.* **ZEIGLER**, however, in at least paragraph 0127 discloses allowing the transaction to proceed if the user is properly authenticated, or preventing the transaction if the user is not properly authenticated. In the competitive business climate, there is a profit-driven motive to maximize the profitability of goods and services that are provided or marketed to customers. Enterprises typically use business planning to make decisions in order to maximize profits. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine/modify the method of **FISHER** with the technique of **ZEIGLER** because, “In any financial transaction, it may be important that the identity of both parties be authenticated in a manner which positively establishes the identities of the parties. It may also be important that the transaction be non-reputable, so that neither party can deny their involvement in the transaction at a later date. Traditionally, the authentication of transactions were established principally by face-to-face meetings and handwritten signatures. People could identify each other and experts could attest to the authenticity of handwriting. Authentication was

Art Unit: 3621

not impervious to fraud, but was strong enough to provide reasonable levels of transactional security.” (**ZEIGLER**: paragraph 0003)

Claim 3:

The combination of **FISHER/ZEIGLER** discloses the limitations as shown in the rejections above. **FISHER** does not specifically disclose:

- *the processing device is further configured to execute computer-readable program code to:*
- *request authentication of the user's identity based on the comparison of the transaction with the permission module;*
- *compare input from the user with the authentication module; and*
- *allow the transaction if the user is authorized to perform the transaction based on the comparison of the input with the authentication module.*

ZEIGLER, however, in at least paragraph 0127 discloses allowing the transaction to proceed if the user is properly authenticated, or preventing the transaction if the user is not properly authenticated. In the competitive business climate, there is a profit-driven motive to maximize the profitability of goods and services that are provided or marketed to customers. Enterprises typically use business planning to make decisions in order to maximize profits. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine/modify the method of **FISHER** with the technique of **ZEIGLER** because, “In any financial transaction, it may be important that the identity of both parties be authenticated in a manner which positively establishes the identities of the parties. It may also be important that the transaction be non-reputable, so that neither party can deny their involvement in the transaction at a later date. Traditionally, the authentication of transactions were established principally by face-to-face meetings and handwritten signatures. People could identify each other and experts could attest to the authenticity of handwriting. Authentication was not impervious to fraud, but

Art Unit: 3621

was strong enough to provide reasonable levels of transactional security.” (ZEIGLER: paragraph 0003)

Art Unit: 3621

Claims 4-7:

The combination of **FISHER/ZEIGLER** discloses the limitations as shown in the rejections above. **FISHER** as shown further discloses:

- *the authentication module comprises at least one security feature. (see at least paragraph 0060)*
- *the at least one security feature is customizable by the user. (see at least paragraph 0060)*
- *the security feature consists of at least one of a username, a password, a challenge question, a voice recognition test, a facial recognition test, a fingerprint identification test, and an iris scan. (see at least paragraph 0010)*
- *the communication device consists of at least one of a keyboard, a scanner, a touchpad, a camera, a speaker, and a microphone. (see at least paragraph 0010)*

Claims 15, 18, 19, 23, and 24:

The combination of **FISHER/ZEIGLER** discloses the limitations as shown in the rejections above. **FISHER** does not specifically disclose:

- *determining that the user is conducting a transaction comprises receiving a signal from a point-of-sale device indicating that the user is attempting to conduct a transaction.*
- *allowing the transaction comprises transferring the user's account information to a point-of-sale device.*
- *the transferring the user's account information to the point-of-sale device comprises wirelessly transferring the account information.*
- *the memory is capable of receiving power from a point-of-sale device.*
- *allowing the transaction if the user is authorized to perform the transaction comprises transferring the user's account information to a point- of-sale device.*

Art Unit: 3621

ZEIGLER, however, in at least paragraph 0011 discloses point-of-sale devices, inherently disclosing the standard functionality and necessary data exchange to facilitate point-of-sale purchases and transactions. In the competitive business climate, there is a profit-driven motive to maximize the profitability of goods and services that are provided or marketed to customers. Enterprises typically use business planning to make decisions in order to maximize profits. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine/modify the method of **FISHER** with the POS device of **ZEIGLER** because, "In any financial transaction, it may be important that the identity of both parties be authenticated in a manner which positively establishes the identities of the parties. It may also be important that the transaction be non-reputable, so that neither party can deny their involvement in the transaction at a later date. Traditionally, the authentication of transactions were established principally by face-to-face meetings and handwritten signatures. People could identify each other and experts could attest to the authenticity of handwriting. Authentication was not impervious to fraud, but was strong enough to provide reasonable levels of transactional security." (**ZEIGLER**: paragraph 0003)

Claim 22:

The combination of **FISHER/ZEIGLER** discloses the limitations as shown in the rejections above. **FISHER** as shown further discloses *the security feature is stored in memory associated with a mobile device*. See at least paragraph 0060.

Claims 12, 13, 17, 20, 21, 25, 26, 28, 29:

The combination of **FISHER/ZEIGLER** discloses the limitations as shown in the rejections of the claims above. The Examiner finds that remaining claims 12, 13, 17, 20, 21, 25, 26, 28, 29 are not patentably distinct from claims 1-7, 15, 18, 19, and 22-24, nor do they produce any new, meaningful, synergetic result that would render the claims novel and therefore, for the

Art Unit: 3621

sake of clarity, has grouped the rejections of claims 1-7 12, 13, 15, 17-26, 28 and 29 accordingly using the same references and citations as above.

11. Claims 8-11, 14, 16, 27, 30-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over **FISHER/ZEIGLER** and further in view of Examiner's **OFFICIAL NOTICE**.

Claims 8-11:

The combination of **FISHER/ZEIGLER** discloses the limitations as shown in the rejections above. **FISHER/ZEIGLER** does not specifically disclose:

- *the permission module comprises instructions on when the user must authenticate the user's identity to perform the transaction.*
- *the instructions are provided by the user.*
- *the instructions are based on a characteristic of the transaction.*
- *the characteristic of the transaction consists of at least one of the dollar amount of the transaction, the identity of the merchant, the category of the expense, the time of the transaction, and the location of the transaction.*

However, the Examiner takes **OFFICIAL NOTICE** that it is old and well known in the OPSEC arts to set standards for ensuring secure transactions. In the competitive business climate, there is a profit-driven motive to maximize the profitability of goods and services that are provided or marketed to customers. Enterprises typically use business planning to make decisions in order to maximize profits. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine/modify the method of **FISHER/ZEIGLER** with the technique of setting specific authentication instructions because in the competitive business climate, there is a profit-driven motive to maximize the profitability of goods and services that are provided or marketed to customers. Enterprises typically use business planning to make decisions in order to maximize profits. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine/modify the method of **FISHER/ZEIGLER**

Art Unit: 3621

with the security standards technique because, "In any financial transaction, it may be important that the identity of both parties be authenticated in a manner which positively establishes the identities of the parties. It may also be important that the transaction be non-reputable, so that neither party can deny their involvement in the transaction at a later date. Traditionally, the authentication of transactions were established principally by face-to-face meetings and handwritten signatures. People could identify each other and experts could attest to the authenticity of handwriting. Authentication was not impervious to fraud, but was strong enough to provide reasonable levels of transactional security." (**ZEIGLER**: paragraph 0003).

Claims 30-33:

The combination of **FISHER/ZEIGLER** discloses the limitations as shown in the rejections above. **FISHER/ZEIGLER** does not specifically disclose:

- *the user's financial account information consists of information associated with at least one of a checking account, a savings account, a money market account, a credit account, an investment account, and a rewards points account.*
- *the permission module requires the user to authenticate the user's identity if a transaction amount is over a predetermined dollar amount.*
- *the permission module requires the user to authenticate the user's identity if the transaction is occurring at a non- approved merchant.*
- *the non-approved merchant is a merchant that the user has not purchased from previously.*

However, the Examiner takes **OFFICIAL NOTICE** that it is old and well known in the online transaction arts to set standards for ensuring secure transactions. In the competitive business climate, there is a profit-driven motive to maximize the profitability of goods and services that are provided or marketed to customers. Enterprises typically use business planning to make decisions in order to maximize profits. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine/modify the method of **FISHER/ZEIGLER**

Art Unit: 3621

with the technique of setting specific authentication instructions because in the competitive business climate, there is a profit-driven motive to maximize the profitability of goods and services that are provided or marketed to customers. Enterprises typically use business planning to make decisions in order to maximize profits. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine/modify the method of **FISHER/ZEIGLER** with the security and accounts standards technique because, "In any financial transaction, it may be important that the identity of both parties be authenticated in a manner which positively establishes the identities of the parties. It may also be important that the transaction be non-reputable, so that neither party can deny their involvement in the transaction at a later date. Traditionally, the authentication of transactions were established principally by face-to-face meetings and handwritten signatures. People could identify each other and experts could attest to the authenticity of handwriting. Authentication was not impervious to fraud, but was strong enough to provide reasonable levels of transactional security." (**ZEIGLER**: paragraph 0003).

Claims 27 and 34-39:

The combination of **FISHER/ZEIGLER** discloses the limitations as shown in the rejections above. **FISHER/ZEIGLER** does not specifically disclose:

- *an executable portion for causing a computer to determine the user's location when the user is conducting the transaction.*
- *the permission module requires the user to authenticate the user's identity if the user has not authenticated the identity within a predetermined time period.*
- *the permission module requires the user to authenticate the user's identity if the user is outside of predetermined geographical areas.*
- *the permission module requires the user to authenticate the user's identity if a transaction amount would lower a balance in the user's account below a predetermined level.*

Art Unit: 3621

- *the permission module requires the user to authenticate the user's identity if the user has already conducted a predetermined number of transactions within a predetermined time period.*
- *allowing the transaction comprises determining an account from which a payment for the transaction is made.*
- *determining the account comprises comparing the transaction to instructions received from the user.*

However, the Examiner takes **OFFICIAL NOTICE** that it is old and well known in the online transaction arts to set standards for ensuring secure transactions. In the competitive business climate, there is a profit-driven motive to maximize the profitability of goods and services that are provided or marketed to customers. Enterprises typically use business planning to make decisions in order to maximize profits. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine/modify the method of **FISHER/ZEIGLER** with the technique of setting specific authentication instructions because in the competitive business climate, there is a profit-driven motive to maximize the profitability of goods and services that are provided or marketed to customers. Enterprises typically use business planning to make decisions in order to maximize profits. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine/modify the method of **FISHER/ZEIGLER** with the security and accounts standards technique because, "In any financial transaction, it may be important that the identity of both parties be authenticated in a manner which positively establishes the identities of the parties. It may also be important that the transaction be non-reputable, so that neither party can deny their involvement in the transaction at a later date. Traditionally, the authentication of transactions were established principally by face-to-face meetings and handwritten signatures. People could identify each other and experts could attest to the authenticity of handwriting. Authentication was not impervious to fraud, but was strong enough to provide reasonable levels of transactional security." (**ZEIGLER**: paragraph 0003).

Claims 14 and 16:

The combination of **FISHER/ZEIGLER** discloses the limitations as shown in the rejections of the claims above. The Examiner finds that remaining claims 14 and 16 are not patentably distinct from claims 8-11 and 30-37, nor do they produce any new, meaningful, synergetic result that would render the claims novel and therefore, for the sake of clarity, has grouped the rejections of claims 8-11, 14, 16, 30-37 accordingly using the same references and citations as above.

CONCLUSION

12. Any inquiry of a general nature or relating to the status of this application or concerning this communication or earlier communications from the Examiner should be directed to **James A. Reagan** (james.reagan@uspto.gov) whose telephone number is **571.272.6710**. The Examiner can normally be reached on Monday-Friday, 9:30am-5:00pm. If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, **ANDREW J. FISCHER** can be reached at **571.272.6779**.

13. Should Applicant desire in the future to receive formal or informal email communications from the Examiner (e.g. acknowledgments, references, courtesy copies of documents, etc.), the electronic file must contain written authorization to conduct email communications. See MPEP §502.03 III. For Applicant's benefit, exemplary language for written authorization is in MPEP §502.03 III. ¶4. The exemplary language is:

Recognizing that Internet communications are not secure, I hereby authorize the USPTO to communicate with me concerning any subject matter of this application by electronic mail. I understand that a copy of these communications will be made of record in the application file.

14. In the situation where Applicant desires to receive email communications from the Examiner, the Examiner suggests placing the above exemplary language in Applicant's next correspondence.

Art Unit: 3621

15. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://portal.uspto.gov/external/portal/pair> . Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at **866.217.9197** (toll-free).

16. Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

Washington, D.C. 20231

or faxed to **571-273-8300**.

17. Hand delivered responses should be brought to the **United States Patent and Trademark Office Customer Service Window**:

Randolph Building

401 Dulany Street

Alexandria, VA 22314.

/James A. Reagan/
Primary Examiner, Art Unit 3621
james.reagan@uspto.gov
571.272.6710 (Office)
571.273.6710 (Desktop Fax)

Notice of References Cited	Application/Control No. 13/017,823		Applicant(s)/Patent Under Reexamination GRIGG ET AL.	
	Examiner JAMES A. REAGAN		Art Unit 3621	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2006/0021003 A1	01-2006	Fisher et al.	726/001
*	B	US-2006/0123465 A1	06-2006	Ziegler, Robert	726/002
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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

Receipt date: 02/18/2011

13017823 - GAU: 3621

Substitute for form 1449/PTO (Revised 07/2005) INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/017,823
				Filing Date	01/31/2011
				First Named Inventor	David M. Grigg, et al.
				Group Art Unit	3621
Examiner Name	To Be Assigned				
Sheet	1	of	1	Attorney Docket Number	4508US1.014033.1145

U. S. PATENT DOCUMENTS					
Examiner Initials*	Cite No.	Document Number Number - Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages of Relevant Figures Appear
		7,071,113 B2	07-04-2006	KIM, ET AL.	

U. S. PATENT APPLICATION DOCUMENTS					
Examiner Initials*	Cite No.	Document Number Number - Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages of Relevant Figures Appear
		2010/0051685 A1	03-04-2010	ROY YURU, ET AL.	
		2010/0125495 A1	05-20-2010	SMITH, ET AL.	

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No.	Foreign Patent Document Country Code - Number Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	English Language Translation Attached

OTHER DOCUMENTS			
Examiner Initials*	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	English Language Translation Attached
		GRIGG, DAVID M., ET AL., US Patent Application No. 13/017,835, Filed 01/31/2011.	

Examiner Signature	/James Reagan/	Date Considered	02/07/2012
--------------------	----------------	-----------------	------------

*Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through 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. /J.R./

EAST Search History**EAST Search History (Prior Art)**

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	20312	(password) and biometric	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/02/09 08:12
S2	2293	S1 and authenticat\$3 and permission and transaction and identity	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/02/09 08:14
S3	11	S2 and "permission module"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/02/09 08:16
S4	5	S3 and (mobile or cell or cellular)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/02/09 08:17
S5	130	S2 and ("permission module" or "authentication module")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/02/09 08:19
S6	102	S5 and (mobile or cell or cellular)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/02/09 08:19
S7	59	S6 and (authenticat\$3 WITH (comparison or compar\$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/02/09 08:55
S8	20312	password and biometric	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/02/09 08:57

2/ 10/ 2012 8:58:59 AM**C:\Users\jreagan\Documents\EAST\Workspaces\13017823.wsp**

Search Notes 	Application/Control No. 13017823	Applicant(s)/Patent Under Reexamination GRIGG ET AL.
	Examiner JAMES A REAGAN	Art Unit 3621

SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
EAST	2/7/2012	JAR

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

--	--



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
13/017,823	01/31/2011	3621	2208	4508US1.014033.1145	39	3

CONFIRMATION NO. 7401

UPDATED FILING RECEIPT



0000000046214700

69603

MOORE & VAN ALLEN, PLLC FOR BOFA
430 DAVIS DRIVE, SUITE 500
POST OFFICE BOX 13706
RESEARCH TRIANGLE PARK, NC 27709

Date Mailed: 02/28/2011

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

DAVID M. GRIGG, Rock Hill, SC;
Patrick B. Kelly, Charlotte, NC;
Alicia C. Jones, Fort Mill, SC;
Marc B. Keller, Charlotte, NC;

Assignment For Published Patent Application

BANK OF AMERICA CORPORATION, Charlotte, NC

Power of Attorney: The patent practitioners associated with Customer Number 69603

Domestic Priority data as claimed by applicant

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.)

Permission to Access - A proper **Authorization to Permit Access to Application by Participating Offices** (PTO/SB/39 or its equivalent) has been received by the USPTO.

If Required, Foreign Filing License Granted: 02/10/2011

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/017,823**

Projected Publication Date: 08/02/2012

Non-Publication Request: No

Early Publication Request: No

Title

MOBILE TRANSACTION DEVICE SECURITY SYSTEM

Preliminary Class

705

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER**Title 35, United States Code, Section 184****Title 37, Code of Federal Regulations, 5.11 & 5.15****GRANTED**

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as

page 2 of 3

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 Assets Control, 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).

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 13/017,823				
APPLICATION AS FILED - PART I										
(Column 1)		(Column 2)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY				
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)			
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	330			
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A	540			
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	220			
TOTAL CLAIMS (37 CFR 1.16(i))	39	minus 20 = * 19				x 52 =	988			
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3	minus 3 = *				x 220 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$270 (\$135 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00			
			TOTAL			TOTAL	2078			
* If the difference in column 1 is less than zero, enter "0" in column 2.										
APPLICATION AS AMENDED - PART II										
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY		
AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=		x	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=		x	=
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
					TOTAL ADD'L FEE				TOTAL ADD'L FEE	
AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=		x	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=		x	=
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
					TOTAL ADD'L FEE				TOTAL ADD'L FEE	
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.										



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/017,823	01/31/2011	DAVID M. GRIGG	4508US1.014033.1145

CONFIRMATION NO. 7401

POA ACCEPTANCE LETTER



OC000000046214551

69603
MOORE & VAN ALLEN, PLLC FOR BOFA
430 DAVIS DRIVE, SUITE 500
POST OFFICE BOX 13706
RESEARCH TRIANGLE PARK, NC 27709

Date Mailed: 02/28/2011

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 02/18/2011.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/hgray/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: David M. Grigg et al. Confirmation No.: 7401
Appl No.: 13/017,823 Group Art Unit: 3621
Filed: January 31, 2011 Examiner: To Be Assigned
Title: **MOBILE TRANSACTION DEVICE SECURITY SYSTEM**

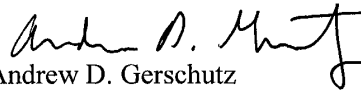
Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSE TO NOTICE TO FILE MISSING PARTS OF APPLICATION

In response to the Notice to File Missing Parts of Application dated February 10, 2011, enclosed are the following:

- ☐ Part 2 of Formalities Letter (Notice to File Missing Parts of Application)
- ☒ Declaration and Power of Attorney for the above-identified application, which has been executed by the named inventor
- ☐ Declaration of Inventors which has been executed by the named inventor(s) and an Assignee Power of Attorney
- ☐ Applicant claims small entity status
- ☒ Fees in the amount of \$130 surcharge under 37 C.F.R. § 1.16(f) are being authorized via EFT when electronically filing
- ☐ English Translation and \$130.00 (37 CFR 1.17(i)) fee for filing late.
- ☐ Other:
- ☒ Any deficiency, additional fee, or credit may be charged to our Deposit Account No. 13-4365.

Respectfully submitted,


Andrew D. Gerschutz
Registration No. 65,529

CUSTOMER NUMBER 69603
MOORE & VAN ALLEN PLLC
430 Davis Drive, Suite 500
Post Office Box 13706
Research Triangle Park, NC 27709
Tel Triangle Office (919) 286-8000
Fax Triangle Office (919) 286-8199

Electronically filed via the EFS-Web Electronic Filing System of the United States Patent and Trademark Office on February 18, 2011.

Doc Code: Oath

Document Description: Oath or declaration filed

PTO/SB/01 (04-09)

Approved for use through 06/30/2010. OMB 0651-0032

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION (37 CFR 1.63)	Attorney Docket Number	4508US1.014033.1145
	First Named Inventor	David M. Grigg
	COMPLETE IF KNOWN	
	Application Number	To Be Assigned
	Filing Date	
	Art Unit	To Be Assigned
	Examiner Name	To Be Assigned

☒ Declaration Submitted With Initial Filing OR ☐ Declaration Submitted After Initial Filing (surcharge (37 CFR 1.16 (f) Required))

I hereby declare that: (1) Each inventor's residence, mailing address, and citizenship are as stated below next to their name; and (2) I believe the inventor(s) named below to be the original and first inventor(s) of the subject matter which is claimed and for which a patent is sought on the invention titled:

MOBILE TRANSACTION DEVICE SECURITY SYSTEM

(Title of the invention)

the application of which

☒ is attached hereto

OR

☐ was filed on (MM/DD/YYYY) _____ as United States Application Number or PCT International

Application Number _____ and was amended on (MM/DD/YYYY) _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified application, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

Authorization To Permit Access To Application by Participating Offices

☒ If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the above-identified patent application is filed access to the above-identified patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the above-identified patent application is filed to have access to the above-identified patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the above-identified patent application with respect to: 1) the above-identified patent application-as-filed; 2) any foreign application to which the above-identified patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the above-identified patent application; and 3) any U.S. application-as-filed from which benefit is sought in the above-identified patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing the Authorization to Permit Access to Application by Participating Offices.

[Page 1 of 7]

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 21 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.

DECLARATION — Utility or Design Patent Application**Claim of Foreign Priority Benefits**

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or (f), or 365(b) of any foreign application(s) for patent, inventor's or plant breeder's rights certificate(s), or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent, inventor's or plant breeder's rights certificate(s), or any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached?	
				YES	NO
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐

☐ Additional foreign application number(s) are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

PTO/SB/01 (04-09)

Approved for use through 06/30/2010. OMB 0651-0032

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

DECLARATION — Utility or Design Patent Application

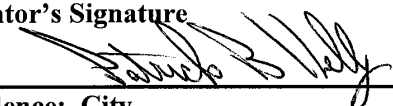
Direct all correspondence to: ☒	The address Associated with Customer Number: 69,603	OR ☐	Correspondence Address below
Name Moore & Van Allen, PLLC			
Address P.O. Box 13706			
City Research Triangle Park		State NC	Zip 27709
Country US	Telephone		Email
<p>WARNING:</p> <p>Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available. Petitioner/applicant is advised that documents which form the record of a patent application (such as the PTO/SB/01) are placed into the Privacy Act system of records DEPARTMENT OF COMMERCE, COMMERCE-PAT-7, System name: Patent Application Files. Documents not retained in an application file (such as the PTO-2038) are placed into the Privacy Act system of COMMERCE/PAT-TM-10, System name: Deposit Accounts and Electronic Funds Transfer Profiles.</p> <p>I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.</p>			
NAME OF SOLE OR FIRST INVENTOR:		☐ A petition has been filed for this unsigned inventor	
Given Name (first and middle [if any]) David M.		Family Name or Surname Grigg	
Inventor's Signature <i>David M. Grigg</i>		Date January 31, 2011	
Residence: City Rock Hill	State SC	Country US	Citizenship US
Mailing Address c/o Bank of America, Mailcode: NC1-002-29-01, 101 S. Tryon Street			
City Charlotte	State NC	Zip 28255	Country US
☒ Additional inventors or a legal representative are being named on the <u>3</u> supplemental sheet(s) PTO/SB/02A or 021.R attached hereto			

(Page 3 of 7)

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

DECLARATION	ADDITIONAL INVENTOR(S) Supplemental Sheet
-------------	---

Page 4 of 7

Name of Additional Joint Inventor, if any:		☐ A petition has been filed for this unsigned inventor	
Given Name (first and middle (if any))		Family Name Or Surname	
Patrick B.		Kelly	
Inventor's Signature 			Date 3 FEB 11
Residence: City	State	Country	Citizenship
Charlotte	NC	US	US
Mailing Address			
c/o Bank of America, Mailcode: NC1-002-29-01, 101 S. Tryon Street			
City	State	Zip	Country
Charlotte	NC	28255	US

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 21 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

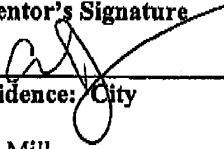
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/02A (07-07)
Approved for use through 06/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

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

DECLARATION	ADDITIONAL INVENTOR(S) Supplemental Sheet
-------------	---

Page 3 of 7

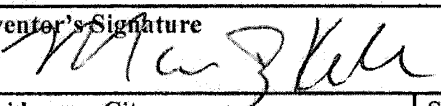
Name of Additional Joint Inventor, if any:	☐ A petition has been filed for this unsigned inventor		
Given Name (first and middle [if any])	Family Name Or Surname		
Alicia C.	Jones		
Inventor's Signature 			Date 1/27/11
Residence: City	State	Country	Citizenship
Fort Mill	SC	US	US
Mailing Address			
c/o Bank of America, Mailcode: NC1-002-29-01, 101 S. Tryon Street			
City	State	Zip	Country
Charlotte	NC	28255	US

This collection of information is required by 36 U.S.C. 116 and 37 CFR 1.83. 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 36 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 21 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 1460, Alexandria, VA 22313-1460. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1460, Alexandria, VA 22313-1460.

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

DECLARATION	ADDITIONAL INVENTOR(S) Supplemental Sheet
-------------	--

Page 6 of 7

Name of Additional Joint Inventor, if any:		☐ A petition has been filed for this unsigned inventor	
Given Name (first and middle [if any])		Family Name Or Surname	
Marc B.		Keller	
Inventor's Signature 		Date 1/31/11	
Residence: City	State	Country	Citizenship
Charlotte	NC	US	US
Mailing Address			
c/o Bank of America, Mailcode: NC1-002-29-01, 101 S. Tryon Street			
City	State	Zip	Country
Charlotte	NC	28255	US

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 21 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.

[Page 7 of 7]

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re United States Patent Application of:

Applicant: David M. Grigg

Application No.: 13/017,823

Date Filed: January 31, 2011

Title: MOBILE TRANSACTION
DEVICE SECURITY SYSTEM

Docket No.: 4508US1.014033.1145

Examiner: Not Yet Assigned

Art Unit: 3621

Conf. No.: 7401

Customer No.:

69,603

INFORMATION DISCLOSURE STATEMENT

Mail Stop Amendment
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

Pursuant to 37 C.F.R. §1.56, the attention of the Patent and Trademark Office is hereby directed to the reference(s) listed on the attached PTO/SB/08A. One copy of each reference is attached. It is respectfully requested that the information be expressly considered during the prosecution of this application, and that the reference(s) be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

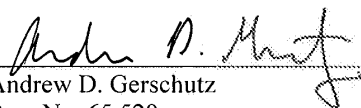
- ☒ 1. This Information Disclosure Statement is being filed within three months of the U.S. filing date OR before the mailing date of a first Office Action on the merits. No certification or fee is required.
- ☐ 2. This Information Disclosure Statement is being filed more than three months after the U.S. filing date AND after the mailing date of the first Office Action on the merits, but before the mailing date of a Final Rejection or Notice of Allowance.
- ☐ a. I hereby certify that each item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Information Disclosure Statement. 37 C.F.R. §1.97(e)(1).

TRI1\755490v1

- ☐ b. I hereby certify that no item of information in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application and, to my knowledge after making reasonable inquiry, was known to any individual designated in 37 CFR §1.56(c) more than three months prior to the filing of this Information Disclosure Statement. 37 C.F.R. §1.97(e)(2).
- ☐ c. Included is our EFT in the amount of **\$180.00** in payment of the fee under 37 C.F.R. §1.17(p). Please credit or debit Deposit Account No. 13-4365 as needed to ensure consideration of the disclosed information. Two duplicate copies of this paper are attached.
- ☐ 3. This Information Disclosure Statement is being filed more than three months after the U.S. filing date and after the mailing date of a Final Rejection or Notice of Allowance, but before payment of the Issue Fee. Applicant(s) hereby petition(s) that the Information Disclosure Statement be considered. Attached is our check no. _____ in the amount of \$180.00 in payment of the petition fee under 37 C.F.R. §1.17(p). Please credit or debit Deposit Account No. _____ as needed to ensure consideration of the disclosed information. Two duplicate copies of this paper are attached.
- ☐ a. I hereby certify that each item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Information Disclosure Statement. 37 C.F.R. §1.97(e)(1).
- ☐ b. I hereby certify that no item of information in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application or, to my knowledge after making reasonable inquiry, was known to any individual designated in 37 CFR §1.56(c) more than three months prior to the filing of this Information Disclosure Statement. 37 C.F.R. §1.97(e)(2).

Respectfully submitted,

Date: February 18, 2011



Andrew D. Gerschütz

Reg. No. 65,529

Attorney for Applicant

Moore & Van Allen, PLLC

Telephone: (919) 286-8000

Facsimile: (919) 286-8199

Substitute for form 1449/PTO (Revised 07/2005) INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/017,823
				Filing Date	01/31/2011
				First Named Inventor	David M. Grigg, et al.
				Group Art Unit	3621
Examiner Name	To Be Assigned				
Sheet	1	of	1	Attorney Docket Number	4508US1.014033.1145

U. S. PATENT DOCUMENTS					
Examiner Initials*	Cite No.	<u>Document Number</u> Number - Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages of Relevant Figures Appear
		7,071,113 B2	07-04-2006	KIM, ET AL.	

U. S. PATENT APPLICATION DOCUMENTS					
Examiner Initials*	Cite No.	<u>Document Number</u> Number - Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages of Relevant Figures Appear
		2010/0051685 A1	03-04-2010	ROY YURU, ET AL.	
		2010/0125495 A1	05-20-2010	SMITH, ET AL.	

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No.	<u>Foreign Patent Document</u> Country Code - Number Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	English Language Translation Attached

OTHER DOCUMENTS			
Examiner Initials*	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	English Language Translation Attached
		GRIGG, DAVID M., ET AL., US Patent Application No. 13/017,835, Filed 01/31/2011.	

Examiner Signature		Date Considered	
-----------------------	--	--------------------	--

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

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(b).

I hereby appoint:

☒ Practitioners associated with the Customer Number:

69603

OR

☐ Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

as attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(b).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(b) to:

☒ The address associated with Customer Number:

69603

OR

☐ Firm or Individual Name			
Address			
City	State	Zip	
Country			
Telephone			Email

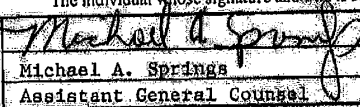
Assignee Name and Address:

Bank of America Corporation
101 South Tryon Street
Charlotte, NC 28255

A copy of this form, together with a statement under 37 CFR 3.73(b) (Form PTO/SB/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(b) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE OF Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee:

Signature		Date	6/7/07
Name	Michael A. Springs	Telephone	704-388-6952
Title	Assistant General Counsel		

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

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

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(b)Applicant/Patent Owner: BANK OF AMERICA CORPORATIONApplication No./Patent No.: 13/017,823Filed/Issue Date: 01/31/2011Titled: MOBILE TRANSACTION DEVICE SECURITY SYSTEMBANK OF AMERICA CORPORATION, a corporation

(Name of Assignee)

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

states that it is:

1. ☒ the assignee of the entire right, title, and interest in;
2. ☐ an assignee of less than the entire right, title, and interest in
(The extent (by percentage) of its ownership interest is _____ %); or
3. ☐ the assignee of an undivided interest in the entirety of (a complete assignment from one of the joint inventors was made)

the patent application/patent identified above, by virtue of either:

- 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 therefore is attached.

OR

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

1. 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.

2. 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.

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.

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

- ☒ As required by 37 CFR 3.73(b)(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.

Signature

Date

Andrew D. Gerschutz

Attorney of Record

Printed or Typed Name

Title

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.

ASSIGNMENT

WHEREAS, I, David M. Grigg ("Assignor"), a citizen of the United States of America, residing in Rock Hill, South Carolina, have invented certain new and useful inventions entitled "MOBILE TRANSACTION DEVICE SECURITY SYSTEM". If the following lines are blank, the above application was filed on even date herewith, otherwise, to comply with 37 C.F.R. §3.21 for recordal of this assignment, I, an assignor below, hereby authorize the attorneys for Bank of America to insert the filing date and application number below after they become known and prior to filing the recordation. U.S. Application No.

13/017,823

filed

January 31, 2011

WHEREAS, BANK OF AMERICA CORPORATION ("Assignee"), a Corporation duly organized under the laws of the State of Delaware, and having its offices and place of business at Charlotte, North Carolina, is desirous of acquiring the entire right, title and interest in and to the aforesaid inventions and in and to all applications and Letters Patent therefor granted in the United States of America, and in any and all countries foreign thereto:

NOW, THEREFORE, TO WHOM IT MAY CONCERN, be it known that, for good and valuable consideration, including salary or payment for the making of inventions, or employee benefits, the receipt and sufficiency of which is hereby acknowledged, I said Assignor, by these presents do sell, assign and transfer unto said Assignee, its successors, assigns and legal representatives, the full and exclusive right, title and interest for the territory of the United States of America and all countries foreign thereto, and throughout the world and in space, (including the right to apply for Letters Patent in foreign countries in its own name and to claim any priority rights for such foreign applications to which such applications are entitled under international conventions, treaties, or otherwise), in and to said inventions and in and to all applications and Letters Patent granted therefor, and all non-provisionals, divisions, reissues, continuations and extensions thereof, and in and to all copyrights, trademarks with their associated goodwill, trade secrets, confidential information, and compilations, necessary or useful to make, use, or sell the inventions. I hereby authorize and request the Commissioner of Patents, and any official whose duty it is to issue patents, to issue all Letters Patent on said inventions or resulting therefrom to said Assignee, or its successors and assigns, as assignee of the entire right, title and interest. I represent and warrant that I have full right to agree to, execute, and deliver this assignment. I agree that I will without further consideration, but at the expense of Assignee, communicate to said Assignee, or its successors, assigns, or nominees, any and all facts known to me regarding said inventions whenever requested, and that I will execute all non-provisional, divisional, reissue and continuation applications, testify in any legal proceedings, sign all lawful papers, make all rightful oaths, and generally do everything reasonable for said Assignee, its successors, assigns, and nominees, to obtain and enforce proper patent protection for said inventions in all countries.

IN WITNESS WHEREOF, I have hereunto set my hand and seal this 31 day of January, 2011

David M. Grigg
DAVID M. GRIGG, Assignor

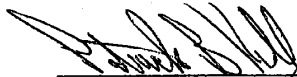
ASSIGNMENT

WHEREAS, I, Patrick B. Kelly ("Assignor"), a citizen of the United States of America, residing in Charlotte, North Carolina, have invented certain new and useful inventions entitled "MOBILE TRANSACTION DEVICE SECURITY SYSTEM". If the following lines are blank, the above application was filed on even date herewith, otherwise, to comply with 37 C.F.R. §3.21 for recordal of this assignment, I, an assignor below, hereby authorize the attorneys for Bank of America to insert the filing date and application number below after they become known and prior to filing the recordation. U.S. Application No. 13/017,823 filed January 31, 2011.

WHEREAS, BANK OF AMERICA CORPORATION ("Assignee"), a Corporation duly organized under the laws of the State of Delaware, and having its offices and place of business at Charlotte, North Carolina, is desirous of acquiring the entire right, title and interest in and to the aforesaid inventions and in and to all applications and Letters Patent therefor granted in the United States of America, and in any and all countries foreign thereto:

NOW, THEREFORE, TO WHOM IT MAY CONCERN, be it known that, for good and valuable consideration, including salary or payment for the making of inventions, or employee benefits, the receipt and sufficiency of which is hereby acknowledged, I said Assignor, by these presents do sell, assign and transfer unto said Assignee, its successors, assigns and legal representatives, the full and exclusive right, title and interest for the territory of the United States of America and all countries foreign thereto, and throughout the world and in space, (including the right to apply for Letters Patent in foreign countries in its own name and to claim any priority rights for such foreign applications to which such applications are entitled under international conventions, treaties, or otherwise), in and to said inventions and in and to all applications and Letters Patent granted therefor, and all non-provisionals, divisions, reissues, continuations and extensions thereof, and in and to all copyrights, trademarks with their associated goodwill, trade secrets, confidential information, and compilations, necessary or useful to make, use, or sell the inventions. I hereby authorize and request the Commissioner of Patents, and any official whose duty it is to issue patents, to issue all Letters Patent on said inventions or resulting therefrom to said Assignee, or its successors and assigns, as assignee of the entire right, title and interest. I represent and warrant that I have full right to agree to, execute, and deliver this assignment. I agree that I will without further consideration, but at the expense of Assignee, communicate to said Assignee, or its successors, assigns, or nominees, any and all facts known to me regarding said inventions whenever requested, and that I will execute all non-provisional, divisional, reissue and continuation applications, testify in any legal proceedings, sign all lawful papers, make all rightful oaths, and generally do everything reasonable for said Assignee, its successors, assigns, and nominees, to obtain and enforce proper patent protection for said inventions in all countries.

IN WITNESS WHEREOF, I have hereunto set my hand and seal this 3 day of FEBRUARY, 2011.


 PATRICK B. KELLY, Assignor

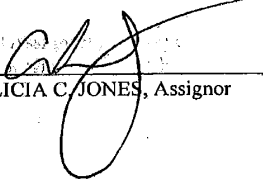
ASSIGNMENT

WHEREAS, I, Alicia C. Jones ("Assignor"), a citizen of the United States of America, residing in Fort Mill, South Carolina, have invented certain new and useful inventions entitled "MOBILE TRANSACTION DEVICE SECURITY SYSTEM". If the following lines are blank, the above application was filed on even date herewith, otherwise, to comply with 37 C.F.R. §3.21 for recordal of this assignment, I, an assignor below, hereby authorize the attorneys for Bank of America to insert the filing date and application number below after they become known and prior to filing the recordation. U.S. Application No. 13/017,823 filed January 31, 2011

WHEREAS, BANK OF AMERICA CORPORATION ("Assignee"), a Corporation duly organized under the laws of the State of Delaware, and having its offices and place of business at Charlotte, North Carolina, is desirous of acquiring the entire right, title and interest in and to the aforesaid inventions and in and to all applications and Letters Patent therefor granted in the United States of America, and in any and all countries foreign thereto:

NOW, THEREFORE, TO WHOM IT MAY CONCERN, be it known that, for good and valuable consideration, including salary or payment for the making of inventions, or employee benefits, the receipt and sufficiency of which is hereby acknowledged, I said Assignor, by these presents do sell, assign and transfer unto said Assignee, its successors, assigns and legal representatives, the full and exclusive right, title and interest for the territory of the United States of America and all countries foreign thereto, and throughout the world and in space, (including the right to apply for Letters Patent in foreign countries in its own name and to claim any priority rights for such foreign applications to which such applications are entitled under international conventions, treaties, or otherwise), in and to said inventions and in and to all applications and Letters Patent granted therefor, and all non-provisionals, divisions, reissues, continuations and extensions thereof, and in and to all copyrights, trademarks with their associated goodwill, trade secrets, confidential information, and compilations, necessary or useful to make, use, or sell the inventions. I hereby authorize and request the Commissioner of Patents, and any official whose duty it is to issue patents, to issue all Letters Patent on said inventions or resulting therefrom to said Assignee, or its successors and assigns, as assignee of the entire right, title and interest. I represent and warrant that I have full right to agree to, execute, and deliver this assignment. I agree that I will without further consideration, but at the expense of Assignee, communicate to said Assignee, or its successors, assigns, or nominees, any and all facts known to me regarding said inventions whenever requested, and that I will execute all non-provisional, divisional, reissue and continuation applications, testify in any legal proceedings, sign all lawful papers, make all rightful oaths, and generally do everything reasonable for said Assignee, its successors, assigns, and nominees, to obtain and enforce proper patent protection for said inventions in all countries.

IN WITNESS WHEREOF, I have hereunto set my hand and seal this 27th day of Jan, 2011.


ALICIA C. JONES, Assignor

ASSIGNMENT

WHEREAS, I, Marc B. Keller ("Assignor"), a citizen of the United States of America, residing in Charlotte, North Carolina, have invented certain new and useful inventions entitled "MOBILE TRANSACTION DEVICE SECURITY SYSTEM". If the following lines are blank, the above application was filed on even date herewith, otherwise, to comply with 37 C.F.R. §3.21 for recordal of this assignment, I, an assignor below, hereby authorize the attorneys for Bank of America to insert the filing date and application number below after they become known and prior to filing the recordation. U.S. Application No. _____ 13/017,823 filed January 31, 2011

WHEREAS, BANK OF AMERICA CORPORATION ("Assignee"), a Corporation duly organized under the laws of the State of Delaware, and having its offices and place of business at Charlotte, North Carolina, is desirous of acquiring the entire right, title and interest in and to the aforesaid inventions and in and to all applications and Letters Patent therefor granted in the United States of America, and in any and all countries foreign thereto;

NOW, THEREFORE, TO WHOM IT MAY CONCERN, be it known that, for good and valuable consideration, including salary or payment for the making of inventions, or employee benefits, the receipt and sufficiency of which is hereby acknowledged, I said Assignor, by these presents do sell, assign and transfer unto said Assignee, its successors, assigns and legal representatives, the full and exclusive right, title and interest for the territory of the United States of America and all countries foreign thereto, and throughout the world and in space, (including the right to apply for Letters Patent in foreign countries in its own name and to claim any priority rights for such foreign applications to which such applications are entitled under international conventions, treaties, or otherwise), in and to said inventions and in and to all applications and Letters Patent granted therefor, and all non-provisionals, divisions, reissues, continuations and extensions thereof, and in and to all copyrights, trademarks with their associated goodwill, trade secrets, confidential information, and compilations, necessary or useful to make, use, or sell the inventions. I hereby authorize and request the Commissioner of Patents, and any official whose duty it is to issue patents, to issue all Letters Patent on said inventions or resulting therefrom to said Assignee, or its successors and assigns, as assignee of the entire right, title and interest. I represent and warrant that I have full right to agree to, execute, and deliver this assignment. I agree that I will without further consideration, but at the expense of Assignee, communicate to said Assignee, or its successors, assigns, or nominees, any and all facts known to me regarding said inventions whenever requested, and that I will execute all non-provisional, divisional, reissue and continuation applications, testify in any legal proceedings, sign all lawful papers, make all rightful oaths, and generally do everything reasonable for said Assignee, its successors, assigns, and nominees, to obtain and enforce proper patent protection for said inventions in all countries.

IN WITNESS WHEREOF, I have hereunto set my hand and seal this 28 day of January, 20 11.

Marc B. Keller
MARC B. KELLER, Assignor

Electronic Patent Application Fee Transmittal				
Application Number:		13017823		
Filing Date:		31-Jan-2011		
Title of Invention:		MOBILE TRANSACTION DEVICE SECURITY SYSTEM		
First Named Inventor/Applicant Name:		DAVID M. GRIGG		
Filer:		Andrew D. Gerschutz/LaKeisha Preddie		
Attorney Docket Number:		4508US1.014033.1145		
Filed as Large Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Late filing fee for oath or declaration	1051	1	130	130
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				130

Electronic Acknowledgement Receipt	
EFS ID:	9477576
Application Number:	13017823
International Application Number:	
Confirmation Number:	7401
Title of Invention:	MOBILE TRANSACTION DEVICE SECURITY SYSTEM
First Named Inventor/Applicant Name:	DAVID M. GRIGG
Customer Number:	69603
Filer:	Andrew D. Gerschutz
Filer Authorized By:	
Attorney Docket Number:	4508US1.014033.1145
Receipt Date:	18-FEB-2011
Filing Date:	31-JAN-2011
Time Stamp:	14:45:16
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Electronic Funds Transfer
Payment was successfully received in RAM	\$ 130
RAM confirmation Number	984
Deposit Account	
Authorized User	

File Listing:

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

1	Miscellaneous Incoming Letter	Transmittal.pdf	53961	no	1
			0cb867d7775d8901443a2a8ee51c46f50921e59		
Warnings:					
Information:					
2	Applicant Response to Pre-Exam Formalities Notice	Response_to_Missing_Parts.pdf	40228	no	1
			0df80916c663eeb8667943a57dda13eb7f70f02d		
Warnings:					
Information:					
3	Oath or Declaration filed	Executed_Declaration.pdf	376171	no	7
			314eefdde07b607ce9b1ca3fd07ab9f85e312e3c		
Warnings:					
Information:					
4	Transmittal Letter	Submission_IDS.pdf	234699	no	2
			914ac7def08253ecd10fb455c3f8efb114b29099		
Warnings:					
Information:					
5	Information Disclosure Statement (IDS) Filed (SB/08)	IDS.pdf	116784	no	1
			427f53c917089ea5c4a78e665e08d5f081133dc4		
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
6	Power of Attorney	PoA.pdf	82855	no	1
			a5e8810f056b7e4a35bfb153292d8e99df90ea6		
Warnings:					
Information:					
7	Assignee showing of ownership per 37 CFR 3.73(b).	Statement.pdf	303236	no	5
			ebfa90105f648e7534900779213a4a672ce677e8		
Warnings:					
Information:					
8	Fee Worksheet (PTO-875)	fee-info.pdf	30150	no	2
			0e12aee1d56dc0bb5385cf87bbfdfa693e69b6c9		
Warnings:					
Information:					
Total Files Size (in bytes):			1238084		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

Doc Code: TRAN.LET

Document Description: Transmittal Letter

PTO/SB/21 (07-09)

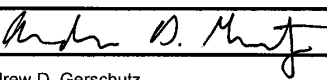
Approved for use through 07/31/2012. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

TRANSMITTAL FORM (to be used for all correspondence after initial filing)	Application Number	13/017,823	
	Filing Date	01/31/2011	
	First Named Inventor	David M. Grigg	
	Art Unit	3621	
	Examiner Name	TBA	
Total Number of Pages in This Submission	18	Attorney Docket Number	4508US1.014033.1145

ENCLOSURES (Check all that apply)		
☐ Fee Transmittal Form ☐ Fee Attached ☐ Amendment/Reply ☐ After Final ☐ Affidavits/declaration(s) ☐ Extension of Time Request ☐ Express Abandonment Request ☒ Information Disclosure Statement ☐ Certified Copy of Priority Document(s) ☒ Reply to Missing Parts/Incomplete Application ☒ Reply to Missing Parts under 37 CFR 1.52 or 1.53	☐ Drawing(s) ☐ Licensing-related Papers ☐ Petition ☐ Petition to Convert to a Provisional Application ☒ Power of Attorney, Revocation Change of Correspondence Address ☐ Terminal Disclaimer ☐ Request for Refund ☐ CD, Number of CD(s) _____ ☐ Landscape Table on CD	☐ After Allowance Communication to TC ☐ Appeal Communication to Board of Appeals and Interferences ☐ Appeal Communication to TC (Appeal Notice, Brief, Reply Brief) ☐ Proprietary Information ☐ Status Letter ☐ Other Enclosure(s) (please identify below):
Remarks		

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT		
Firm Name	MOORE & VAN ALLEN, PLLC	
Signature		
Printed name	Andrew D. Gerschütz	
Date	02/18/2011	Reg. No. 65,529

CERTIFICATE OF TRANSMISSION/MAILING		
I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:		
Signature		
Typed or printed name		Date

This collection of information is required by 37 CFR 1.5. 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 2 hours 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.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 13/017,823				
APPLICATION AS FILED - PART I										
(Column 1)		(Column 2)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY				
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)			
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	330			
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A	540			
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	220			
TOTAL CLAIMS (37 CFR 1.16(i))	39	minus 20 = *	19			x 52 =	988			
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3	minus 3 = *				x 220 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$270 (\$135 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00			
				TOTAL		TOTAL	2078			
* If the difference in column 1 is less than zero, enter "0" in column 2.										
APPLICATION AS AMENDED - PART II										
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY		
AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=		x	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=		x	=
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
						TOTAL ADD'L FEE			TOTAL ADD'L FEE	
AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=		x	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=		x	=
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
						TOTAL ADD'L FEE			TOTAL ADD'L FEE	
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.										



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/017,823	01/31/2011	DAVID M. GRIGG	4508US1.014033.1145

CONFIRMATION NO. 7401

FORMALITIES LETTER



0000000045948674

69603

MOORE & VAN ALLEN, PLLC FOR BOFA
430 DAVIS DRIVE, SUITE 500
POST OFFICE BOX 13706
RESEARCH TRIANGLE PARK, NC 27709

Date Mailed: 02/10/2011

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The oath or declaration is missing.

A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.

Note: If a petition under 37 CFR 1.47 is being filed, an oath or declaration in compliance with 37 CFR 1.63 signed by all available joint inventors, or if no inventor is available by a party with sufficient proprietary interest, is required.

The applicant needs to satisfy supplemental fees problems indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- A surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.16(f) of **\$130** for a non-small entity, must be submitted.

SUMMARY OF FEES DUE:

Total fee(s) required within **TWO MONTHS** from the date of this Notice is **\$130** for a non-small entity

- **\$130** Surcharge.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.

<https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html>

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at <http://www.uspto.gov/ebc>.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

/spathammavong/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO.	TOT CLAIMS	IND CLAIMS
13/017,823	01/31/2011	3621	2078	4508US1.014033.1145	39	3

CONFIRMATION NO. 7401

69603

MOORE & VAN ALLEN, PLLC FOR BOFA
430 DAVIS DRIVE, SUITE 500
POST OFFICE BOX 13706
RESEARCH TRIANGLE PARK, NC 27709

FILING RECEIPT



0000000045948672

Date Mailed: 02/10/2011

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

DAVID M. GRIGG, Rock Hill, SC;
Patrick B. Kelly JR., Charlotte, NC;
Alicia C. Jones, Fort Mill, SC;
Marc B. Keller, Charlotte, NC;

Assignment For Published Patent Application

BANK OF AMERICA CORPORATION, Charlotte, NC

Power of Attorney: None

Domestic Priority data as claimed by applicant

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.)

If Required, Foreign Filing License Granted: 02/10/2011

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/017,823**

Projected Publication Date: To Be Determined - pending completion of Missing Parts

Non-Publication Request: No

Early Publication Request: No

Title

MOBILE TRANSACTION DEVICE SECURITY SYSTEM

Preliminary Class

705

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER**Title 35, United States Code, Section 184****Title 37, Code of Federal Regulations, 5.11 & 5.15****GRANTED**

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as

page 2 of 3

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 Assets Control, 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).

UTILITY PATENT APPLICATION TRANSMITTAL (Only for new nonprovisional applications under 37 CFR 1.53(b))	Attorney Docket No 4508US1.014033.1145
	First Named Inventor David M. Grigg et al.
	Title MOBILE TRANSACTION DEVICE SECURITY SYSTEM
	Filed via EFS-Web on January 31, 2011

ADDRESS TO: **COMMISSIONER FOR PATENTS**
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

Transmitted herewith for filing in the United States Patent Office is a patent application for:

Inventors: David M. Grigg; Patrick B. Kelly; Alicia C. Jones; Marc B. Keller

Assignee of this invention is Bank of America Corporation

1. ☒ The Filing Fee has been calculated as shown below:
 2. ☐ No Applicant claims Small Entity Status. See 37 CFR 1.27.

		Small Entity Rate		Large Entity Rate	
		Fee		Fee	
No. Filed	No. Extra				
BASIC FEE		\$ 0		\$ 330	
SEARCH FEE		\$ 0		\$ 540	
EXAMINATION FEE		\$ 0		\$ 220	
TOTAL CLAIMS:	39 - 20 = 19	X 26 =	\$ 0	19 x 52 =	\$ 988
INDEP CLAIMS:	3 - 3 = 0	X 110 =	\$ 0	0 x 220 =	\$ 0
APPLICATION SIZE FEE	If the specification, drawings, and sequence listing exceed 100 sheets of paper, the application size fee due is \$270 (\$135 for small entity) for each additional 50 sheets or fraction thereof.	\$ 0		\$ 0	
No MULTIPLE DEPENDENT CLAIMS PRESENTED		+195 =	\$ 0	+390 =	\$ 0
*If the difference in Column 1 is less than zero, enter "0" in Column 2.		TOTAL	\$ 0	TOTAL	\$2,078

The Commissioner is hereby authorized to credit any overpayment or charge any deficiency of the following fees to Deposit Acct. No. 13-4365.

- a. ☐ Fees required under 37 CFR 1.16 (National filing fees).
 b. ☐ Fees required under 37 CFR 1.17 (National application processing fees) including any extension of time fees under 37 CFR § 1.136(a) that are required for consideration of papers filed during prosecution.
- ☐ A check in the amount of \$ for the filing fee is enclosed.
- ☒ The filing fees paid via EFT in the amount of \$2,078.00 when e-filing.
- ☐ The above filing fee will be paid along with Applicant(s) Response to the Notice to File Missing Parts.
3. ☒ Specification [Total Pages 38]

4. ☒ 9 Sheets of Drawing(s) (35 USC 113)
5. ☐ Declaration [Total Pages]
- a. ☐ Newly executed (original or copy)
- b. ☐ Copy from a prior application (37 CFR 1.63(d)) (if box 18 completed)
- i. ☐ DELETION OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) & 1.33(b).
6. ☒ Application Data Sheet. See 37 CFR 1.76
7. ☐ CD-ROM or CD-R in duplicate, large table or Computer Program (Appendix)
8. Nucleotide and/or Amino Acid Sequence Submission (if applicable, all necessary)
- a. ☐ Computer Readable Copy (CRF)
- b. ☐ Request for Transfer of Computer Readable Form of Sequence Listing under 37 CFR § 1.821(e) and MPEP 2422.05 (must be compliant with new rules)
- c. ☐ Specification Sequence Listing on:
- i. ☐ CD-ROM or CD-R (3 copies); or
- ii. ☐ Paper (Pages)
- d. ☐ Statements verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

9. ☐ Assignment Papers (cover sheet & document(s) including a check for the \$40.00 fee)
10. ☐ 37 CFR 3.73(b) Statement and General Power of Attorney by Assignee. OR
☐ Application Specific Power of Attorney by Assignee
11. ☐ English Translation Document (if applicable)
12. ☐ Information Disclosure Statement (IDS)/PTO-1449; Copies of IDS Citations
13. ☐ Preliminary Amendment
14. ☐ Return Receipt Postcard (MPEP 503) (Should be specifically itemized)
15. ☐ Certified Copy of Priority Document(s) (if foreign priority is claimed)
☐ Foreign Priority is claimed as Application No. , filed
16. ☐ NonPublication Request under 35 U.S.C. 122(b)(2)(B)(i).
Applicant **must** attach form PTO/SB35 or its equivalent.
17. ☐ Request for Early Publication Under 37 CFR § 1.219. Fee of \$300.00 is enclosed.
18. **If a CONTINUING APPLICATION, check appropriate box and supply the requisite information below and in a preliminary amendment, or in an Application Data Sheet under 37 CFR 1.76:**
- ☐ Continuation ☐ Divisional ☐ Continuation in Part (CIP)

of prior Application No: _____; Filed _____

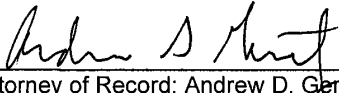
Prior Application Information: Examiner _____

Group/Art Unit: _____

For CONTINUATION or DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 5b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

19. **CORRESPONDENCE ADDRESS**
CUSTOMER NUMBER 69603

Signature:


Attorney of Record: Andrew D. Gerschütz
Registration No. 65,529

January 31, 2011

MOORE & VAN ALLEN PLLC FOR BOFA

430 Davis Drive, Suite 500
Post Office Box 13706
Research Triangle Park, NC 27709
Tel Triangle Office (919) 286-8000
Fax Triangle Office (919) 286-8199

Electronically filed via the EFS-Web Electronic Filing System of the United States Patent and Trademark Office on January 31, 2011.

Electronic Patent Application Fee Transmittal				
Application Number:				
Filing Date:				
Title of Invention:		MOBILE TRANSACTION DEVICE SECURITY SYSTEM		
First Named Inventor/Applicant Name:		DAVID M. GRIGG		
Filer:		Andrew D. Gerschutz		
Attorney Docket Number:		4508US1.014033.1145		
Filed as Large Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Utility application filing	1011	1	330	330
Utility Search Fee	1111	1	540	540
Utility Examination Fee	1311	1	220	220
Pages:				
Claims:				
Claims in excess of 20	1202	19	52	988
Miscellaneous-Filing:				
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				2078

Electronic Acknowledgement Receipt	
EFS ID:	9341761
Application Number:	13017823
International Application Number:	
Confirmation Number:	7401
Title of Invention:	MOBILE TRANSACTION DEVICE SECURITY SYSTEM
First Named Inventor/Applicant Name:	DAVID M. GRIGG
Customer Number:	69603
Filer:	Andrew D. Gerschutz
Filer Authorized By:	
Attorney Docket Number:	4508US1.014033.1145
Receipt Date:	31-JAN-2011
Filing Date:	
Time Stamp:	16:51:05
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Electronic Funds Transfer
Payment was successfully received in RAM	\$ 2078
RAM confirmation Number	4285
Deposit Account	
Authorized User	

File Listing:

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

1	Drawings-only black and white line drawings	Figures.pdf	422834 16d4ec9227abfcfb7c74f27f98a8fae4059c44871	no	9
Warnings:					
Information:					
2		Specification.pdf	208700 61e49c7dcfaeef5c69b7c10287026c6037e037f	yes	38
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Specification		1	30	
	Claims		31	37	
	Abstract		38	38	
Warnings:					
Information:					
3	Application Data Sheet	signed_ADS.pdf	277328 5a2ef999a032ea1b563603d0d87df9d20ae05253	no	5
Warnings:					
Information:					
This is not an USPTO supplied ADS fillable form					
4	Transmittal of New Application	signed_transmittal.pdf	103571 b6dba3a8b8ea36da5c3b1b786a0265b0d43f5d7b	no	3
Warnings:					
Information:					
5	Fee Worksheet (PTO-875)	fee-info.pdf	36714 793e203ac611643f9f4fcb43988de52a41b04ce8	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			1049147		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

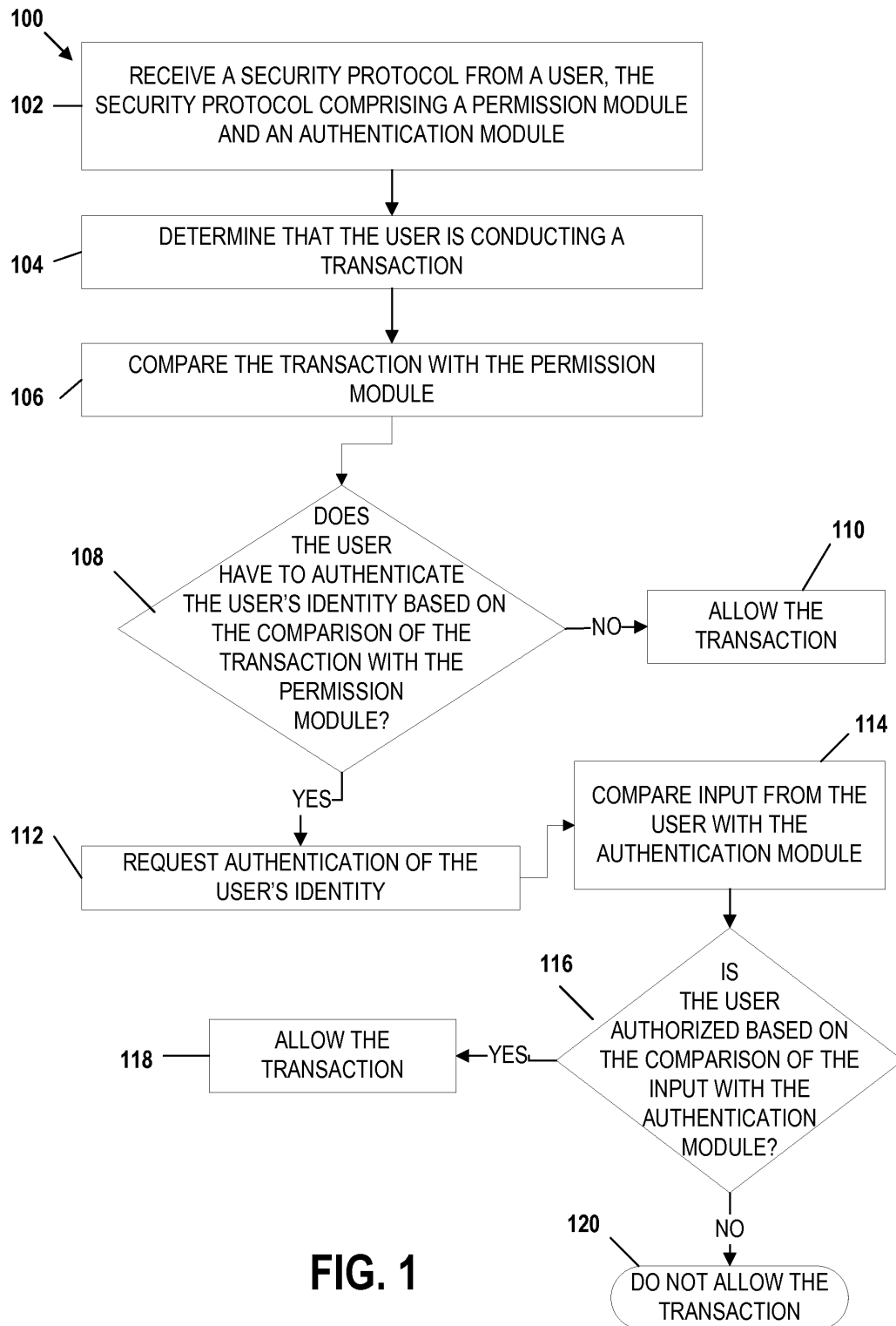


FIG. 1

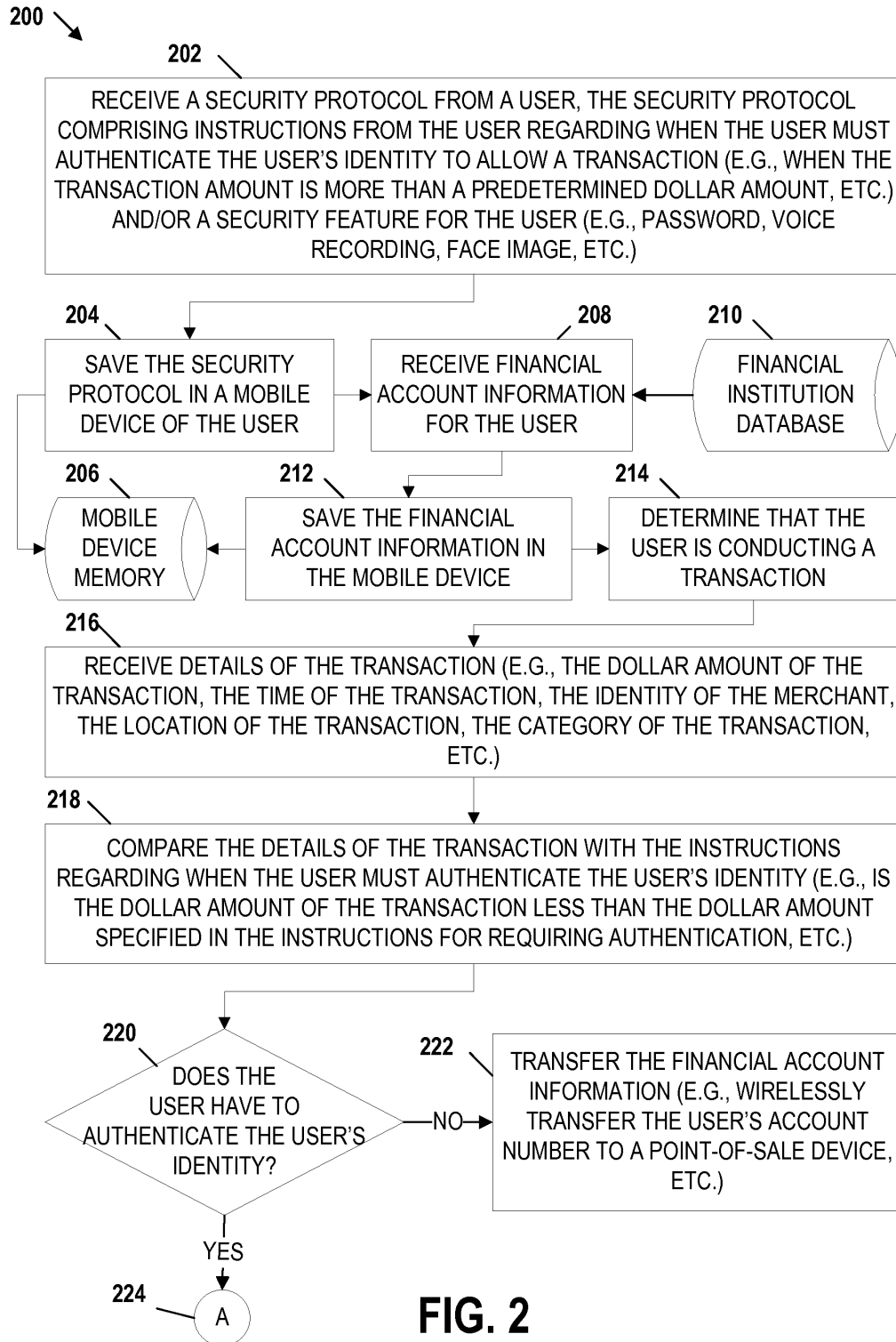


FIG. 2

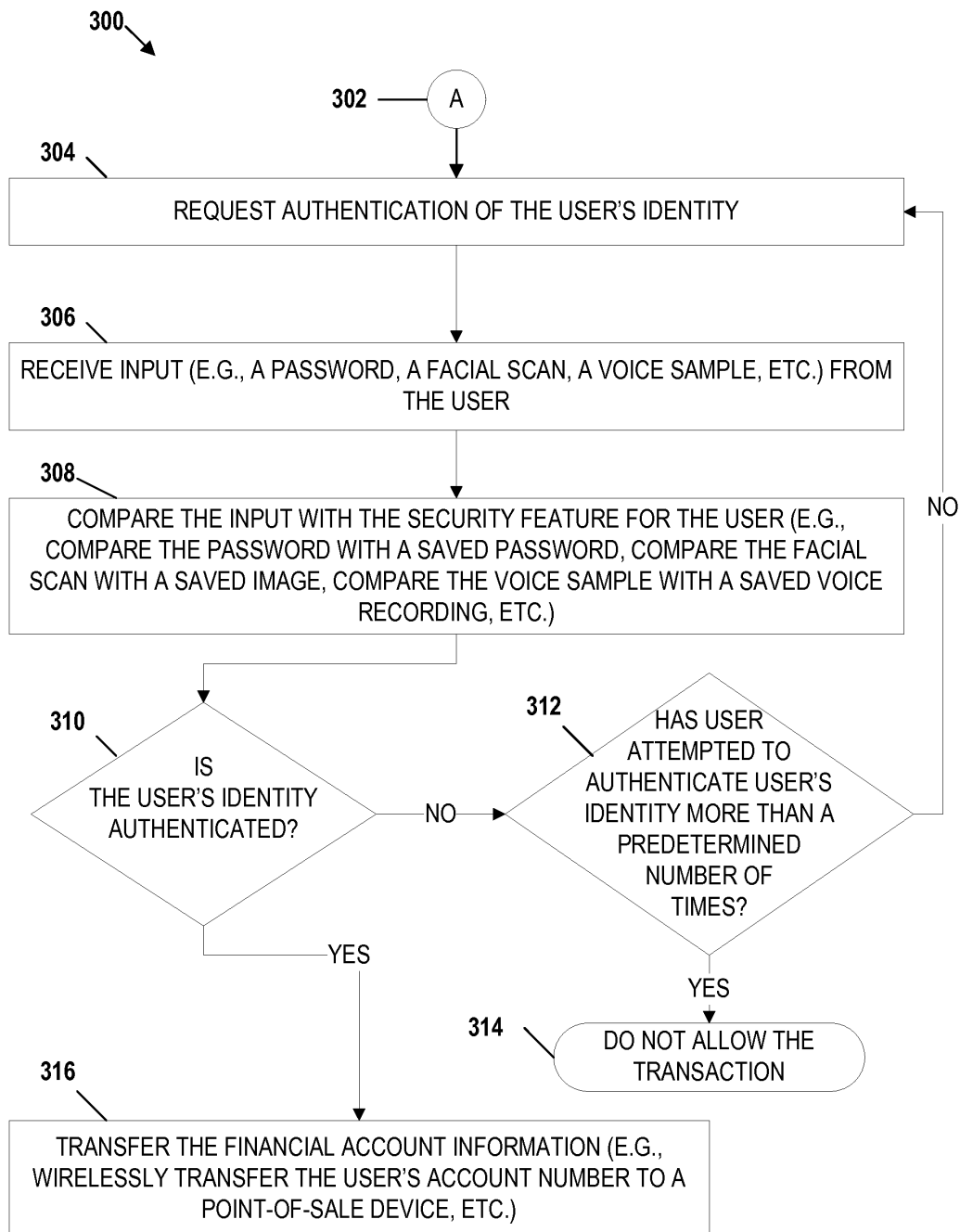


FIG. 3

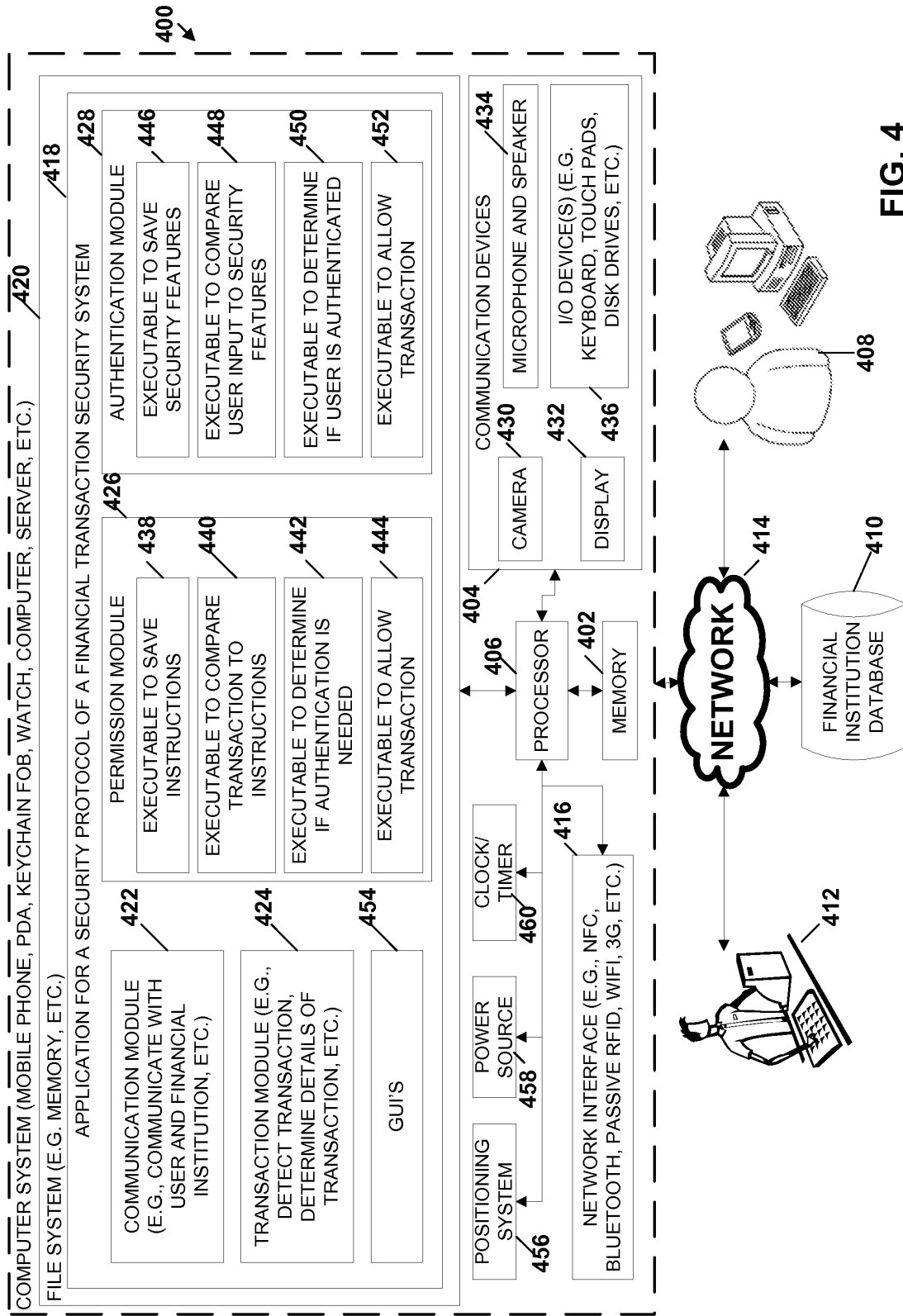


FIG. 4

500

503	FINANCIAL TRANSACTION SECURITY SYSTEM				502	☒
504	HOME USER INFORMATION ACCOUNTS PERMITTED TRANSACTIONS USER AUTHENTICATION HELP					
506	CURRENT USER: JOE SMITH					
508	ACCOUNT INFORMATION: CHECKING ACCOUNT AND CREDIT ACCOUNTS ACTIVE					
510	PERMITTED TRANSACTIONS: CUSTOM BASED ON TRANSACTION AMOUNT, MERCHANT, AND CATEGORY					
512	USER AUTHENTICATION: USERNAME, FACIAL SCANNING, AND VOICE RECOGNITION ACTIVE					
	<u>RECENT TRANSACTIONS</u>					
	<u>PAYEE NAME</u> — 514	<u>AMOUNT</u> — 516	<u>DATE</u> — 518	<u>SECURITY</u> — 520		
	GAS STATION	\$30.00	12/01/2010	AUTOMATIC PAYMENT		
	PAY FROM: CREDIT ACCOUNT					
	PREVIOUS BALANCE: \$140.00					
	GROCERY STORE	\$120.00	12/03/2010	VOICE SCAN CONFIRMED	522	
	PAY FROM: CHECKING ACCOUNT					
	PREVIOUS BALANCE: \$2200					
	COFFEE SHOP	\$3.00	12/04/2010	AUTOMATIC PAYMENT	524	
	PAY FROM: CHECKING ACCOUNT					
	PREVIOUS BALANCE: \$2080					

FIG. 5

600

FINANCIAL TRANSACTION SECURITY SYSTEM

502

X

HOME | USER INFORMATION | ACCOUNTS | PERMITTED TRANSACTIONS | USER AUTHENTICATION | HELP

604

CURRENT USER: JOE SMITH

602

EDIT

608

LOG OUT

610

606

MAILING ADDRESS:

STREET: 123 MAIN STREET

CITY, STATE, ZIP: CHAPEL HILL, NC 27516

PHONE NUMBER: 123-123-4567

EMAIL ADDRESS: JOE.SMITH@GMAIL.COM

612

ADD A USER:

MAILING ADDRESS:

STREET: _____

CITY, STATE, ZIP: _____

PHONE NUMBER: _____

EMAIL ADDRESS: _____

614

AUTHORIZE THIS USER FOR CURRENT ACCOUNTS? _____ YES _____ NO _____ CUSTOMIZE

616

FIG. 6

700 →

704

FINANCIAL TRANSACTION SECURITY SYSTEM 702 502

HOME | USER INFORMATION | ACCOUNTS | PERMITTED TRANSACTIONS | USER AUTHENTICATION | HELP

ACTIVE ACCOUNTS: CREDIT ACCOUNT AND CHECKING ACCOUNT EDIT UPDATE ACCOUNTS

CREDIT ACCOUNT ENDING IN 1007: — 706

LIMIT: \$10,000 708

BALANCE: \$170.00

CATEGORIES: GAS STATIONS — 710

CHECKING ACCOUNT ENDING IN 9292 — 711

BALANCE: \$2080.00

CATEGORIES: GROCERY STORE — 713
RESTAURANT

ADD AN ACCOUNT: — 716

ACCOUNT NUMBER: — 718

BILLING ADDRESS: — 720
/ 722

SELECT CATEGORIES FOR USE: — RESTAURANTS — GROCERY STORE — GAS STATION — CUSTOM

712

714

FIG. 7

800 →

804	FINANCIAL TRANSACTION SECURITY SYSTEM	502	802	⊗
	HOME USER INFORMATION ACCOUNTS <u>PERMITTED TRANSACTIONS</u> USER AUTHENTICATION HELP			
	INSTRUCTIONS FOR ALLOWING A TRANSACTION WITHOUT AUTHENTICATING IDENTITY			EDIT
806	(A) DOLLAR AMOUNT THAT DOES NOT REQUIRE AUTHENTICATION: \$5.00 836 826			
808	(B) TIME SINCE PREVIOUS AUTHENTICATION BEFORE REQUIRING AUTHENTICATION: NOT SELECTED			
810	(C) DISTANCE FROM BILLING ADDRESS BEFORE REQUIRING AUTHENTICATION: NOT SELECTED			
812	(D) MERCHANTS THAT DO NOT REQUIRE AUTHENTICATION: MERCHANTS PURCHASED FROM MORE THAN TEN TIMES IN PREVIOUS YEAR — 828 WALMART — 830 HARRIS TEETER AT 120 N. OAK STREET, DURHAM NC 27707 — 832			
818	(E) TRANSACTION CATEGORIES THAT DO NOT REQUIRE AUTHENTICATION: GAS STATIONS — 834 COFFEE SHOPS —			
820	(F) LOW BALANCE IN ACCOUNT BEFORE REQUIRING AUTHENTICATION: NOT SELECTED			
822	(G) CUSTOM INSTRUCTIONS: NOT SELECTED			

FIG. 8

900

FINANCIAL TRANSACTION SECURITY SYSTEM

502

902

X

HOME | USER INFORMATION | ACCOUNTS | PERMITTED TRANSACTIONS | USER AUTHENTICATION | HELP

904

CURRENT USER: JOE SMITH

906

CLEAR

908

USERNAME: JSMITH

914

EDIT

PASSWORD: *****

EDIT

916

CHALLENGE QUESTION: NOT SELECTED

920

ADD

910

FACIAL SCAN: IMAGE STORED AND ACTIVE

EDIT

912

VOICE SCAN: VOICE RECORDING STORED AND ACTIVE

EDIT

922

IRIS SCAN: NOT SUPPORTED

928

FINGERPRINT SCAN: FINGERPRINT NOT SAVED

ADD

924

CUSTOM DEVICE SECURITY FEATURE: NOT SUPPORTED

926

CHANGE CURRENT USER

FIG. 9

MOBILE TRANSACTION DEVICE SECURITY SYSTEM

BACKGROUND

[0001] People desire convenience and speed when conducting financial transactions but are also concerned about the security of the transactions. Many people conduct transactions at a variety of merchants, such as coffee shops and grocery stores, and would like both convenience and control over their transaction security. Currently, people use debit cards, credit cards, checks, or cash when paying for goods and services. These current forms of payment can be inconvenient to use and lack effective customizable security measures.

[0002] When using a debit card or credit card to conduct a financial transaction, the user is often required to enter a personal identification number (PIN) into a point-of-sale (POS) terminal, provide a signature, and/or show a separate form of picture identification (ID). Checks also require separate identification and must be written out, taking up valuable time. Paying for transactions with cash requires that the person carry the cash with them, wait while change is counted out, and risk losing the cash.

[0003] There are also efforts to create a “mobile wallet” system where people use their mobile phones or similar mobile devices to engage in financial transactions. In such systems, a person’s mobile phone communicates payment information to the POS terminal and the POS terminal then uses this payment information to approve the transaction. These mobile wallet systems also often require the user to take one or more steps to authenticate the user’s identity, such as the steps of having to enter a PIN, show a picture ID, provide a signature, etc.

[0004] All of these inconveniences can add up to wasted time, effort, and worry for people as they conduct transactions. Furthermore, while some people may think that the security procedures required to use a certain payment device are too onerous and inconvenient, other people may think that the required security procedures are not tough enough for the user to overcome.

[0005] Thus, there is a need for improved systems and methods for managing mobile transaction device security in a way that is both convenient and effective for the interested parties.

BRIEF SUMMARY

[0006] Embodiments of the present invention address the above needs and/or achieve other advantages by providing an apparatus (e.g., a system, computer program product, and/or other device) and method allowing a user to customize payment procedures and authentication protocols for a mobile payment device, such as a mobile wallet. In some embodiments of the invention the user can provide instructions that control the authentication procedures based on details of a transaction or of the user.

[0007] For example, some embodiments of the present invention provide a security management module for managing the security protocols of an electronic wallet in accordance with the preferences of the user of the electronic wallet. As used herein, an “electronic wallet,” also referred to herein as a “mobile wallet,” refers to an electronic mobile device (e.g., a cell phone, personal data assistant, mp3 player, handheld computer, etc.) that is configured to be used as a payment device (such as a credit or debit card). The electronic wallet stores payment information in its memory that can be used to identify one or more financial accounts. The electronic wallet is further equipped with a wireless communication interface configured to communicate payment information to a payment terminal.

[0008] For example, some embodiments of the invention provide a mobile transaction device security system that defines a security protocol for performing a transaction using the mobile payment device, such as a cell phone. The security protocol includes a permission module, which determines whether the user does not need to authenticate his identity to perform the transaction, and an authentication module, which authenticates the identity of the user. If user does not need to authenticate his identity or if the user successfully identifies himself, the financial transaction security system allows the transaction. In some embodiments, allowing the transaction includes transmitting financial account information to a point-of-sale device. The financial account information can be data associated with a checking account, a credit account, a money market account, a rewards account, a prepaid account, or any other type of account used to pay for goods or services.

[0009] In some embodiments, the user provides instructions relating to when the user does not need to authenticate his identity to perform a transaction. In some

embodiments, the instructions relate to details of the transaction, including the amount of the transaction, the time of the transaction, the identity of the merchant, the category of the expense, and the location of the transaction. For example, the user may not require authentication for transactions of less than five dollars. In some embodiments, the instructions relate to the financial account of the user, such as the balance in the financial account or previous purchases by the user from the account. For example, the user may not require authentication when the balance on the account is greater than two hundred dollars. In further embodiments, the instructions relate to both the transaction and the user. For example, the user can provide instructions in the permission module to not require authentication if the user has made a purchase at the merchant in the previous thirty days. In some embodiments, transactions at specific merchants selected by the user do not require authentication. In other embodiments, merchants are categorized and the user selects categories that do not require authentication. For example, merchants can be categorized as grocery stores, gas stations, coffee shops, restaurants, or user-defined categories. In this example, the user may not require authentication for transactions at gas stations. In some embodiments, merchants are categorized into more than one category. In an embodiment, the user selects default instructions provided by a bank. In a further embodiment, the instructions are customized by the user.

[0010] In another embodiment, the user provides security features to the financial transaction security system, which are then available to the mobile device. For example, the user may establish a user name and password or provide a voice recording. In some embodiments, the user provides input to authenticate his identity in order to allow the transaction. In various embodiments, the input is in the form of a user name and/or password, a voice sample, a facial scan, a fingerprint scan, an iris scan, a response to a challenge question, or any other form of input capable of validating the user's identity. The authentication module compares the input with the security feature to authenticate the identity of the user. In some embodiments, the user's financial account information is transmitted to the point-of-sale device at the merchant if the user successfully authenticates his identity.

[0011] In an embodiment, the user can manage the financial transaction security system from an application on the mobile device, through software on a personal

computer, or via a webpage. In some embodiments, managing the financial transaction security system allows the user to view account settings and recent transactions. Further embodiments, the user is able to edit, update, and/or add additional users and accounts to the financial transaction security system. In still further embodiments, the user is able to provide instructions for allowing a transaction without requiring authentication of the user's identity. In some embodiments, the user provides security features and is able to add, edit, or update saved security features. The financial transaction security system provides numerous opportunities for the user to customize security protocols relating to financial transactions conducted through mobile devices.

[0012] In some embodiments, as explained herein the mobile device is a mobile wallet, such as but not limited to a smartphone or PDA that allows a user to enter into transactions using the smartphone or PDA. The mobile device allows the user to make a purchase at a store or over the internet by transmitting through a wired or wireless connection between the mobile device and the systems used to make the transaction. However, it is to be understood that the mobile device can be another type of mobile device, which can be scanned, transmit a wireless signal, be entered manually into a system, etc. in order to make payments using the mobile payment device, as will be described in further detail later.

[0013] One embodiment of the invention is an application on a smartphone that stores the user's security protocol, determines that the user is conducting a transaction at a point-of-sale device, and compares the transaction with the instructions provided by the user. If, based on the instructions, the transaction can occur without authentication of the user's identity then the user's financial account information is transmitted to the point-of-sale device. If, however, authentication of the user's identity is required based on the instructions then the user provides input, such as providing a voice sample, and the application compares the input to saved security features. If the application authenticates the user's identity based on the comparison, the user's financial account information is transmitted to the point-of-sale device.

[0014] The features, functions, and advantages that have been discussed may be achieved independently in various embodiments of the present invention or may be

combined in yet other embodiments, further details of which can be seen with reference to the following description and drawings.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

[0015] Having thus described embodiments of the invention in general terms, reference will now be made to the accompanying drawings, wherein:

[0016] Figure 1 provides a high level process flow illustrating a financial transaction security system, in accordance with one embodiment of the present invention;

[0017] Figure 2 provides a flow chart of a financial transaction security system wherein the system determines if authentication is not necessary, in accordance with one embodiment of the present invention;

[0018] Figure 3 provides a flow chart of a financial transaction security system wherein the user authenticates the user's identity, in accordance with one embodiment of the present invention;

[0019] Figure 4 provides a block schematic of a financial transaction security system, in accordance with one embodiment of the present invention;

[0020] Figure 5 provides an interface for setting up a financial transaction security system, in accordance with one embodiment of the present invention;

[0021] Figure 6 provides an interface for viewing and editing user information in a financial transaction security system, in accordance with one embodiment of the present invention;

[0022] Figure 7 provides an interface for viewing and editing financial account information in a financial transaction security system, in accordance with one embodiment of the present invention;

[0023] Figure 8 provides an interface for viewing and editing instructions for allowing a transaction without requiring authentication, in accordance with one embodiment of the present invention; and

[0024] Figure 9 provides an interface for viewing and editing security features capable of authenticating a user's identity in a financial transaction security system, in accordance with one embodiment of the present invention.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

[0025] Embodiments of the present invention now will be described more fully hereinafter with reference to the accompanying drawings, in which some, but not all, embodiments of the invention are shown. Indeed, the invention may be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will satisfy applicable legal requirements. Like numbers refer to like elements throughout.

[0026] It should be understood that terms like “bank,” “financial institution,” and “institution” are used herein in their broadest sense. Institutions, organizations, or even individuals that process financial transactions are widely varied in their organization and structure. Terms like “financial institution” are intended to encompass all such possibilities, including but not limited to banks, finance companies, stock brokerages, credit unions, savings and loans, mortgage companies, insurance companies, and/or the like. Additionally, disclosed embodiments may suggest or illustrate the use of agencies or contractors external to the financial institution to perform some of the calculations, data delivery services, and/or authentication services. These illustrations are examples only, and an institution or business can implement the entire invention on their own computer systems or even a single work station if appropriate databases are present and can be accessed.

[0027] Figure 1 provides a high level process flow illustrating a mobile transaction device security system **100**, in accordance with one embodiment of the present invention. The high level process flow will be discussed in greater detail in Figures 2 and 3. At a high-level, the financial transaction security system **100** receives a security protocol from a user **102**. In some embodiments, the user enters the security protocol into an interface on a mobile device application, a software program, or a webpage. For example, the user may initiate an application on a mobile phone and then enter details relating to the security protocol into the application. In some embodiments, the security protocol is a default level of security provided by a bank. In other embodiments, the security protocol is customizable by the user. The user may change the security protocol in the same manner or in a different manner from which the protocol was initially established.

[0028] In some embodiments, the security protocol includes a permission module and an authentication module. As will be discussed in greater detail in Figures 2 and 3, the permission module and the authentication module aggregate steps in the method of providing a financial transaction security system. The permission module includes the instructions relating to when the user does not need to authenticate his identity as well as any hardware and/or software used to implement those instructions. The authentication module includes the security features provided by the user as well as any hardware and/or software used to compare an input from the user to those security features. The permission module and the authentication module can be hosted completely on the mobile device, completely on a remote server, or partially on both the mobile device and the remote server.

[0029] In an embodiment, the system **100** is configured to determine that the user is conducting a transaction **104**. For example, the system may determine that the user is attempting to purchase a product at a merchant using the mobile device. In some embodiments, the system determines that the user is conducting a transaction by detecting a signal from a point-of-sale device. In other embodiments, the system determines that the user is conducting a transaction by receiving an input from the user. For example, the mobile device may have a hotkey, a software application, or a speech recognition program that the user activates in order to indicate that he is conducting a transaction. In an embodiment, the transaction is a purchase of a good or service from a merchant. In other embodiments, however, the transaction is a transfer of funds, a deposit, a loan, etc. The transaction can be to a merchant, another user, a bank, an internet retailer, or an ATM. As is well-known, a wide variety of types of financial transactions are possible. The system **100** provides a customizable set of security protocols for the wide variety of financial transactions.

[0030] In some embodiments, the system **100** compares the transaction with the permission module **106**. By comparing details of the transaction with the instructions provided by the user on when authentication is not necessary, the system **100** can determine whether the user does not need to authenticate his identity before allowing a transaction **108**. For example, the instructions in the permission module may not require authentication for transaction amounts less than five dollars. In some embodiments, if

the user does not need to authenticate his identity the transaction is automatically allowed **110**. In other embodiments, even if the user does not need to authenticate his identity based on the comparison further input from the user, such as confirmation of the transaction merchant or amount, may be necessary. In an embodiment, if the comparison of the transaction with the permission module indicates that authentication is necessary the system **100** continues on to block **112**.

[0031] In block **112**, the system **100** requests authentication of the user's identity. For example, the system **100** can provide a prompt on a display screen of a mobile device requesting entry of a user name and password. The request can be visual or audible. The request can prepare the mobile device for receiving input from the user. For example, when a request for identification is made the system **100** may activate the microphone and camera on the mobile device in order to capture voice commands or facial scans. The system **100** receives the input from the user in response to the request for authentication of the user's identity.

[0032] In some embodiments, the system **100** compares the input from the user with the authentication module **114**. The system **100** compares the voice command or the facial scan, for example, with security features saved by the user as part of the authentication module.

[0033] Based on the comparison between the input and the authentication module, the system **100** determines whether the user is authorized **116**. For example, software associated with the authentication module compares the input with the saved security feature to determine whether the identity of the user is authenticated. If the identity of the user is authenticated, the system **100** allows the transaction **118**. If, however, the user is not authorized based on the comparison of the input with the authentication module the system **100** does not allow the transaction **120**.

[0034] The high level process flow of Figure 1 illustrates general principles and embodiments of the system and method of providing a financial transaction security system. The examples included above are not limiting and as will be discussed in greater detail later additional steps and or features may be included in the systems and methods.

[0035] Turning now to Figure 2, a flow chart **200** of a financial transaction security system wherein the system determines if authentication is not required is

provided, in accordance with one embodiment of the present invention. In block **202**, the system receives the security protocol from the user, wherein the security protocol includes instructions from the user regarding when the user does not need to authenticate the user's identity to allow a transaction. In some embodiments, the system also receives at least one security feature from the user, which will be discussed in greater detail in Figure 3. The system can receive the security protocol from the user in a variety of ways, such as through a software application, through a webpage, in the form of in person instructions at a bank, as written instructions, or in any other form in which the user can provide instructions.

[0036] In some embodiments, the instructions relate to the transaction that the user is conducting. For example, the instructions can relate to the transaction amount, the transaction location, the transaction time, the transaction category, or the transaction merchant. In other embodiments, the instructions relate to the user, such as the balance in the user's financial account, the amount recently spent by the user, or the number of transactions recently performed by the user.

[0037] In some embodiments, the instructions relate to the transaction amount. For example, in some embodiments the user instructs the system to allow a transaction without authentication when the transaction amount is less than a predetermined amount. The predetermined amount can be an amount provided by the bank, a default amount, or a custom amount. In some embodiments, multiple amounts are provided. For example, the bank can provide default instructions relating to multiple amounts. In one embodiment, the default instructions require tiered levels of security such as no authentication for less than \$20, a user name and password for amounts between \$20 and \$100, and a biometric scan for amounts greater than \$100. The users may also determine that different transaction amounts require different types of authentication or lack thereof. For example, a couple may decide that for transaction amounts greater than \$200 authentication by both individuals is required. The couple may also decide that for transaction amounts less than \$10 no authentication is required and that for amounts between \$10 and \$200 authentication by at least one individual is required. In other embodiments, the user instructs the system to allow a transaction without authentication for amounts greater than a predetermined level, within a predetermined range, at an exact

amount, or any other relationship between the transaction amount and permission to conduct transactions.

[0038] In some embodiments, the instructions relate to the transaction location. For example, the user may provide instructions that authentication is not required for transactions performed within twenty miles of the user's home. In some embodiments, the system determines the user's location when the user is conducting a transaction by means of a positioning system, such as a GPS or software that determines the user's location based on proximity to cell towers. In an embodiment, the user provides instructions relating to distance from a predetermined location, such as the user's residence or billing address. For example, a user may not want to authenticate transactions within five miles of a work address so that transactions can be performed quickly. In another embodiment, the user provides instructions relating to political boundaries, such as city, county, and state. When the system determines the user's location, that location can be cross-referenced to maps and/or coordinates. In this manner, the political entities in which the user is located can be determined. For example, the GPS on a user's cell phone can determine the user's latitude and longitude. The system can compare that latitude and longitude to maps and determine which city, county, and state the user is currently located within. The user may desire to allow transactions without authentication for convenience or security.

[0039] In some embodiments, the instructions relate to the transaction time. For example, the user's mobile device may include a clock or timer which determines the time at which the user is attempting to conduct the transaction. In an embodiment, the user provides instructions that allow transactions without authentication during predetermined time windows. For example, the user may allow transactions without authentication between 8 AM and 5 PM so that the user can quickly and easily conduct transactions during work hours. In another embodiment, the user provides instructions that do not require authentication if the user has authenticated his identity within a predetermined time period. For example, the user can provide instructions that allow transactions without authentication if the user has authenticated his identity within the previous two hours. When the user attempts to conduct a transaction, the system determines the time and determines whether the previous authentication is within the past

hour. If the user has authenticated his identity within the previous two hours, the system does not require authentication. Again, by allowing customization of when the user does not need to authenticate his identity the system provides convenience along with customized security for financial transactions.

[0040] In some embodiments, the user provides instructions that allow transactions without authentication when the transaction is within a specific category. For example, the user may instruct the system to allow transactions at gas stations without authentication. Other examples of transaction categories include grocery stores, coffee shops, restaurants, home goods stores, clothing stores, or other known or custom categories of stores. Certain stores may be included in more than one category. For example, some stores include both groceries and a pharmacy and may be included in the grocery store category and the drug store category. In some embodiments, the categories are defined by the bank. In other embodiments, the categories are defined by, edited, or modified by the user. In some embodiments, the user determines that authentication is not needed in general categories. In other embodiments, the user sets different levels of security required in different categories. For example, gas stations may require no authentication so that transactions are quick and easy but restaurants may require a higher level of security.

[0041] In a still further embodiment, the user provides instructions to allow transactions without authentication based on the transaction merchant. For example, the user may allow transactions without authentication at predetermined specific merchants. The users can select the merchants from a list provided by the bank, the user can input specific merchants, the user can select merchants from previous transactions, the user can provide an indication during a transaction that transactions at the merchant do not need authentication in the future, or the user can select merchants in any other way in which they are able to provide details regarding specific merchants. In another embodiment, the user provides instructions to allow transactions without authentication at merchants where the user has previously performed a transaction. For example, the user may allow transactions without authentication at merchants that the user has purchased from within the past month, or at merchants the user has purchased from more than ten times in the past year, or at merchants where the user has at any time performed a transaction. In

some embodiments the user can select a chain store merchant and allow transactions without authentication at any one of the chain stores. In other embodiments, the user selects a specific chain store and does not expand the permission to include all other stores within the same chain.

[0042] In some embodiments, the instructions relate to the user at the time of the transaction. For example, the instructions can relate to the user's financial account information. In an embodiment, the instructions allow transactions without authentication so long as there is a minimum balance in the user's financial account. If the transaction would bring the account below a predetermined amount, the user will have to authenticate his identity in order to allow the transaction. In another embodiment, the instructions allow transaction without authentication if the user has not performed a predetermined number of transactions recently. For example, the instructions may allow transactions without authentication if the user has performed fewer than twenty transactions in the current month. Both the number of transactions and the time period are customizable by the user. In a still further embodiment, the instructions allow transactions without authentication until the user spends a certain amount in the predetermined period of time. For example, the user may be able to conduct transactions without authentication if the user has not spent above \$400 in a month; all transactions after reaching \$400 in purchases may require authentication. By adjusting the security levels based on user information, the user is able to customize the security levels, assist in budgeting, and gain greater control over expenses.

[0043] In a still further embodiment, the instructions are combined in a variety of ways. For example, the user can provide instructions that combine the number of recent transactions with the transaction categories. For example, a user may provide instructions allowing transactions without authentication for purchases at restaurants until the user has made more than six purchases at restaurants in the current month. Users can, for example, customize their instructions based on combinations of the transaction amount, transaction location, transaction time, transaction category, transaction merchant, account balance, number of transactions, and/or total expenses. The instructions provided by the user allow each user to customize a security protocol for conducting financial transactions with ease, security, and speed.

[0044] Turning now to block **204**, in some embodiments the security protocol is saved in a mobile device of the user. For example, the security protocol can be saved in mobile device memory **206**. The memory can be a removable card, such as an SD-card, or an embedded hard drive. Other types of memory are also possible, as is known. In an embodiment, the mobile device is a cell phone or Personal Digital Assistant (PDA). In another embodiment, the mobile device is specifically designed for conducting financial transactions with the financial transaction security system, such as a keychain dongle. The form factor of the security system can vary widely if the method and functions associated with the system can be configured to operate on the form factor. For example, the financial transaction security system could be incorporated into a watch or other electronic device. In other embodiments, the security protocol is saved on a server and accessed via a network when the user attempts to conduct a transaction. In still further embodiments, parts of the security protocol are saved in the mobile device and other parts of the security protocol are saved on a server accessed via the network. In another embodiment, the mobile device and/or mobile device memory is encrypted so that the instructions and security features are protected if the mobile device is lost or stolen.

[0045] In block **208**, the system receives financial account information for the user. In some embodiments, the system only receives the account number from a financial institution database **210**. In other embodiments, however, the system receives the account number and other related information, such as previous transactions, balances, addresses and contact information associated with the account, other accounts associated with the user, and other account information available from the financial institution database **210**. The system can receive the financial account information wirelessly or through a wired connection. In some embodiments, the system updates the account information, such as on a regular schedule, intermittently, when the system is able to connect to the financial institution, or when prompted to do so by the user. The system also saves the financial account information for access by the mobile device **212**. In some embodiments, the financial account information is saved in the mobile device memory **206**. As with the security protocol, the financial account information may be encrypted and/or hosted in whole or in part on a server and accessed when needed.

[0046] In block **214**, the system determines that the user is conducting a transaction. In some embodiments, the system determines that the user is conducting a transaction by detecting or receiving a signal from a point-of-sale device. The system can activate in response to receiving the signal from the point-of-sale device. In other embodiments, the system determines that the user is conducting a transaction by receiving an input from the user. For example, the mobile device may have a hotkey, a software application, or a speech recognition program that the user activates in order to indicate that he is conducting a transaction.

[0047] In some embodiments of the invention, as depicted in block **216**, the system receives details of the transaction. In an embodiment, the system receives details of the transaction from the merchant, such as when the merchant provides a signal that the user is conducting a transaction. In other embodiments, the system receives details of the transaction from the user, such as input from the user into the mobile device. In a still further embodiment, the system receives details of the transaction from the user's financial institution, alone or in combination with either of the merchant or the user. In an exemplary embodiment, the system receives details of the transaction wirelessly from a point-of-sale device.

[0048] Details of the transaction that may be received by the system include the amount of the transaction, the time of the transaction, the identity of the merchant, the location of the transaction, the category of the transaction, or any other features associated with a transaction that can be provided by the user, the mobile device, the merchant, or the financial institution. For example, the system can receive details from the merchant about the identity of the merchant and from the user's financial institution regarding the number of times the user has frequented that merchant in the past year. In another example the system receives details regarding the amount of the transaction from the merchant and the category of the transaction from the user. The system may prompt the user to select or input a category for the expense. In yet another example the system receives the time of the transaction from a clock or timer associated with the mobile device. Similarly, the system can receive the location of the transaction from a GPS unit, through triangulation based on cell phone signals, from the merchant, from a financial institution, or from the user.

[0049] In block **218**, in some embodiments the system compares the details of the transaction with the instructions regarding when the user must authenticate his identity. The system provides software capable of comparing the details of the transaction with the instructions to determine when the user must authenticate his identity. In an embodiment, the system compares the details with the instructions using software embedded on the user's mobile device. In another embodiment, the system compares the details with the instructions using software on a server that is remotely accessed. An example of comparing the details to the instructions is comparing the amount of the transaction with the instructions allowing transactions without authentication when the transaction amount is below a predetermined level. Another example is when the identity of the merchant is compared to instructions allowing transactions without authentication at predetermined merchants. A further example is when the details of the transaction include the location of the transaction and the location is compared to instructions that allow the user to perform transactions without authentication within a specified city. A still further example is when the time of the transaction is determined based on the mobile device clock and the system compares the length of time since the previous user authentication to instructions allowing transactions without authentication before a predetermined period of time has elapsed, for example authentication may not be required if the user has authenticated his identity within the previous four hours. As discussed previously, a multitude of instructions relating to transactions and/or the user are possible. Similarly, a multitude of details regarding transactions can be received by the system from the user, the mobile device, the financial institution, and/or the merchant. By combining and comparing the details with the instructions, the system provides a customizable security system for financial transactions.

[0050] In block **220**, the system determines whether the user must authenticate the user's identity based on the comparison of the details of the transaction with the instructions. In some embodiments, if the user does not have to authenticate his identity based on the comparison, the system transfers the user's financial account information to allow the transaction **222**. In an embodiment, the system wirelessly transfers the user's financial account information to a point-of-sale device. In this embodiment, the point-of-sale device can then complete the transaction through standard methods of completing

transactions, such as with credit or debit cards. If the user does need to authenticate his identity based on the comparison the system moves from the permission module to the authentication module, as indicated at **224** and depicted in Figure 3.

[0051] Figure 3 depicts a flow chart of a financial transaction security system wherein the user authenticates the user's identity **300**, in accordance with one embodiment of the present invention. The flowchart corresponds to the authentication module of the financial transaction security system. If the system determines that the user must authenticate his identity **302**, the system will request authentication of the user's identity **304**.

[0052] Requesting authentication of the user's identity **304** can occur in a variety of ways. In an embodiment, the user's mobile device prompts the user to authenticate his identity. The request can be visual or audible. In an embodiment, the request allows a user to authenticate his identity in any manner. For example the user may be able to authenticate his identity using a username and password, a facial scan, or a voice scan. In this embodiment, the system would request authentication using any of these methods. In another embodiment, the system requests authentication in a specific manner. For example, the system may specifically request a facial scan. Determination of the method for authentication can be based on the transaction, instructions from the financial institution, instructions from the user, instructions from the merchant, or randomly. For example, the user's bank may require authentication based on one of the biometric scans for transaction amounts greater than \$1000. As discussed in a previously described example, the user may set different tiers of authentication depending on the transaction amount. The user may allow a transaction without authentication for transaction amounts less than \$5, require authentication by a username and password for transaction amounts between \$5 and \$100, and require a biometric scan for transactions greater than \$100.

[0053] In block **306**, the system receives input from the user in an embodiment. The input may be, for example, a username or password, a facial scan, a voice sample, an iris scan, a fingerprint scan, a response to a challenge question, etc. In an embodiment, the system receives the input from a communication device associated with the user's mobile device. For example, the system may receive the input from the keyboard, a touch screen, a microphone, and/or a camera associated with the user's mobile device.

[0054] In some embodiments, the input provided by the user is in the form of a hotkey, application, voice command, or movement of the mobile device. In these embodiments, the input automatically indicates that the transaction is authorized without needing to authenticate the user's identity further. U.S. Patent Application Serial No. _____ to Grigg *et al.*, entitled "Transaction Authorization System for a Mobile Commerce Device," and filed concurrently herewith, describes such a device, system, and method in greater detail and is hereby incorporated by reference in its entirety.

[0055] The system receives security features for use with the authentication module, in some embodiments. For example, the security feature may be a username and password provided by the user and stored in the mobile device memory or on a server. Other examples of security features include facial images for use with facial recognition software, voice recordings for use with voice recognition software, iris images for use with iris scanning software, a bank of challenge questions and answers, a scanned fingerprint for use with fingerprint scanning software, or other features that are capable of authenticating the user's identity in conjunction with input from the user.

[0056] In an embodiment, the system compares the input with the security feature for the user **308**. For example, the system can compare the username and password entered by the user with a username and password previously stored by the user in the system to determine if the system is able to authenticate the user's identity. Similarly, the system could compare the facial scan with the saved image of the user's face, the voice sample with the saved voice recording, the response to the challenge question with the bank of challenge questions and answers previously saved by the user, the iris scan with the previously stored image of the user's iris, the fingerprint scan with the previously stored image of the user's fingerprint, or any other security feature capable of authenticating the user's identity.

[0057] In some embodiments, the system determines whether the user's identity is authenticated based on the comparison **310**. For example, if the input username and password match the saved username and password then the user's identity is authenticated. If, however, the user's identity is not authenticated based on the comparison of the input with the security feature the system can determine whether the user should have another opportunity to authenticate his identity **312**. For example, the

user may have incorrectly entered the password and desire another opportunity to enter it correctly. The user and/or the financial institution can set a predetermined number of times that the user is able to attempt authentication of his identity, such as three times. If the user exceeds that predetermined number of times then the system can end and not allow the transaction **314**. This provides greater security in case the mobile device is lost or stolen. If the user has not exceeded the predetermined number of times then the system can again request authentication of the user's identity, as depicted in block **304**. In another embodiment, the system requests authentication of the user's identity using a different method than previously attempted by the user. For example, if the user unsuccessfully attempted to authenticate his identity using a facial scan the first time, the system may next prompt the user to authenticate his identity using a voice scan.

[0058] If the user has successfully authenticated his identity, in some embodiments the system transfers the user's financial account information **316**. In an embodiment, the system wirelessly transfers the user's financial account information to the point-of-sale device so that the merchant may complete the transaction through standard means. In other embodiments, the system wirelessly transfers the user's financial account information to another user, an ATM, or to an online retailer to complete a transaction.

[0059] Figure 4 is a schematic block diagram of a financial transaction security system **400**, in accordance with an embodiment of the invention. In some embodiments, the system **400** includes a computer system such as a mobile phone, PDA, keychain fobs, watch, computer, server, electronic device, etc. In an exemplary embodiment, the financial transaction security system is a mobile phone including a memory device **402**, a communication device **404**, and a processing device **406**. In some embodiments, the system interacts with the user **408**, the financial institution **410**, and the merchant **412** over a network **414**. The system may additionally include a network interface device **416**, such as a Near Field Communication (NFC) device, a Bluetooth device, a Radio Frequency Identification (RFID) device, or other device capable of interacting with the network **414**.

[0060] The network **414** may be a global area network (GAN), such as the Internet, a wide area network (WAN), a local area network (LAN), a wifi network, a 3G

network or any other type of network or combination of networks. The network **414** may provide for wireline, wireless, or a combination of wireline and wireless communication between devices on the network.

[0061] As used herein, the term “processing device” generally includes circuitry used for implementing the communication and/or logic functions of a particular system. For example, a processing device **406** may include a digital signal processor device, a microprocessor device, and various analog-to-digital converters, digital-to-analog converters, and other support circuits and/or combinations of the foregoing. Control and signal processing functions of the system are allocated between these processing devices according to their respective capabilities. The processing device **406** may include functionality to operate one or more software programs based on computer-readable instructions thereof, which may be stored in the memory device **402**.

[0062] The processing device **406** is operatively coupled to the communication device **404** and the memory device **402**. The processing device **406** uses the communication device **404** to communicate with the user **408**. Additionally the processing device uses the network interface **416** to communicate with the network **414** and other devices on the network **414**, such as, but not limited to, the financial institution database **410** and the merchant **412**.

[0063] As further illustrated in Figure 4, the financial transaction security system includes computer-readable instructions **420** stored in a file system, which in one embodiment includes the computer-readable instructions **420** of a security protocol application **418**.

[0064] In the embodiment illustrated in Figure 4 and described throughout much of this specification, the security protocol application **418** allows for communication between a communication module **422**, a transaction module **424**, a permission module **426**, and an authentication module **428** to send, receive, and store information related to the financial transaction security system, determine details relating to a transaction, determine whether user authentication is not necessary, and authenticate the user's identity.

[0065] Specifically, the communication module **422** facilitates communication between the security system and the user **408**. In some embodiments, the communication

module **422** controls the communication devices associated with the system. For example, the communication module **422** can control a camera **430**, a display **432**, a microphone and/or speaker **434**, and I/O devices such as keyboards, touchpads, etc. **436**. In some embodiments, the communication module **422** also controls the network interface **416** for facilitating communication with the user's financial institution **410**, other users, and the merchant **412**.

[0066] In some embodiments, the transaction module **424** determines that the user is conducting a transaction and determines the details of the transaction. In an embodiment, the transaction module **424** interacts with the communication module **422** to receive a signal from a point-of-sale device at a merchant **412** to determine that the user is conducting the transaction, establishes a connection with the point-of-sale device, receives details of the transaction, and completes the transaction.

[0067] In some embodiments, the permission module **426** determines whether a user must authenticate his identity before allowing a transaction. In some embodiments, the permission module includes at least one of an executable to save instructions **438**, an executable to compare the transaction to the instructions **440**, an executable to determine if authentication is needed **442**, and an executable to allow the transaction **444**. The executables can be subroutines available to the security protocol application and called up when input is received or output is needed.

[0068] In some embodiments, the executable to save instructions **438** receives instructions from the user **408** and saves them to the memory device **402**. The executable to save instructions **438** interacts with the communication module **422** and the communication devices **404** to receive the instructions regarding when the user does not need to authenticate his identity. In an embodiment, the executable to save instructions **438** provides default instructions that are selected by the user. In another embodiment, the executable to save instructions guides **438** the user through a process of providing instructions.

[0069] In some embodiments, the executable to compare the transaction to the instructions **440** compares details of the transaction with the instructions. For example, the executable **440** may compare the transaction amount received from the transaction module **424** with the instructions regarding the amount below which authentication is not

needed. The executable **440** interacts with the transaction module **424** and the memory device **402** to receive the data used to make the comparison.

[0070] In some embodiments, the executable to determine if authentication is needed **442** evaluates the output of the comparison provided by executable **440** and determines whether the instructions indicate that the user need not authenticate his identity. If the executable to determine if authentication is needed **442** determines that authentication is not needed, in some embodiments the executable to allow transactions **444** transfers the user's financial account information. The executable to allow transactions **444** interacts with the transaction module **424** and the network interface **416** to transfer the user's financial account information to a point-of-sale device at the merchant **412**, for example.

[0071] In some embodiments, the authentication module **428** includes at least one of an executable to save security features **446**, an executable to compare user input to security features **448**, an executable to determine if the user is authenticated **450**, and an executable to allow the transaction **452**.

[0072] The executable to save security features **446** receives security features from the user **408** and saves them in the memory device **402**, in some embodiments. For example, the user can provide a username and password as security features, which the executable to save security features **446** would receive through the communication module **422**. The executable to save security features **446** can prompt the user to update and/or enter new security features after a period of time or a number of failures to authenticate the user. For example, the voice recording saved may be of poor quality and after five times of being unable to authenticate the user using the voice recording, the executable to save security features **446** could delete the saved recording and prompt the user to record a new one.

[0073] In some embodiments, the executable to compare the user input to the security features **448** evaluates input from the user **408** received through communication devices **404** to saved security features stored in the memory device **402**. For example, the executable to compare the input to the security features **448** may include voice recognition software to compare the voice sample to a saved voice recording. In another example, the executable **448** includes software to compare an answer to a challenge

question to a saved answer previously provided by the user. The executable **448** interacts with the communication module **422** and the memory device **402** to receive the data used to make the comparison, in some embodiments.

[0074] In an embodiment, the executable to determine if the user is authenticated **450** evaluates the results of the comparison from the executable to compare the user input to the security features **448**. In some embodiments, the executable **450** determines that the user is authenticated if the comparison indicates the input is identical to the security feature. In another embodiment, the input must merely be similar to the security feature, such as with a facial scan, voice scan, iris scan, and fingerprint scan. The system is configured to consider the limitations of the communication devices **404** and determine that the user is authenticated if the input is close enough to the security feature to allow the transaction. In some embodiments, the user is able to select the level of similarity that must be present before the system determines that the user's identity is authenticated. In other embodiments, the financial institution determines the level of similarity that must be present before the user's identity is authenticated. For example, the financial institution may determine that a fingerprint scan must have 90% similarity with a saved fingerprint before authenticating the user's identity.

[0075] In some embodiments, the executable to allow transactions **452** transfers the user's financial account information if the user's identity is authenticated. In an embodiment, the executable to allow transactions **452** wirelessly transfers the user's financial information to a point-of-sale device at a merchant **412** when the user's identity is authenticated. In some embodiments, the executable to allow transactions **452** interacts with the transaction module **424** and the network interface **416** to securely transfer the user's account information.

[0076] The security protocol application **418** also includes Graphical User Interfaces (GUI's) **454**, in some embodiments. The GUI's **454** assist in communication between the user **408** and the system. Multiple GUI's **454** can be available for the communication module **422**, the transaction module **424**, the permission module **426**, and the authentication module **428**. GUI's **454** can also be provided that assist the user in utilizing the communication devices **404**, or any other feature of the financial transaction security system **400**.

[0077] In some embodiments, the system also includes a positioning system **456**, a power source **458**, and a clock or timer **460**. In an embodiment, the positioning system **456** is a Global Positioning System (GPS). In another embodiment, the positioning system is an accelerometer. In some embodiments, the power source **458** is a battery, such as a battery coupled to the mobile device. In other embodiments, the power source **458** is a receiver for receiving power from a remote source. For example, the power source may be receiver that receives power from a point-of-sale device through Near Field Communication devices. In some embodiments, the system operates without onboard power if the power source **458** is configured to receive power from the point-of-sale device.

[0078] It is understood that the servers, systems, and devices described herein illustrate one embodiment of the invention. It is further understood that one or more of the servers, systems, and devices can be combined in other embodiments and still function in the same or similar way as the embodiments described herein.

[0079] Figure 5 illustrates an interface **500** for setting up a financial transaction security system, in accordance with one embodiment of the present invention. The interface **500** can include a variety of tabs **502** for viewing and editing information related to the financial transaction security system. One of the tabs can be a home tab **503** that provides general information related to the security system. For example, the home tab **503** can include information related to the current user **504**, the account information **506**, the permitted transactions **508**, the types of user authentication available to the user **510**, and recent transactions **512** that have occurred through the security system.

[0080] In an embodiment, information relating to the current user **504** is available because more than one user may share a mobile device and desire to log in to the security system so that personal instructions and security features are available. In an embodiment (not illustrated), more than one user is listed at **504** and instructions, accounts, and security features for each user may be concurrently available through the mobile device. In some embodiments, the account information **506** is provided on a home page so that the user quickly and easily knows which accounts can be drawn from during a transaction. In the example illustrated in Figure 5, the user's checking and credit

accounts are active. In some embodiments, general descriptions of the permitted transactions **508** are provided on the home page. For example, the general descriptions may include descriptions of the instructions for allowing transactions without authentication. In the example depicted in Figure 5, the instructions permit transactions without authentication based on the transaction amount, the transaction merchant, and the transaction category. This allows the user to quickly know that a transaction will not be allowed without authentication based on geographic location. In a still further embodiment, the home page includes information related to user authentication **510**. For example, Figure 5 depicts that the security system includes security features related to a username, a facial scan, and a voice scan. This information allows the user to quickly determine whether providing a facial scan could authenticate the user's identity if needed.

[0081] Figure 5 also includes an interface describing recent transactions **512**, in accordance with an embodiment of the invention. In some embodiments, the interface describing recent transaction **512** includes the payee name **514**, the transaction amount **516**, the date of the transaction **518**, and the type of security applied to the transaction **520**. For example, the security applied to the transaction **520** can be automatic payment based on a comparison of the details of the transaction with the instructions **522** or it can be based on a comparison of the user input with the security features **524**. In general, the home tab **503** provides overview information so that a user is kept up-to-date regarding recent transactions and the status of the financial transaction security system.

[0082] Turning now to Figure 6, an interface for viewing and editing user information in a financial transaction security system is presented **600**, in accordance with one embodiment of the present invention. The interface includes the tabs **502** that allow the user to switch between multiple interfaces. In an embodiment, one tab provides content relating to user information **602**. In some embodiments, the user information interface **600** includes content related to the current user **602**, the current user's contact information **606**, and the ability to add a user **612**. In an embodiment, the identity of the current user **604** is provided so that the person viewing the financial transaction security system on the mobile device will know whether his identity is active in the system. For example, if more than one person uses a cell phone each person may want to have a different security protocol on the cell phone and hence would need to change users as the

phone changed hands. An edit button **608** allows the users to be changed for the financial transaction security system, in some embodiments. Contact information **606** may also be provided for the user. In an embodiment, this contact information is used for both information purposes and in conjunction with instructions relating to when authentication is not required. For example, the mailing address can be used in conjunction with instructions relating to the user's location. In some embodiments, if the user is located within ten miles of the user's mailing address when the user is conducting a transaction, the user does not need to authenticate his identity. The contact information may also be updated and/or added to by the edit button **608**, for example by adding a business address. The current user **604** is also able to log out **610** of the financial transaction security system.

[0083] In some embodiments, the user information tab **602** includes the ability to add a user **612** to the financial transaction security system. The additional user can be added to the current security protocol **614** or can create a customized security protocol **616**. User information can be provided for the additional user **612**. In some embodiments, the ability to add an additional user allows a single mobile device to serve as a transaction device for multiple people. Further, the transaction device can be personalized for each user.

[0084] In Figure 7, an interface for viewing and editing financial account information in a financial transaction security system is provided **700**, in accordance with one embodiment of the present invention. In some embodiments, the interface **700** includes tabs **502** for switching between different content-providing interfaces. In an embodiment, an Accounts tab **702** provides content related to the user's accounts, including display and editing of the financial account information. For example, in some embodiments the Accounts tab **702** includes information related to the active accounts **704** in the financial transaction security system. For each account, the type of account and at least a portion of the account number are displayed **706**. Information **708** pertaining to each account, such as the credit limit and account balance is provided. In some embodiments, additional information pertaining to the instructions for allowing transaction without authentication is also included. For example, in an embodiment different accounts are linked to different transaction categories. In the example disclosed

in Figure 7, the credit account **706** is associated with transactions occurring at gas stations **710** while the checking account **711** is associated with transaction occurring at grocery stores and restaurants **713**. By linking accounts to transaction categories, users are able to direct transactions through specific accounts based on categories. In other embodiments, the user is able to link specific accounts to transaction amounts, transaction location, transaction merchants, or other details of the transaction or user account information. This allows greater control over transactions and budgeting from multiple accounts for the user.

[0085] In an embodiment, the Accounts tab **702** includes the ability to add accounts **716** to the financial transaction security system. In some embodiments, the accounts include checking accounts, savings accounts, money market accounts, credit accounts, rewards accounts, or other types of financial accounts. The user can add the account number **718**, the billing address **720** or other account information (e.g., the credit limit), and indicate the transaction categories **722** for which the account is active. In an embodiment (not shown), the user is able to also indicate other characteristics of the transaction or user account information for which the account is active. For example, the user can indicate that a new account should be used for all transactions less than \$5. In another example, the user can indicate that a new account should be used until the balance in the account is below \$100 or within \$500 of the credit limit.

[0086] In some embodiments, as depicted in Figure 8 the system provides an interface for viewing and editing instructions for allowing a transaction without requiring authentication **800**, in accordance with one embodiment of the present invention. In an embodiment, the tabs **502** include a Permitted Transactions tab **802** that provides content and editing related to the instructions for allowing a transaction without authenticating the user's identity **804**. In some embodiments, the most common types of instructions are displayed on the interface so that the user can easily and quickly view the instructions that control when a user can conduct a transaction without authentication. For example, the interface can display the transaction amount below which the user does not need to authenticate his identity **806**, the time since the previous authentication before authentication is necessary **808**, the distance from the billing address before requiring authentication **810**, merchants that do not require authentication **812**, transaction

categories that do not require authentication **818**, low balances before requiring authentication **820**, or custom instructions **822**. In an embodiment, the specific instruction is displayed **824**, for example the transaction amount below which authentication is not required is \$5 in Figure 8. In another embodiment, the interface indicates that instructions are not selected or provided **826**, for example for time since previous authentication and distance from billing address in Figure 8. In a still further embodiment, instructions related to merchant identity may be subdivided into instructions that relate to merchants the user has frequented recently **828**, chain merchants **830** such that the user can conduct transactions at any of the chain merchant stores, or specific merchants **832** defined by a location. In another embodiment, the transaction categories for which authentication is not needed **834** are also provided for ease of reference by the user. The interface can provide a level of content regarding the instructions so that the user can easily review and edit **836** the instructions if needed.

[0087] Turning now to Figure 9, an interface for viewing and editing security features capable of authenticating a user's identity in a financial transaction security system is provided **900**, in accordance with one embodiment of the present invention. In some embodiments, the interface **900** includes tabs **502**, such as a User Authentication tab **902**. The User Authentication tab **902** may include the identity of the current user **904** and the types of security features **906** that are uploaded to the financial transaction security system for that user. In the example displayed in Figure 9, the user's username and password **908**, the user's facial scan **910**, and the user's voice scan **912** are available to the financial transaction security system. In an embodiment, the user is able to edit **914** the stored features using the mobile device. The interface may also indicate which security features are not available to the user because they have not been provided to the system yet. For example, in Figure 9 challenge questions **916** and fingerprint scans **918** have not been saved to the financial transaction security system yet. In an embodiment, the interface allows the user to add **920** these security features using the mobile device. In a still further embodiment, the interface also indicates security features which the financial transaction security system is capable of evaluating but which the mobile device does not support **928**. For example, in Figure 9 the mobile device does not support iris scanning **922** and has no custom device security features **924** available to the user. For

example, the camera on a mobile phone may be unable to scan the user's iris with sufficient accuracy to be able to authenticate the user's identity, while another mobile phone may have a camera with high enough resolution to perform the scan (in which case the iris scan would be supported). In a still further embodiment, the interface allows the user to change **926** the current user **904** so that custom security features are saved for multiple users associated with the mobile device.

[0088] As will be appreciated by one of skill in the art, the present invention may be embodied as a method (including, for example, a computer-implemented process, a business process, and/or any other process), apparatus (including, for example, a system, machine, device, computer program product, and/or the like), or a combination of the foregoing. Accordingly, embodiments of the present invention may take the form of an entirely hardware embodiment, an entirely software embodiment (including firmware, resident software, micro-code, etc.), or an embodiment combining software and hardware aspects that may generally be referred to herein as a "system." For example, various embodiments may take the form of web-implemented computer software. Furthermore, embodiments of the present invention may take the form of a computer program product on a computer-readable medium having computer-executable program code embodied in the medium.

[0089] It will be understood that any suitable computer-readable medium may be utilized. The computer-readable medium may include, but is not limited to, a non-transitory computer-readable medium, such as a tangible electronic, magnetic, optical, electromagnetic, infrared, and/or semiconductor system, device, and/or other apparatus. For example, in some embodiments, the non-transitory computer-readable medium includes a tangible medium such as a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), a compact disc read-only memory (CD-ROM), and/or some other tangible optical and/or magnetic storage device. In other embodiments of the present invention, however, the computer-readable medium may be transitory, such as, for example, a propagation signal including computer-executable program code portions embodied therein.

[0090] One or more computer-executable program code portions for carrying out operations of the present invention may include object-oriented, scripted, and/or unscripted programming languages, such as, for example, Java, Perl, Smalltalk, C++, SAS, SQL, Python, Objective C, and/or the like. In some embodiments, the one or more computer-executable program code portions for carrying out operations of embodiments of the present invention are written in conventional procedural programming languages, such as the “C” programming languages and/or similar programming languages. The computer program code may alternatively or additionally be written in one or more multi-paradigm programming languages, such as, for example, F#.

[0091] Some embodiments of the present invention are described herein with reference to flowchart illustrations and/or block diagrams of apparatuses and/or methods. It will be understood that each block included in the flowchart illustrations and/or block diagrams, and/or combinations of blocks included in the flowchart illustrations and/or block diagrams, may be implemented by one or more computer-executable program code portions. These one or more computer-executable program code portions may be provided to a processor of a general purpose computer, special purpose computer, and/or some other programmable data processing apparatus in order to produce a particular machine, such that the one or more computer-executable program code portions, which execute via the processor of the computer and/or other programmable data processing apparatus, create mechanisms for implementing the steps and/or functions represented by the flowchart(s) and/or block diagram block(s).

[0092] The one or more computer-executable program code portions may be stored in a transitory and/or non-transitory computer-readable medium (e.g., a memory, etc.) that can direct, instruct, and/or cause a computer and/or other programmable data processing apparatus to function in a particular manner, such that the computer-executable program code portions stored in the computer-readable medium produce an article of manufacture including instruction mechanisms which implement the steps and/or functions specified in the flowchart(s) and/or block diagram block(s).

[0093] The one or more computer-executable program code portions may also be loaded onto a computer and/or other programmable data processing apparatus to cause a series of operational steps to be performed on the computer and/or other programmable

apparatus. In some embodiments, this produces a computer-implemented process such that the one or more computer-executable program code portions which execute on the computer and/or other programmable apparatus provide operational steps to implement the steps specified in the flowchart(s) and/or the functions specified in the block diagram block(s). Alternatively, computer-implemented steps may be combined with, and/or replaced with, operator- and/or human-implemented steps in order to carry out an embodiment of the present invention.

[0094] As used herein, a processor/computer, which may include one or more processors/computers, may be “configured to” perform a stated function in a variety of ways, including, for example, by having one or more general-purpose circuits perform the stated function by executing one or more computer-executable program code portions embodied in a computer-readable medium, and/or by having one or more application-specific circuits perform the stated function.

[0095] While certain exemplary embodiments have been described and shown in the accompanying drawings, it is to be understood that such embodiments are merely illustrative of, and not restrictive on, the broad invention, and that this invention not be limited to the specific constructions and arrangements shown and described, since various other changes, combinations, omissions, modifications and substitutions, in addition to those set forth in the above paragraphs, are possible. Those skilled in the art will appreciate that various adaptations, modifications, and combinations of the just described embodiments may be configured without departing from the scope and spirit of the invention. Therefore, it is to be understood that, within the scope of the appended claims, the invention may be practiced other than as specifically described herein.

WHAT IS CLAIMED IS:

1. A mobile transaction device security system comprising:
 - a memory device;
 - a communication device; and
 - a processing device coupled to the memory device, wherein the processing device is configured to:
 - receive a security protocol from a user, the security protocol comprising a permission module and an authentication module;
 - determine that the user is conducting a transaction;
 - compare the transaction with the permission module; and
 - determine a process for authenticating the user, the determination based on the comparison of the transaction with the permission module.
2. The system of claim 1, wherein the processing device is configured to determine the process for authenticating the user by determining if the user must authenticate an identity of the user based on the comparison of the transaction with the permission module, and wherein the processing device is further configured to allow the transaction if the user does not need to authenticate the user's identity.
3. The system of claim 1, wherein the processing device is further configured to execute computer-readable program code to:
 - request authentication of the user's identity based on the comparison of the transaction with the permission module;
 - compare input from the user with the authentication module; and
 - allow the transaction if the user is authorized to perform the transaction based on the comparison of the input with the authentication module.
4. The system of claim 1, wherein the authentication module comprises at least one security feature.

5. The system of claim 3, wherein the at least one security feature is customizable by the user.
6. The system of claim 3, wherein the security feature consists of at least one of a username, a password, a challenge question, a voice recognition test, a facial recognition test, a fingerprint identification test, and an iris scan.
7. The system of claim 1, wherein the communication device consists of at least one of a keyboard, a scanner, a touchpad, a camera, a speaker, and a microphone.
8. The system of claim 1, wherein the permission module comprises instructions on when the user must authenticate the user's identity to perform the transaction.
9. The system of claim 7, wherein the instructions are provided by the user.
10. The system of claim 7, wherein the instructions are based on a characteristic of the transaction.
11. The system of claim 9, wherein the characteristic of the transaction consists of at least one of the dollar amount of the transaction, the identity of the merchant, the category of the expense, the time of the transaction, and the location of the transaction.
12. A computer-implemented method of providing financial transaction security, the method comprising:
 - receiving a security protocol from a user, the security protocol comprising a permission module and an authentication module;
 - determining that the user is conducting a transaction;
 - comparing the transaction with the permission module;
 - determining if the user must authenticate an identity of the user based on the comparison of the transaction with the permission module; and

allowing the transaction if the user does not need to authenticate the user's identity.

13. The method of claim 12, the method further comprising:

requesting authentication of the user's identity based on the comparison of the transaction with the permission module;

comparing input from the user with the authentication module; and

allowing the transaction if the user is authorized to perform the transaction based on the comparison of the input with the authentication module.

14. The method of claim 12, wherein receiving the security protocol from the user comprises receiving instructions for prompting the authentication module and receiving security features for authenticating the user's identity.

15. The method of claim 12, wherein determining that the user is conducting a transaction comprises receiving a signal from a point-of-sale device indicating that the user is attempting to conduct a transaction.

16. The method of claim 12, wherein comparing the transaction with the permission module comprises comparing at least one of the transaction amount, the transaction time, the transaction location, the transaction merchant, and the transaction category with predetermined instructions in the permission module.

17. The method of claim 12, wherein determining if the user must authenticate an identity of the user comprises determining whether a characteristic of the transaction permits the user to conduct the transaction without authenticating the user's identity.

18. The method of claim 12, wherein allowing the transaction comprises transferring the user's account information to a point-of-sale device.

19. The method of claim 18, wherein the transferring the user's account information to the point-of-sale device comprises wirelessly transferring the account information.
20. The method of claim 13, wherein requesting authentication of the user's identity comprises receiving input of at least one of a username, a password, an answer to a challenge question, a voice recognition scan, a facial scan, a fingerprint scan, and an iris scan.
21. The method of claim 20, wherein comparing the input from the user with the authentication module comprises comparing the input from the user with a security feature.
22. The method of claim 21, wherein the security feature is stored in memory associated with a mobile device.
23. The method of claim 22, wherein the memory is capable of receiving power from a point-of-sale device.
24. The method of claim 23, wherein allowing the transaction if the user is authorized to perform the transaction comprises transferring the user's account information to a point-of-sale device.
25. A computer program product for providing a financial transaction security product, the computer program product comprising:
- a non-transitory computer-readable medium comprising:
 - an executable portion for causing a computer to receive a security protocol from a user, the security protocol comprising a permission module and an authentication module;
 - an executable portion for causing a computer to determine that the user is conducting a transaction;

an executable portion for causing a computer to compare the transaction with the permission module;

an executable portion for causing a computer to determine if the user must authenticate an identity of the user based on the comparison of the transaction with the permission module; and

an executable portion for causing a computer to allow the transaction if the user does not need to authenticate the user's identity.

26. The computer program product of claim 25, wherein the non-transitory computer readable medium further comprises:

an executable portion for causing a computer to request authentication of the user's identity based on the comparison of the transaction with the permission module;

an executable portion for causing a computer to compare an input from the user with the authentication module; and

an executable portion for causing a computer to allow the transaction if the user is authorized to perform the transaction based on the comparison of the input with the authentication module.

27. The computer program product of claim 25, further comprising an executable portion for causing a computer to determine the user's location when the user is conducting the transaction.

28. The computer program product of claim 25, further comprising memory coupled to the non-transitory computer readable medium.

29. The computer program product of claim 28, wherein the memory stores at least one of financial account information for the user, instructions associated with the permission module for the user, and security features associated with the authentication module for the user.

30. The computer program product of claim 29, wherein the user's financial account information consists of information associated with at least one of a checking account, a savings account, a money market account, a credit account, an investment account, and a rewards points account.

31. The computer program product of claim 25, wherein the permission module requires the user to authenticate the user's identity if a transaction amount is over a predetermined dollar amount.

32. The computer program product of claim 25, wherein the permission module requires the user to authenticate the user's identity if the transaction is occurring at a non-approved merchant.

33. The computer program product of claim 32, wherein the non-approved merchant is a merchant that the user has not purchased from previously.

34. The computer program product of claim 25, wherein the permission module requires the user to authenticate the user's identity if the user has not authenticated the identity within a predetermined time period.

35. The computer program product of claim 25, wherein the permission module requires the user to authenticate the user's identity if the user is outside of predetermined geographical areas.

36. The computer program product of claim 25, wherein the permission module requires the user to authenticate the user's identity if a transaction amount would lower a balance in the user's account below a predetermined level.

37. The computer program product of claim 25, wherein the permission module requires the user to authenticate the user's identity if the user has already conducted a predetermined number of transactions within a predetermined time period.

38. The computer program product of claim 25, wherein allowing the transaction comprises determining an account from which a payment for the transaction is made.

39. The computer program product of claim 38, wherein determining the account comprises comparing the transaction to instructions received from the user.

MOBILE TRANSACTION DEVICE SECURITY SYSTEM

ABSTRACT

Embodiments of the invention include apparatuses, methods, and computer-program products that provide for a unique financial transaction security system. In one embodiment, the financial transaction security system receives a security protocol from a user. The security protocol includes instructions for allowing transactions without authentication and security features for the user if authentication is necessary. The system then determines that the user is conducting a transaction, compares the transaction to the instructions, and determines whether the transaction can occur without authentication. If the user is required to authenticate his identity, the system requests input from the user, compares the input to the security feature, and determines if the user is authenticated. The user is able to customize both the instructions and the security features to provide greater control over financial transaction security.

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

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	4508US1.014033.1145
		Application Number	
Title of Invention	MOBILE TRANSACTION DEVICE SECURITY SYSTEM		
<p>The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.</p> <p>This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.</p>			

Secrecy Order 37 CFR 5.2

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

Applicant Information:

Applicant 1					
Applicant Authority ☒ Inventor		☐ Legal Representative under 35 U.S.C. 117		☐ Party of Interest under 35 U.S.C. 118	
Prefix	Given Name	Middle Name	Family Name	Suffix	
	David	M.	Grigg		
Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service					
City	Rock Hill	State/Province	SC	Country of Residence	US
Citizenship under 37 CFR 1.41(b)		US			
Mailing Address of Applicant:					
Address 1		c/o Bank of America Mailcode: NC1-002-29-01			
Address 2		101 South Tryon Street			
City	Charlotte	State/Province	NC		
Postal Code	28255	Country	US		
Applicant 2					
Applicant Authority ☒ Inventor		☐ Legal Representative under 35 U.S.C. 117		☐ Party of Interest under 35 U.S.C. 118	
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Patrick	B.	Kelly	Jr.	
Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service					
City	Charlotte	State/Province	NC	Country of Residence	US
Citizenship under 37 CFR 1.41(b)		US			
Mailing Address of Applicant:					
Address 1		c/o Bank of America, Mailcode: NC1-002-29-01			
Address 2		101 South Tryon Street			
City	Charlotte	State/Province	NC		
Postal Code	28255	Country	US		
Applicant 3					
Applicant Authority ☒ Inventor		☐ Legal Representative under 35 U.S.C. 117		☐ Party of Interest under 35 U.S.C. 118	
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Alicia	C.	Jones		
Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service					
City	Fort Mill	State/Province	SC	Country of Residence	US

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

Application Data Sheet 37 CFR 1.76		Attorney Docket Number 4508US1.014033.1145	
		Application Number	
Title of Invention	MOBILE TRANSACTION DEVICE SECURITY SYSTEM		
Citizenship under 37 CFR 1.41(b)	US		
Mailing Address of Applicant:			
Address 1	c/o Bank of America, Mailcode: NC1-002-29-01		
Address 2	101 South Tryon Street		
City	Charlotte	State/Province	NC
Postal Code	28255	Country	US
Applicant 4			
Applicant Authority	☒ Inventor ☐ Legal Representative under 35 U.S.C. 117 ☐ Party of Interest under 35 U.S.C. 118		
Prefix	Given Name	Middle Name	Family Name Suffix
	Marc	B.	Keller
Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service			
City	Charlotte	State/Province	NC Country of Residence US
Citizenship under 37 CFR 1.41(b)	US		
Mailing Address of Applicant:			
Address 1	c/o Bank of America, Mailcode: NC1-002-29-01		
Address 2	101 South Tryon Street		
City	Charlotte	State/Province	NC
Postal Code	28255	Country	US
All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the Add button.			<input type="button" value="Add"/>

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).	
☐ An Address is being provided for the correspondence information of this application.	
Customer Number	69603
Email Address	<input type="button" value="Add Email"/> <input type="button" value="Remove Email"/>

Application Information:

Title of the Invention	MOBILE TRANSACTION DEVICE SECURITY SYSTEM		
Attorney Docket Number	4508US1.014033.1145	Small Entity Status Claimed ☐	
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)		Sub Class (if any)	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)	9	Suggested Figure for Publication (if any)	

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

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	4508US1.014033.1145
		Application Number	
Title of Invention	MOBILE TRANSACTION DEVICE SECURITY SYSTEM		

Publication Information:

☐	Request Early Publication (Fee required at time of Request 37 CFR 1.219)
☐	Request Not to Publish. I hereby request that the attached application not be published under 35 U.S. C. 122(b) and certify that the invention disclosed in the attached application has not and will not be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Enter either Customer Number or complete the Representative Name section below. If both sections are completed the Customer Number will be used for the Representative Information during processing.			
Please Select One:	☒ Customer Number	☐ US Patent Practitioner	☐ Limited Recognition (37 CFR 11.9)
Customer Number	69603		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.					
Prior Application Status		Patented		Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the Add button.					

Foreign Priority Information:

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).			
Remove			
Application Number	Country ¹	Parent Filing Date (YYYY-MM-DD)	Priority Claimed
			☐ Yes ☐ No
Additional Foreign Priority Data may be generated within this form by selecting the Add button.			

Assignee Information:

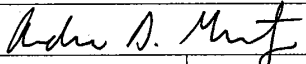
Providing this information in the application data sheet does not substitute for compliance with any requirement of part 3 of Title 37 of the CFR to have an assignment recorded in the Office.
Assignee 1

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

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	4508US1.014033.1145
		Application Number	
Title of Invention	MOBILE TRANSACTION DEVICE SECURITY SYSTEM		

If the Assignee is an Organization check here. ☒			
Organization Name	BANK OF AMERICA CORPORATION		
Mailing Address Information:			
Address 1	101 South Tryon Street		
Address 2			
City	Charlotte	State/Province	NC
Country	US	Postal Code	28255
Phone Number		Fax Number	
Email Address			
Additional Assignee Data may be generated within this form by selecting the Add button.			

Signature:

A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.					
Signature			Date (YYYY-MM-DD)	2011-01-31	
First Name	Andrew D.	Last Name	Gerschutz	Registration Number	65529

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

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

UTILITY PATENT APPLICATION TRANSMITTAL (Only for new nonprovisional applications under 37 CFR 1.53(b))	Attorney Docket No 4508US1.014033.1145
	First Named Inventor David M. Grigg et al.
	Title MOBILE TRANSACTION DEVICE SECURITY SYSTEM
	Filed via EFS-Web on January 31, 2011

ADDRESS TO: **COMMISSIONER FOR PATENTS**
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

Transmitted herewith for filing in the United States Patent Office is a patent application for:

Inventors: David M. Grigg; Patrick B. Kelly; Alicia C. Jones; Marc B. Keller

Assignee of this invention is Bank of America Corporation

1. ☒ The Filing Fee has been calculated as shown below:
 2. ☐ No Applicant claims Small Entity Status. See 37 CFR 1.27.

		Small Entity Rate		Large Entity Rate	
		No. Filed	No. Extra	Fee	Fee
BASIC FEE				\$ 0	\$ 330
SEARCH FEE				\$ 0	\$ 540
EXAMINATION FEE				\$ 0	\$ 220
TOTAL CLAIMS:	39 - 20 = 19	X 26 =		\$ 0	19 x 52 = \$ 988
INDEP CLAIMS:	3 - 3 = 0	X 110 =		\$ 0	0 x 220 = \$ 0
APPLICATION SIZE FEE	If the specification, drawings, and sequence listing exceed 100 sheets of paper, the application size fee due is \$270 (\$135 for small entity) for each additional 50 sheets or fraction thereof.			\$ 0	\$ 0
No MULTIPLE DEPENDENT CLAIMS PRESENTED		+195 =		\$ 0	+390 = \$ 0
*If the difference in Column 1 is less than zero, enter "0" in Column 2.		TOTAL		\$ 0	TOTAL \$2,078

The Commissioner is hereby authorized to credit any overpayment or charge any deficiency of the following fees to Deposit Acct. No. 13-4365.

- a. ☐ Fees required under 37 CFR 1.16 (National filing fees).
 b. ☐ Fees required under 37 CFR 1.17 (National application processing fees) including any extension of time fees under 37 CFR § 1.136(a) that are required for consideration of papers filed during prosecution.
- ☐ A check in the amount of \$ for the filing fee is enclosed.
- ☒ The filing fees paid via EFT in the amount of \$2,078.00 when e-filing.
- ☐ The above filing fee will be paid along with Applicant(s) Response to the Notice to File Missing Parts.
3. ☒ Specification [Total Pages 38]

4. ☒ 9 Sheets of Drawing(s) (35 USC 113)
5. ☐ Declaration [Total Pages]
- a. ☐ Newly executed (original or copy)
- b. ☐ Copy from a prior application (37 CFR 1.63(d)) (if box 18 completed)
- i. ☐ DELETION OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) & 1.33(b).
6. ☒ Application Data Sheet. See 37 CFR 1.76
7. ☐ CD-ROM or CD-R in duplicate, large table or Computer Program (Appendix)
8. Nucleotide and/or Amino Acid Sequence Submission (if applicable, all necessary)
- a. ☐ Computer Readable Copy (CRF)
- b. ☐ Request for Transfer of Computer Readable Form of Sequence Listing under 37 CFR § 1.821(e) and MPEP 2422.05 (must be compliant with new rules)
- c. ☐ Specification Sequence Listing on:
- i. ☐ CD-ROM or CD-R (3 copies); or
- ii. ☐ Paper (Pages)
- d. ☐ Statements verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

9. ☐ Assignment Papers (cover sheet & document(s) including a check for the \$40.00 fee)
10. ☐ 37 CFR 3.73(b) Statement and General Power of Attorney by Assignee. OR
☐ Application Specific Power of Attorney by Assignee
11. ☐ English Translation Document (if applicable)
12. ☐ Information Disclosure Statement (IDS)/PTO-1449; Copies of IDS Citations
13. ☐ Preliminary Amendment
14. ☐ Return Receipt Postcard (MPEP 503) (Should be specifically itemized)
15. ☐ Certified Copy of Priority Document(s) (if foreign priority is claimed)
☐ Foreign Priority is claimed as Application No. , filed
16. ☐ NonPublication Request under 35 U.S.C. 122(b)(2)(B)(i).
Applicant **must** attach form PTO/SB35 or its equivalent.
17. ☐ Request for Early Publication Under 37 CFR § 1.219. Fee of \$300.00 is enclosed.
18. **If a CONTINUING APPLICATION, check appropriate box and supply the requisite information below and in a preliminary amendment, or in an Application Data Sheet under 37 CFR 1.76:**
- ☐ Continuation ☐ Divisional ☐ Continuation in Part (CIP)

of prior Application No: _____; Filed _____

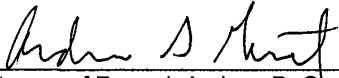
Prior Application Information: Examiner _____

Group/Art Unit: _____

For CONTINUATION or DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 5b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

19. **CORRESPONDENCE ADDRESS**
CUSTOMER NUMBER 69603

Signature:



Attorney of Record: Andrew D. Gerschütz
Registration No. 65,529

January 31, 2011

MOORE & VAN ALLEN PLLC FOR BOFA

430 Davis Drive, Suite 500
Post Office Box 13706
Research Triangle Park, NC 27709
Tel Triangle Office (919) 286-8000
Fax Triangle Office (919) 286-8199

Electronically filed via the EFS-Web Electronic Filing System of the United States Patent and Trademark Office on January 31, 2011.

SCORE Placeholder Sheet for IFW Content

Application Number: 13017823

Document Date: 1/31/2011

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

- Drawings – Other than Black and White Line Drawings

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

To access the documents in the SCORE database, refer to instructions developed by SIRA.

At the time of document entry (noted above):

- Examiners may access SCORE content via the eDAN interface.
- Other USPTO employees can bookmark the current SCORE URL (<http://es/ScoreAccessWeb/>).
- External customers may access SCORE content via the Public and Private PAIR interfaces.

Form Revision Date: February 8, 2006