UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/123,018	10/18/2022	11475105	MJAKP026	1102

21912 7590 09/28/2022

VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

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

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

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

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

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

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

Bjorn Markus Jakobsson, Portola Valley, CA;

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

RightQuestion, LLC, Portola Valley, CA

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/123,018	12/15/2020	Bjorn Markus Jakobsson	MJAKP026	1102

21912 7590 08/16/2022
VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

EXAMINER	
STEINLE, ANDREW J	

ART UNIT	PAPER NUMBER
2497	

NOTIFICATION DATE	DELIVERY MODE
08/16/2022	ELECTRONIC

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

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

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

usptocorrespondence@ip-patent.com

Response to Rule 312 Communication	Application No.	Applicant(s)	
	17/123,018	Jakobsson, Bjorn Markus	
	Examiner	Art Unit	AIA (FITF) Status
	ANDREW J STEINLE	2497	No

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

1. ☑ The amendment filed on 09 August 2022 under 37 CFR 1.312 has been considered, and has been:
   a) ☑ entered.
   b) ☐ entered as directed to matters of form not affecting the scope of the invention.
   c) ☐ disapproved because the amendment was filed after the payment of the issue fee.
      Any amendment filed after the date the issue fee is paid must be accompanied by a petition under 37 CFR 1.313(c)(1) and the required fee to withdraw the application from issue.
   d) ☐ disapproved. See explanation below.
   e) ☐ entered in part. See explanation below.
   f) ☐ not entered because the supplemental or corrected Application Data sheet (ADS)
      ☐ was not accompanied by a petition to accept an unintentionally delayed claim under 37 CFR 1.55 or 27 CFR 1.78;
      ☐ did not identify the information being changed in accordance with 37 CFR 1.76(c)(2);
      ☐ was not properly signed in accordance with 37 CFR 1.76(e) (or 37 CFR 1.33(b) for applications filed prior to September 16, 2012).

/ANDREW J STEINLE/
Primary Examiner, Art Unit 2497

OK TO ENTER: /A.J.S/

08/11/2022

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.:	17/123,018	Examiner:	Andrew J. Steinle
Filed:	December 15, 2020	Art Unit:	2497
Confirmation No.:	1102	Docket No.:	MJAKP026
First Inventor:	Bjorn Markus Jakobsson		
Title:	AUTHENTICATION TRANSLATION		

AMENDMENT AFTER ALLOWANCE, BEFORE/WITH PAYMENT OF ISSUE FEE PURSUANT TO 37 C.F.R. §1.312

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

Dear Sir:

Please amend the above-identified application as follows:

IN THE CLAIMS

Please amend the claims as follows:

1. (Previously presented) A system, comprising:

one or more processors configured to:

receive, at a first device, a request to access a resource external to the first device, wherein the resource external to the first device is associated with a user;

access at least one record stored on the first device, the at least one record including authentication information associated with the user and credential information associated with the external resource to which the user has requested access, wherein the credential information comprises a cryptographic key;

receive authentication input from the user;

determine that the authentication input from the user matches the authentication information associated with the user included in the at least one record stored on the first device;

retrieve at least a portion of the credential information from the at least one record stored on the first device;

facilitate access of the user to the external resource at least in part by transmitting, on behalf of the user, from the first device, output based at least in part on the at least portion of the credential information retrieved from the at least one record, wherein the user of the first device is granted access to the external resource based at least in part on the output transmitted from the first device on behalf of the user; and

based at least in part on the first device being a same brand as a second device, initiate a backup, to the second device, of at least a portion of the at least one record; and

a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.

2. (Original) The system of claim 1, wherein the second device is used to authenticate the user to one or more external resources.

3. (Original) The system of claim 1, wherein the backup is completed after the first device has performed a verification that the second device conforms to a policy associated with the at least one record stored on the first device.

4. (Original) The system of claim 1, wherein the backup is completed after a secure channel is established by at least one of the first device and the second device.

5. (Original) The system of claim 1, wherein the first device and the second device are configured to complete a pairing process.

6. (Original) The system of claim 5, wherein the pairing process comprises a comparison of data generated from one or more authentication inputs.

7. (Original) The system of claim 1, wherein subsequent to completion of the backup, the second device comprises a first profile associated with the user of the first device, and a second profile associated with a second user different from the user of the first device.

8. (Original) The system of claim 1, wherein the one or more processors are further configured to:

determine that the authentication input from the user does not match authentication information of a first profile; and

subsequent to determining that the authentication input from the user does not match the authentication information of the first profile, determine that the authentication input from the user matches authentication information of a second profile, wherein the first profile is associated with a different user than the second profile.

9. (Currently amended) The system of claim 1, wherein the at least one record stored on the first device is stored in a secure storage, and wherein the one or more processors are configured to access the at least one record stored on the secure storage using a restricted interface.

10. (Original) The system of claim 9, wherein the restricted interface comprises a dedicated physical connection.

11. (Original) The system of claim 9, wherein the restricted interface comprises an application programming interface.

12. (Original) The system of claim 1, wherein the backup causes a certificate to be transmitted to the second device.

13. (Original) The system of claim 12, wherein the certificate is generated at least in part by the first device.

14. (Original) The system of claim 1, wherein the authentication input from the user is received using a biometric user input element.

15. (Original) The system of claim 1, wherein the backup comprises copying a modified version of a vault to the second device.

16. (Cancelled)

17. (Previously presented) A method, comprising:

receiving, at a first device, a request to access a resource external to the first device, wherein the resource external to the first device is associated with a user;

accessing at least one record stored on the first device, the at least one record including authentication information associated with the user and credential information associated with the external resource to which the user has requested access, wherein the credential information comprises a cryptographic key;

receiving authentication input from the user;

determining that the authentication input from the user matches the authentication information associated with the user included in the at least one record stored on the first device;

retrieving at least a portion of the credential information from the at least one record stored on the first device;

facilitating access of the user to the external resource at least in part by transmitting, on behalf of the user, from the first device, output based at least in part on the at least portion of the credential information retrieved from the at least one record, wherein the user of the first device is granted access to the external resource based at least in part on the output transmitted from the first device on behalf of the user; and

based at least in part on the first device being a same brand as a second device, initiating a backup, to the second device, of at least a portion of the at least one record.

18. (Previously presented) A computer program product embodied in a non-transitory computer readable storage medium and comprising computing instructions for:

receiving, at a first device, a request to access a resource external to the first device, wherein the resource external to the first device is associated with a user;

accessing at least one record stored on the first device, the at least one record including authentication information associated with the user and credential information associated with the external resource to which the user has requested access, wherein the credential information comprises a cryptographic key;

receiving authentication input from the user;

determining that the authentication input from the user matches the authentication information associated with the user included in the at least one record stored on the first device;

retrieving at least a portion of the credential information from the at least one record stored on the first device;

facilitating access of the user to the external resource at least in part by transmitting, on behalf of the user, from the first device, output based at least in part on the at least portion of the credential information retrieved from the at least one record, wherein the user of the first device is granted access to the external resource based at least in part on the output transmitted from the first device on behalf of the user; and

based at least in part on the first device being a same brand as a second device, initiating a backup, to the second device, of at least a portion of the at least one record.

19. (Previously presented) The system of claim 1, wherein the one or more processors are configured to access records associated with at least two different users.

20. (Previously presented) The system of claim 19, wherein the records associated with the at least two different users are stored on the first device.

21. (Previously presented) The method of claim 17, comprising accessing records associated with at least two different users.

22. (Previously presented) The method of claim 21, wherein the records associated with the at least two different users are stored on the first device.

23. (Previously presented) The method of claim 17, wherein the second device is used to authenticate the user to one or more external resources.

24. (Previously presented) The method of claim 17, wherein the backup is completed after the first device has performed a verification that the second device conforms to a policy associated with the at least one record stored on the first device.

25. (Previously presented) The method of claim 17, wherein the backup is completed after a secure channel is established by at least one of the first device and the second device.

26. (Previously presented) The method of claim 17, wherein the first device and the second device are configured to complete a pairing process.

27. (Previously presented) The method of claim 26, wherein the pairing process comprises a comparison of data generated from one or more authentication inputs.

28. (Previously presented) The method of claim 17, wherein subsequent to completion of the backup, the second device comprises a first profile associated with the user of the first device, and a second profile associated with a second user different from the user of the first device.

29. (Previously presented) The method of claim 17, further comprising:

determining that the authentication input from the user does not match authentication information of a first profile; and

subsequent to determining that the authentication input from the user does not match the authentication information of the first profile, determining that the authentication input from the user matches authentication information of a second profile, wherein the first profile is associated with a different user than the second profile.

30. (Currently amended) The method of claim 17, wherein the at least one record stored on the first device is stored in a secure storage, and further comprising accessing the <u>at least one</u> record stored on the secure storage using a restricted interface.

31. (Previously presented) The method of claim 30, wherein the restricted interface comprises a dedicated physical connection.

32. (Previously presented) The method of claim 30, wherein the restricted interface comprises an application programming interface.

33. (Previously presented) The method of claim 17, wherein the backup causes a certificate to be transmitted to the second device.

34. (Previously presented) The method of claim 33, wherein the certificate is generated at least in part by the first device.

35. (Previously presented) The method of claim 17, wherein the authentication input from the user is received using a biometric user input element.

36. (Previously presented) The method of claim 17, wherein the backup comprises copying a modified version of a vault to the second device.

REMARKS

A Notice of Allowance has been received in the above-identified application but the issue fee has not yet been paid. Applicant hereby respectfully requests that on recommendation of the Examiner and approval by the Commissioner that this amendment be entered.

A review of the allowed claims has revealed minor antecedent basis errors in Claims 9 and 30 which are now sought to be corrected. In view of these minor errors, it is respectfully submitted that no new search is required.

Reconsideration of the application and allowance of all claims are respectfully requested based on the preceding remarks. If at any time the Examiner believes that an interview would be helpful, please contact the undersigned.

Respectfully submitted,

Dated: August 9, 2022

/Yeu-Ting George Cheng/

Yeu-Ting George Cheng
Registration No. 69408
408-207-4765

VAN PELT, YI & JAMES LLP
10050 N. Foothill Blvd., Suite 200
Cupertino, CA 95014
Fax 408-973-2595

Electronic Patent Application Fee Transmittal

Application Number:	17123018
Filing Date:	15-Dec-2020
Title of Invention:	AUTHENTICATION TRANSLATION
First Named Inventor/Applicant Name:	Bjorn Markus Jakobsson
Filer:	Yeu-Ting George Cheng/Elaine Nguyen
Attorney Docket Number:	MJAKP026

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
UTILITY APPL ISSUE FEE	1501	1	1200	1200

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**1200**

Electronic Acknowledgement Receipt	
EFS ID:	46376760
Application Number:	17123018
International Application Number:	
Confirmation Number:	1102
Title of Invention:	AUTHENTICATION TRANSLATION
First Named Inventor/Applicant Name:	Bjorn Markus Jakobsson
Customer Number:	21912
Filer:	Yeu-Ting George Cheng/Elaine Nguyen
Filer Authorized By:	Yeu-Ting George Cheng
Attorney Docket Number:	MJAKP026
Receipt Date:	09-AUG-2022
Filing Date:	15-DEC-2020
Time Stamp:	19:38:06
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$1200
RAM confirmation Number	E202289J38532848
Deposit Account	500685
Authorized User	Elaine Nguyen
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.16 (National application filing, search, and examination fees) 37 CFR 1.17 (Patent application and reexamination processing fees)	

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	MJAKP026_IF_Transmittal.pdf	2093783 d6ff4a2d92235b90af4c7f53668cd43ba01e2c59	no	1
Warnings:					
Information:					
2	Amendment after Notice of Allowance (Rule 312)	MJAKP026_AMD_312.pdf	102927 f4cb15f37e60ef72333da122b64983cf8c081491	no	8
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	37981 345c5bfcea4a40cf8eec7cf4c5e66169a9cd9da3	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	2234691		

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

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PART B - FEE(S) TRANSMITTAL

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

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

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

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

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

21912 7590 07/21/2022
VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

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

Certificate of Mailing or Transmission

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

Elaine Nguyen	(Typed or printed name)
/Elaine Nguyen/	(Signature)
August 9, 2022	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/123,018	12/15/2020	Bjorn Markus Jakobsson	MJAKP026	1102

TITLE OF INVENTION: AUTHENTICATION TRANSLATION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	~~SMALL~~ UNDISCOUNTED	~~$600~~ $1200	$0.00	$0.00	~~$600~~ $1200	10/21/2022

EXAMINER	ART UNIT	CLASS-SUBCLASS
STEINLE, ANDREW J	2497	216-024000

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

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

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

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

1 Van Pelt, Yi & James LLP
2
3

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

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: RightQuestion, LLC

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Portola Valley, CA

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

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

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

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

☑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. 50-0685

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

☐ Applicant certifying micro entity status. See 37 CFR 1.29

☐ Applicant asserting small entity status. See 37 CFR 1.27

☑ Applicant changing to regular undiscounted fee status.

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

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

Authorized Signature /Yeu-Ting George Cheng/ Date August 9, 2022

Typed or printed name Yeu-Ting George Cheng Registration No. 69408

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.:	17/123,018	Examiner:	Andrew J. Steinle
Filed:	December 15, 2020	Art Unit:	2497
Confirmation No.:	1102	Docket No.:	MJAKP026
First Inventor:	Bjorn Markus Jakobsson		
Title:	AUTHENTICATION TRANSLATION		

AMENDMENT AFTER ALLOWANCE, BEFORE/WITH PAYMENT OF ISSUE FEE PURSUANT TO 37 C.F.R. §1.312

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

Dear Sir:

Please amend the above-identified application as follows:

IN THE CLAIMS

Please amend the claims as follows:

1. (Previously presented) A system, comprising:

one or more processors configured to:

receive, at a first device, a request to access a resource external to the first device, wherein the resource external to the first device is associated with a user;

access at least one record stored on the first device, the at least one record including authentication information associated with the user and credential information associated with the external resource to which the user has requested access, wherein the credential information comprises a cryptographic key;

receive authentication input from the user;

determine that the authentication input from the user matches the authentication information associated with the user included in the at least one record stored on the first device;

retrieve at least a portion of the credential information from the at least one record stored on the first device;

facilitate access of the user to the external resource at least in part by transmitting, on behalf of the user, from the first device, output based at least in part on the at least portion of the credential information retrieved from the at least one record, wherein the user of the first device is granted access to the external resource based at least in part on the output transmitted from the first device on behalf of the user; and

based at least in part on the first device being a same brand as a second device, initiate a backup, to the second device, of at least a portion of the at least one record; and

a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.

2. (Original) The system of claim 1, wherein the second device is used to authenticate the user to one or more external resources.

3. (Original) The system of claim 1, wherein the backup is completed after the first device has performed a verification that the second device conforms to a policy associated with the at least one record stored on the first device.

4. (Original) The system of claim 1, wherein the backup is completed after a secure channel is established by at least one of the first device and the second device.

5. (Original) The system of claim 1, wherein the first device and the second device are configured to complete a pairing process.

6. (Original) The system of claim 5, wherein the pairing process comprises a comparison of data generated from one or more authentication inputs.

7. (Original) The system of claim 1, wherein subsequent to completion of the backup, the second device comprises a first profile associated with the user of the first device, and a second profile associated with a second user different from the user of the first device.

8. (Original) The system of claim 1, wherein the one or more processors are further configured to:

determine that the authentication input from the user does not match authentication information of a first profile; and

subsequent to determining that the authentication input from the user does not match the authentication information of the first profile, determine that the authentication input from the user matches authentication information of a second profile, wherein the first profile is associated with a different user than the second profile.

9. (Currently amended) The system of claim 1, wherein the at least one record stored on the first device is stored in a secure storage, and wherein the one or more processors are configured to access the at least one record stored on the secure storage using a restricted interface.

10. (Original) The system of claim 9, wherein the restricted interface comprises a dedicated physical connection.

11. (Original) The system of claim 9, wherein the restricted interface comprises an application programming interface.

12. (Original) The system of claim 1, wherein the backup causes a certificate to be transmitted to the second device.

13. (Original) The system of claim 12, wherein the certificate is generated at least in part by the first device.

14. (Original) The system of claim 1, wherein the authentication input from the user is received using a biometric user input element.

15. (Original) The system of claim 1, wherein the backup comprises copying a modified version of a vault to the second device.

16. (Cancelled)

17. (Previously presented) A method, comprising:

receiving, at a first device, a request to access a resource external to the first device, wherein the resource external to the first device is associated with a user;

accessing at least one record stored on the first device, the at least one record including authentication information associated with the user and credential information associated with the external resource to which the user has requested access, wherein the credential information comprises a cryptographic key;

receiving authentication input from the user;

determining that the authentication input from the user matches the authentication information associated with the user included in the at least one record stored on the first device;

retrieving at least a portion of the credential information from the at least one record stored on the first device;

facilitating access of the user to the external resource at least in part by transmitting, on behalf of the user, from the first device, output based at least in part on the at least portion of the credential information retrieved from the at least one record, wherein the user of the first device is granted access to the external resource based at least in part on the output transmitted from the first device on behalf of the user; and

based at least in part on the first device being a same brand as a second device, initiating a backup, to the second device, of at least a portion of the at least one record.

18. (Previously presented) A computer program product embodied in a non-transitory computer readable storage medium and comprising computing instructions for:

receiving, at a first device, a request to access a resource external to the first device, wherein the resource external to the first device is associated with a user;

accessing at least one record stored on the first device, the at least one record including authentication information associated with the user and credential information associated with the external resource to which the user has requested access, wherein the credential information comprises a cryptographic key;

receiving authentication input from the user;

determining that the authentication input from the user matches the authentication information associated with the user included in the at least one record stored on the first device;

retrieving at least a portion of the credential information from the at least one record stored on the first device;

facilitating access of the user to the external resource at least in part by transmitting, on behalf of the user, from the first device, output based at least in part on the at least portion of the credential information retrieved from the at least one record, wherein the user of the first device is granted access to the external resource based at least in part on the output transmitted from the first device on behalf of the user; and

based at least in part on the first device being a same brand as a second device, initiating a backup, to the second device, of at least a portion of the at least one record.

19. (Previously presented) The system of claim 1, wherein the one or more processors are configured to access records associated with at least two different users.

20. (Previously presented) The system of claim 19, wherein the records associated with the at least two different users are stored on the first device.

21. (Previously presented) The method of claim 17, comprising accessing records associated with at least two different users.

22. (Previously presented) The method of claim 21, wherein the records associated with the at least two different users are stored on the first device.

23. (Previously presented) The method of claim 17, wherein the second device is used to authenticate the user to one or more external resources.

24. (Previously presented) The method of claim 17, wherein the backup is completed after the first device has performed a verification that the second device conforms to a policy associated with the at least one record stored on the first device.

25. (Previously presented) The method of claim 17, wherein the backup is completed after a secure channel is established by at least one of the first device and the second device.

26. (Previously presented) The method of claim 17, wherein the first device and the second device are configured to complete a pairing process.

27. (Previously presented) The method of claim 26, wherein the pairing process comprises a comparison of data generated from one or more authentication inputs.

28. (Previously presented) The method of claim 17, wherein subsequent to completion of the backup, the second device comprises a first profile associated with the user of the first device, and a second profile associated with a second user different from the user of the first device.

29. (Previously presented) The method of claim 17, further comprising:

determining that the authentication input from the user does not match authentication information of a first profile; and

subsequent to determining that the authentication input from the user does not match the authentication information of the first profile, determining that the authentication input from the user matches authentication information of a second profile, wherein the first profile is associated with a different user than the second profile.

30. (Currently amended) The method of claim 17, wherein the at least one record stored on the first device is stored in a secure storage, and further comprising accessing the <u>at least one</u> record stored on the secure storage using a restricted interface.

31. (Previously presented) The method of claim 30, wherein the restricted interface comprises a dedicated physical connection.

32. (Previously presented) The method of claim 30, wherein the restricted interface comprises an application programming interface.

33. (Previously presented) The method of claim 17, wherein the backup causes a certificate to be transmitted to the second device.

34. (Previously presented) The method of claim 33, wherein the certificate is generated at least in part by the first device.

35. (Previously presented) The method of claim 17, wherein the authentication input from the user is received using a biometric user input element.

36. (Previously presented) The method of claim 17, wherein the backup comprises copying a modified version of a vault to the second device.

REMARKS

A Notice of Allowance has been received in the above-identified application but the issue fee has not yet been paid. Applicant hereby respectfully requests that on recommendation of the Examiner and approval by the Commissioner that this amendment be entered.

A review of the allowed claims has revealed minor antecedent basis errors in Claims 9 and 30 which are now sought to be corrected. In view of these minor errors, it is respectfully submitted that no new search is required.

Reconsideration of the application and allowance of all claims are respectfully requested based on the preceding remarks. If at any time the Examiner believes that an interview would be helpful, please contact the undersigned.

Respectfully submitted,

Dated: August 9, 2022

/Yeu-Ting George Cheng/

Yeu-Ting George Cheng
Registration No. 69408
408-207-4765

VAN PELT, YI & JAMES LLP
10050 N. Foothill Blvd., Suite 200
Cupertino, CA 95014
Fax 408-973-2595

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

21912 7590 07/21/2022

VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

EXAMINER	
STEINLE, ANDREW J	
ART UNIT	PAPER NUMBER
2497	

DATE MAILED: 07/21/2022

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/123,018	12/15/2020	Bjorn Markus Jakobsson	MJAKP026	1102

TITLE OF INVENTION: AUTHENTICATION TRANSLATION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$600	$0.00	$0.00	$600	10/21/2022

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

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

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

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

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

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PTOL-85 (Rev. 02/11)

PART B - FEE(S) TRANSMITTAL

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

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

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

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

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

21912 7590 07/21/2022
VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

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

Certificate of Mailing or Transmission

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

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/123,018	12/15/2020	Bjorn Markus Jakobsson	MJAKP026	1102

TITLE OF INVENTION: AUTHENTICATION TRANSLATION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$600	$0.00	$0.00	$600	10/21/2022

EXAMINER	ART UNIT	CLASS-SUBCLASS
STEINLE, ANDREW J	2497	216-024000

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

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

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

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

1_____
2_____
3_____

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

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

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

4a. Fees submitted: ❑Issue Fee ❑Publication Fee (if required) ❑Advance Order - # of Copies _____

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

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

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

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

❑ Applicant certifying micro entity status. See 37 CFR 1.29

❑ Applicant asserting small entity status. See 37 CFR 1.27

❑ Applicant changing to regular undiscounted fee status.

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

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

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/123,018	12/15/2020	Bjorn Markus Jakobsson	MJAKP026	1102

21912 7590 07/21/2022

VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

EXAMINER	
STEINLE, ANDREW J	
ART UNIT	PAPER NUMBER
2497	

DATE MAILED: 07/21/2022

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

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

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

PTOL-85 (Rev. 02/11)

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 17/123,018	Applicant(s) Jakobsson, Bjorn Markus	
	Examiner ANDREW J STEINLE	Art Unit 2497	AIA (FITF) Status No

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

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

1. ☑ This communication is responsive to 6/17/2022.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

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

3. ☑ The allowed claim(s) is/are 1-15 and 17-36 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information , please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

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

   Certified copies:

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

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

   * Certified copies not received: _____ .

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

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

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

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

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☑ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____.
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date. _____.
5. ☐ Examiner's Amendment/Comment
6. ☑ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/ANDREW J STEINLE/
Primary Examiner, Art Unit 2497

DETAILED ACTION

Notice of Pre-AIA or AIA Status

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

Response to Amendment

This action is in response to the communications and remarks filed on 6/17/2022. **Claims 1-15 and 17-36** are presently pending for examination.

Response to Arguments

Applicant's arguments, see pages 9-10, filed 6/17/2022, regarding the 103 rejections of **Claims 1-15 and 17-36,** have been fully considered and are persuasive. The rejections have been withdrawn and the claims are in condition for allowance.

Terminal Disclaimer

The terminal disclaimer filed on 6/17/2022 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of **U.S. Patents 9,294,452, 10,360,351, 10,521,568, and 10,929,512** has been reviewed and is accepted. The terminal disclaimer has been recorded.

Allowable Subject Matter

Claims 1-15 and 17-36 are allowed.

This communication warrants No Examiner's Reason for Allowance, applicant's reply make evident the reasons for allowance, satisfying the “record as a whole” proviso of the rule 37 CFR 1.104(e). **Specifically, the substance of applicant's arguments filed on 6/17/2022 are persuasive**, as such the reasons for allowance are in all probability evident from the record and no statement is deemed necessary (see MPEP 1302.14).

Any comments Applicants considers necessary must be submitted no later than the payment of the Issue Fee and to avoid processing delays, should preferable accompany the Issue Fees. Such submission should be clearly labeled "Comments on Statement of Reasons for Allowance". In event of any post-allowance papers (e.g. IDS, 312 amendment, petition, etc.), Applicant is exhorted to mail papers to the Production Control branch in Publications or faxed to post-allowance papers correspondence branch at (703) 308-5864 to expedite issuing process or call PUB's Customer Service if any questions at (703) 305-8497.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ANDREW J STEINLE whose telephone number is (571)272-9923. The examiner can normally be reached M-F 10am-6pm CT.

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

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Eleni Shiferaw can be reached on (571) 272-3867. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

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

/ANDREW J STEINLE/
Primary Examiner, Art Unit 2497

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/123,018	Jakobsson, Bjorn Markus
	Examiner	Art Unit
	ANDREW J STEINLE	2497

CPC - Searched*		
Symbol	**Date**	**Examiner**
CPC Classification Search G06F21/10, 121, 128, 31, 32, 44, H04L63 /0861, 10, 20, 0815, 0823, 083, 0869 limited by text	07/12/2022	AS

CPC Combination Sets - Searched*		
Symbol	**Date**	**Examiner**

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	**Date**	**Examiner**
PE2E Search class limited w/text search (see search history)	07/12/2022	AS
PE2E Search inventor and assignee search (see search history)	07/12/2022	AS
PE2E Search text search (see search history)	07/12/2022	AS
NPL Search via Google patents	07/12/2022	AS

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**
	General Interference and search of claims (USPGPB, USPAT)	07/12/2022	AS

/ANDREW J STEINLE/ Primary Examiner, Art Unit 2497	

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/123,018	Jakobsson, Bjorn Markus
	Examiner	**Art Unit**
	ANDREW J STEINLE	2497

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

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

CLAIM		DATE								
Final	Original	01/25/2022	07/12/2022							
1	1	✓	=							
2	2	✓	=							
3	3	✓	=							
4	4	✓	=							
5	5	✓	=							
6	6	✓	=							
7	7	✓	=							
8	8	✓	=							
9	9	✓	=							
10	10	✓	=							
11	11	✓	=							
12	12	✓	=							
13	13	✓	=							
14	14	✓	=							
15	15	✓	=							
	16	✓	-							
18	17	✓	=							
35	18	✓	=							
16	19	✓	=							
17	20	✓	=							
19	21	✓	=							
20	22	✓	=							
21	23		=							
22	24		=							
23	25		=							
24	26		=							
25	27		=							
26	28		=							
27	29		=							
28	30		=							
29	31		=							
30	32		=							
31	33		=							
32	34		=							
33	35		=							
34	36		=							

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/123,018	Jakobsson, Bjorn Markus
	Examiner	**Art Unit**
	ANDREW J STEINLE	2497

CPC						
Symbol					**Type**	**Version**
G06F	/	21	/	10	F	2013-01-01
H04L	/	63	/	0815	I	2013-01-01
H04L	/	63	/	0823	I	2013-01-01
H04L	/	63	/	0861	I	2013-01-01
G06F	/	21	/	31	I	2013-01-01
G06F	/	21	/	32	I	2013-01-01
G06F	/	21	/	44	I	2013-01-01
G06F	/	21	/	121	I	2013-01-01
G06F	/	21	/	128	I	2013-01-01
H04L	/	63	/	083	I	2013-01-01
H04L	/	63	/	10	I	2013-01-01
H04L	/	63	/	20	I	2013-01-01
H04L	/	63	/	08	I	2013-01-01
H04L	/	63	/	0281	A	2013-01-01
H04L	/	63	/	0869	A	2013-01-01

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

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	35	
/ANDREW J STEINLE/ Primary Examiner, Art Unit 2497	12 July 2022	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

U.S. Patent and Trademark Office — Part of Paper No.: 20220712

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/123,018	Jakobsson, Bjorn Markus
	Examiner	**Art Unit**
	ANDREW J STEINLE	2497

INTERNATIONAL CLASSIFICATION				
CLAIMED				
G06F	/	21	/	00

NON-CLAIMED				
	/		/	

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**

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

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	35	
/ANDREW J STEINLE/ Primary Examiner, Art Unit 2497	12 July 2022	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

U.S. Patent and Trademark Office — Part of Paper No.: 20220712

APPL-1002
APPLE INC. / Page 36 of 419

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/123,018	Jakobsson, Bjorn Markus
	Examiner	**Art Unit**
	ANDREW J STEINLE	2497

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

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	10	10	16	19	26	28								
2	2	11	11	17	20	27	29								
3	3	12	12	19	21	28	30								
4	4	13	13	20	22	29	31								
5	5	14	14	21	23	30	32								
6	6	15	15	22	24	31	33								
7	7		16	23	25	32	34								
8	8	18	17	24	26	33	35								
9	9	35	18	25	27	34	36								

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 35	
/ANDREW J STEINLE/ Primary Examiner, Art Unit 2497 (Primary Examiner)	12 July 2022 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 1

U.S. Patent and Trademark Office — Part of Paper No.: 20220712

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

BIB DATA SHEET

CONFIRMATION NO. 1102

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
17/123,018	12/15/2020	216	2497	MJAKP026

APPLICANTS
RightQuestion, LLC, Portola Valley, CA

INVENTORS
Bjorn Markus Jakobsson, Portola Valley, CA;

**** CONTINUING DATA ***************************
This application is a CIP of 17/027,481 09/21/2020
which is a CON of 16/773,767 01/27/2020 PAT 10929512
which is a CON of 16/563,715 09/06/2019 PAT 10824696
which is a CON of 16/273,797 02/12/2019 PAT 10521568
which is a CON of 15/042,636 02/12/2016 PAT 10360351
which is a CON of 13/706,254 12/05/2012 PAT 9294452
which claims benefit of 61/587,387 01/17/2012
and claims benefit of 61/569,112 12/09/2011

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
12/30/2020

Foreign Priority claimed	❑ Yes ☑ No	❑ Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
35 USC 119(a-d) conditions met	❑ Yes ☑ No		CA	15	~~22~~ 38	3
Verified and Acknowledged	/ANDREW J STEINLE/ Examiner's Signature	Initials				

ADDRESS
VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014
UNITED STATES

TITLE
AUTHENTICATION TRANSLATION

FILING FEE RECEIVED	FEES: Authority has been given in Paper	
1660	No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	❑ All Fees ❑ 1.16 Fees (Filing) ❑ 1.17 Fees (Processing Ext. of time) ❑ 1.18 Fees (Issue) ❑ Other _____ ❑ Credit

BIB (Rev. 05/07).

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L261	288	((("Jakobsson") near3 ("Bjorn") near3 ("Markus"))).INV.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2022/07/12 10:04 PM
L262	438	((("Jakobsson") near3 ("Bjorn") near3 ("Markus"))).INV.	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/07/12 10:04 PM
L263	14	(RightQuestion).as.	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/07/12 10:04 PM
L264	46	(("(H01836") or ("20110066858") or ("20110066858") or ("6055637") or ("20030084171") or ("20030140230") or ("20060157559") or ("5832211") or ("5862323") or ("5659165") or ("5825003") or ("6446218") or ("20020099671") or ("20040002878") or ("20070044144") or ("7450584") or ("20050058132") or	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:04 PM

APPL-1002
APPLE INC. / Page 39 of 419

		("6006018") or ("20090113522") or ("4924515") or ("8599267") or ("20090096871") or ("6668327") or ("6067623") or ("7089584") or ("7210167") or ("20030065940") or ("20060075224") or ("20050108546") or ("20100228967") or ("8094634") or ("20090122770") or ("7085840") or ("7275260") or ("7496751") or ("7903611") or ("7903611") or ("20030084170") or ("20030084172") or ("20030084288") or ("20030084302") or ("20080117879") or ("5594789") or ("5850450") or ("6061799") or ("6061799") or ("6078805") or ("6108789") or ("6134327") or ("6141752") or (").pn.")).PN.					
L265	10747	(bjorn jakobsson).in.	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:04 PM
L266	770	(bjorn jakobsson).in. and authentication	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:04 PM
L267	113	(bjorn jakobsson).in. and authentication and translation	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:04 PM
L268	22	authentication adj translator	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:04 PM
L269	206	(proxy intermediate intermediary behalf adj2 of) near4 (cookie certificate ticket credential) with (transaction bank merchant) and biometric	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:04 PM
L270	209	(proxy intermediate intermediary behalf adj2 of) near4 (cookie certificate ticket credential) with	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:04 PM

		(transaction bank merchant vendor) and biometric					
L271	3	(proxy intermediate intermediary behalf adj2 of) near4 (cookie certificate ticket credential) with (transaction bank merchant vendor) and biometric and (726/5-7,10,18-19,28 713/170,172,185-186 382/115).ccls.	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:04 PM
L272	391	(forward$3) near4 (cookie certificate ticket credential) with (transaction bank merchant vendor) and biometric	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:04 PM
L273	438	biometric with authenticat$ with (proxy$4 intermediate intermediary)	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:04 PM
L274	171	(biometric fingerprint retinal) with (authenticat$ authoriz$ valid$ verif$ confirm$4 near3 identity) near2 (proxy$4 intermediate intermediary)	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:04 PM
L275	15	L14 AND ((713/186).CCLS.)	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:04 PM
L276	41	(biometric or fingerprint or retinal) with (authenticat$ authoriz$ valid$ verif$ confirm$4 near3 identity) near2 (proxy$4 intermediate intermediary)	(FPRS; EPO; JPO; DERWENT)	OR	ON	ON	2022/07/12 10:04 PM
L277	1	"20090100269".pn. and (proxy intermediate intermediary behalf adj2 cookie certificate ticket credential transaction bank merchant biometric)	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:04 PM
L278	1	"20090100269".pn. and (proxy intermediate intermediary behalf adj2 cookie certificate ticket credential transaction bank merchant biometric authentication)	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:04 PM

L279	1	"20080120707".pn. and (proxy intermediate intermediary behalf adj2 cookie certificate ticket credential transaction bank merchant biometric authentication)	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:04 PM
L280	391	(forward$3) near4 (cookie certificate ticket credential) with (transaction bank merchant vendor) and biometric	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:04 PM
L281	438	biometric with authenticat$ with (proxy$4 intermediate intermediary)	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:04 PM
L282	3	L21 and renegotiat$3	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:04 PM
L283	1	"20110205016".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:04 PM
L284	2	("20120110341" "20100242102").pn.	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:04 PM
L285	1	"20110231652".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:04 PM
L286	10	(US-20090100269-$ or US-20110231651-$ or US-20050198348-$ or US-20060247982-$ or US-20110205016-$ or US-20120110341-$ or US-20100242102-$).did. or (US-7512965-$ or US-7950051-$ or US-8549300-$).did.	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:04 PM
L287	3	L26 and cookie	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:04 PM
L288	10	(US-20090100269-$ or US-20110231651-$ or US-20050198348-$ or US-20060247982-$ or US-20110205016-$ or US-20120110341-$ or US-20100242102-$).did. or (US-7512965-$ or US-7950051-$ or US-8549300-$).did.	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:04 PM
L289	10	(US-20090100269-$ or US-20110231651-$ or US-20050198348-$ or US-20060247982-$ or US-20110205016-$ or US-20120110341-$ or US-20100242102-	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:04 PM

		$).did. or (US-7512965-$ or US-7950051-$ or US-8549300-$).did.					
L290	16	("20040107170"|"20040236632"|"20050198348"|"20090100269"|"20100242102"|"20110205016"|"20110231651"|"20120110341"|"20120167193"|"6016476"|"7512965"|"7950051"|"8549300"|"8577813"|"8856539"|"9100826").PN.	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:04 PM
L291	7	L30 and credential	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:04 PM
L292	5	L31 and login	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:04 PM
L293	0	L32 and backup	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:04 PM
L294	10	(US-20090100269-$ or US-20110231651-$ or US-20050198348-$ or US-20060247982-$ or US-20110205016-$ or US-20120110341-$ or US-20100242102-$).did. or (US-7512965-$ or US-7950051-$ or US-8549300-$).did.	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:04 PM
L295	1	L34 and (password same change)	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:04 PM
L369	9055270	@ad<="20111209"	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:40 PM
L370	8	L36 and ((password near3 change) same (without near3 (user adj (input knowledge notification))))	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:40 PM
L371	1	"20090132807".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:40 PM
L372	42	@ad<="20111209" and renegotiation same proxy	(US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/07/12 10:40 PM
L373	3	@ad<="20111209" and (non-security adj transparent adj proxy)	(US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/07/12 10:40 PM
L374	3	"20130205360"	(US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/07/12 10:40 PM
L375	3	"20090132807"	(US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/07/12 10:40 PM
L376	2	"20110231651".pn.	(US-PGPUB; USPAT;	OR	ON	ON	2022/07/12

			EPO; JPO; DERWENT; IBM_TDB)				10:40 PM
L377	17	ssl adj renegotiation	(US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/07/12 10:40 PM
L378	12742	@ad<="20111209" and restricted adj access	(US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/07/12 10:40 PM
L379	4398	@ad<="20111209" and authenticat$ and (restricted adj access)	(US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/07/12 10:40 PM
L380	1192	@ad<="20111209" and authenticat$ and biometric and (restricted adj access)	(US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/07/12 10:40 PM
L381	341	@ad<="20111209" and authenticat$ and biometric and (restricted adj access) and proxy	(US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/07/12 10:40 PM
L382	2	("6178505" | "6453419").PN.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2022/07/12 10:40 PM
L383	78	@ad<="20111209" and (authenticat$ adj server) and (restricted adj access) and (access adj control adj policy)	(US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/07/12 10:40 PM
L384	82	@ad<="20111209" and (authenticat$ adj server) and (restricted adj access or partial adj access) and (access adj control adj policy)	(US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/07/12 10:40 PM
L385	32	@ad<="20111209" and (authenticat$3 adj server) and remot$3 and password adj (updat$3 chang$3) and biometric and legacy	(US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/07/12 10:40 PM
L386	32	@ad<="20111209" and (authenticat$3 adj server) and password adj (updat$3 chang$3) and biometric and legacy	(US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/07/12 10:41 PM
L387	5	@ad<="20111209" and updat$3 near3 (password) with (automatic automatically) with expir$3	(US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/07/12 10:41 PM
L388	16	("2007/0124807").URPN.	(USPAT)	OR	ON	ON	2022/07/12 10:41 PM
L389	1210	@ad<="20111209" and (use adj condition)	(US-PGPUB; USPAT; EPO; JPO;	OR	ON	ON	2022/07/12 10:41 PM

APPL-1002
APPLE INC. / Page 44 of 419

		near3 information	DERWENT; IBM_TDB)				
L390	129	biometric with (authenticat$ authoriz$ valid$ verif$ confirm$4 near3 identity) near2 (proxy$4 intermediate intermediary)	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:41 PM
L391	20748	@ad<="20111209" and 713/186,168,155,152.ccls.	(US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/07/12 10:41 PM
L392	18	(biometric or fingerprint or retinal) with (authenticat$ authoriz$ valid$ verif$ confirm$4 near3 identity) near2 (proxy$4 intermediate intermediary) and @ad<="20111209" and 713/186,168,155,152.ccls.	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:41 PM
L393	1	"8549300".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:41 PM
L394	8	(biometric or fingerprint or retinal) with (authenticat$ authoriz$ valid$ verif$ confirm$4 near3 identity) near2 (proxy$4 intermediate intermediary) and @ad<="20111209" and 726/1,5,4,21,26.ccls.	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:41 PM
L395	7	(biometric or fingerprint or retinal) with (authenticat$ authoriz$ valid$ verif$ confirm$4 near3 identity) near2 (proxy$4 intermediate intermediary) and @ad<="20111209" and 705/38,3,8,141,67.ccls.	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:41 PM
L396	1	"20080071545".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:41 PM
L397	171	(biometric or fingerprint or retinal) with (authenticat$ authoriz$ valid$ verif$ confirm$4 near3 identity) near2 (proxy$4 intermediate intermediary)	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:41 PM
L398	41	("2011/0289314").URPN.	(USPAT)	OR	ON	ON	2022/07/12 10:41 PM
L399	14960	@ad<="20111209" and authenticat$ and cookie	(US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/07/12 10:41 PM

L400	78	(proxy intermediate intermediary behalf adj2 of) near4 cookie and biometric	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:41 PM
L401	36971	@ad<="20111209" and biometric and (authenticat$ authoriz$ valid$ verif$ confirm$4) and (transmit transmission)	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:41 PM
L402	36971	@ad<="20111209" and biometric and (authenticat$ authoriz$ valid$ verif$ confirm$4) and (transmit transmission)	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:41 PM
L403	5135	@ad<="20111209" and biometric same (authenticat$ authoriz$ valid$ verif$ confirm$4) same (transmit transmission)	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 10:41 PM
L404	1393	@ad<="20111209" and biometric with (authenticat$ authoriz$ valid$ verif$ confirm$4) with (transmit transmission)	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 11:11 PM
L405	358	@ad<="20111209" and biometric with (authenticat$ authoriz$ valid$ verif$ confirm$4) with (transmit transmission) and (proxy intermediate intermediary behalf adj2 of)	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 11:11 PM
L406	1	"7107220".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 11:11 PM
L407	0	@ad<="20111209" and (identify identifier id) adj of adj a near2 requesting near2 (service site website resource application app)	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 11:11 PM
L408	1562	@ad<="20111209" and (identify identifier id) near3 requesting near2 (service site website resource application app)	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 11:11 PM
L409	114	@ad<="20111209" and (identify identifier id) near3 requesting near2	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 11:11 PM

		(service site website resource application app) and biometric					
L410	6	(US-20120110341-$ or US-20110231651-$ or US-20100242102-$).did. or (US-8549300-$ or US-7950051-$ or US-7512965-$).did.	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 11:11 PM
L411	1	L76 and cookie	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 11:11 PM
L412	2	(US-20120110341-$).did. or (US-8549300-$).did.	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 11:11 PM
L413	0	L78 and cooki	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 11:11 PM
L414	10	(US-20120110341-$ or US-20110231651-$ or US-20110205016-$ or US-20090100269-$ or US-20060247982-$ or US-20100242102-$ or US-20050198348-$).did. or (US-8549300-$ or US-7950051-$ or US-7512965-$).did.	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 11:11 PM
L415	0	L80 and cooki	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 11:11 PM
L416	6	("6016476" "8577813" "8856539" "9100826" "20040107170" "20040236632").pn.	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 11:11 PM
L417	591028	"6" and authentication	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 11:11 PM
L418	5	L82 and authentication	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 11:11 PM
L419	5	L84 and key	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 11:11 PM
L420	0	L85 and cookie	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 11:11 PM
L421	11	(US-20090100269-$ or US-20110231651-$ or US-20050198348-$ or US-20060247982-$ or US-20110205016-$ or US-20120110341-$ or US-20100242102-$ or US-20120167193-$).did. or (US-7512965-$ or US-7950051-$ or US-8549300-$).did.	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 11:11 PM
L422	40629	(G06F21/31,32,44).cpc.	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 11:11 PM

L423	16	L88 and authentication adj translator	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/07/12 11:11 PM
L424	92	L88 and (credential and (external adj resource) and login)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/07/12 11:11 PM
L425	34	L90 and backup	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/07/12 11:11 PM
L426	4	("7697729" "8145916" "8984596" "20110078771").pn.	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 11:11 PM
L427	1	L92 and backup	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 11:11 PM
L428	31	("20060085844" OR "20070266256" OR "20080059804" OR "20090191846" OR "20110138450" OR "7780080" OR "8776214" OR "10872152" OR "5010571" OR "5499298" OR "20040107170" OR "20040236632" OR "20050198348" OR "20090100269" OR "20100242102" OR "20110078771" OR "20110205016" OR "20110231651" OR "20120110341" OR "20120167193" OR "6016476" OR "6691232" OR "7512965" OR "7697729" OR "7950051" OR "8145916" OR "8549300" OR "8577813" OR "8856539" OR "8984596" OR "9100826").pn.	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 11:11 PM
L429	1	"20070257104".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 11:11 PM
L430	1	243 AND (backup (back ADJ up))	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB,	OR	ON	ON	2022/07/12 11:11 PM

			HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L431	17	((US-20090100269-A1 OR US-20110231651-A1 OR US-20050198348-A1 OR US-20060247982-A1 OR US-20110205016-A1 OR US-20120110341-A1 OR US-20100242102-A1 OR US-20120167193-A1 OR US-20080059804-A1 OR US-20090191846-A1 OR US-20060085844-A1 OR US-20070257104-A1).did. AND PGPB.dbnm.) OR ((US-7512965-B1 OR US-7950051-B1 OR US-8549300-B1 OR US-8776214-B1 OR US-7780080-B2).did. AND USPT.dbnm.)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/07/12 11:11 PM
L432	2	243 AND (pair$3)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/07/12 11:11 PM
L433	17	((US-20090100269-A1 OR US-20110231651-A1 OR US-20100242102-A1 OR US-20120110341-A1 OR US-20110205016-A1 OR US-20060247982-A1 OR	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DK, EA, EE, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV,	OR	ON	ON	2022/07/12 11:11 PM

APPL-1002
APPLE INC. / Page 49 of 419

		US-20050198348-A1 OR US-20120167193-A1 OR US-20080059804-A1 OR US-20090191846-A1 OR US-20060085844-A1 OR US-20070257104-A1).did. AND PGPB.dbnm.) OR ((US-8549300-B1 OR US-7950051-B1 OR US-7512965-B1 OR US-8776214-B1 OR US-7780080-B2).did. AND USPT.dbnm.)	MA, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L434	0	250 AND (copy$3 SAME (modif$3 modification, alter$3 edit$3) SAME (backup (back ADJ up)))	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DK, EA, EE, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/07/12 11:11 PM
L435	190	239 AND (copy$3 SAME (modif$3 modification, alter$3 edit$3) SAME (backup (back ADJ up)))	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DK, EA, EE, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/07/12 11:11 PM
L436	3	252 AND ((backup (back ADJ up)) SAME brand)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DK, EA, EE, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR,	OR	ON	ON	2022/07/12 11:11 PM

			TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L437	1	"20140250079".pn.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2022/07/12 11:11 PM
L438	102101	(G06F21/10,121,128,31,32,44, H04L63/0861,10,20).cpc.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2022/07/12 11:11 PM
L439	70588	(H04L63/08,0815,0823,083,0281,0869).cpc.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2022/07/12 11:11 PM
L440	773	(257 258) AND (copy$3 SAME (modif$3 modification, alter$3 edit$3) SAME (backup (back ADJ up)))	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DK, EA, EE, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/07/12 11:11 PM
L441	32	259 AND ((backup (back ADJ up)) SAME brand)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DK, EA, EE, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/07/12 11:11 PM
L442	1	"20170230179".pn.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2022/07/12 11:13 PM
L443	0	442 AND brand	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2022/07/12 11:13 PM

PE2E SEARCH - Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
N92	0	((first ADJ device ADJ being) near3 ("same brand") near4 (second ADJ device)).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2022/07/12 11:15 PM

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	17123018
Filing Date	2020-12-15
First Named Inventor	Bjorn Markus Jakobsson
Art Unit	2497
Examiner Name	Andrew J. Steinle
Attorney Docket Number	MJAKP026

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20170230179		2017-08-10	MANNAN MOHAMMAD	

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17123018
	Filing Date	2020-12-15
	First Named Inventor	Bjorn Markus Jakobsson
	Art Unit	2497
	Examiner Name	Andrew J. Steinle
	Attorney Docket Number	MJAKP026

	1		

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

EXAMINER SIGNATURE

Examiner Signature	/ANDREW J STEINLE/	Date Considered	07/12/2022

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

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

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

backup a modified version of the vault

All Videos Shopping News More Tools

About 3,780 results (0.40 seconds)

www.google.com/patents/US9495252

Continuous data backup using real time delta storage

Grant · Filed Mar 14, 2014 · Issued Nov 15, 2016 · Shunhui Zhu · Dell Software Inc.

The backup agent is running on a computing machine on which the particular version of the data file was previously stored. ... Then processing logic sends the ...

Overview · Related · Discuss

www.google.com/patents/US7165154

System and method for data backup

Grant · Filed Mar 18, 2003 · Issued Jan 16, 2007 · David Lawrence Coombs · Net Integration Technologies Inc.

Each full backup comprises a copy of the data selected from the first storage device in accordance with a first criteria and attribute data representative ...

Overview · Related · Discuss

www.google.com/patents/US4686620

Database backup method

Grant · Filed Jul 26, 1984 · Issued Aug 11, 1987 · Fred K. Ng · American Telephone And Telegraph Company, At&T Bell Laboratories

A method of generating a backup copy of a database system. Modifications made to the database since the generation of a prior backup copy are summarized in ...

Overview · Related · Discuss

www.google.com/patents/US7702867

System and method for data backup

Grant · Filed Nov 13, 2006 · Issued Apr 20, 2010 · David Lawrence Coombs · International Business Machines Corporation

Full and incremental backups of data stored to a first storage device ... If the data is regularly copied to another storage device, a recent copy can be ...

Overview · Related · Discuss

www.google.com/patents/US8099605

Intelligent storage device for backup system

Grant · Filed Jun 1, 2007 · Issued Jan 17, 2012 · Leif Olov Billsröm · InventSec AB

A data storage and data backup device that offers automatic reduction of ... By using this method, there is always a copy in the vault and there is always a ...

Overview · Related · Discuss

www.google.com/patents/US5276860

Digital data processor with improved backup storage

Grant · Filed Dec 19, 1989 · Issued Jan 4, 1994 · Richard W. Fortier · Epoch Systems, Inc.

1. The backup processor 12 scans the filesystem, e.g., the directories of system disks 18, for candidate files to copy to the baseline backup volume 20. 2. The ...

Overview · Related · Discuss

www.google.com/patents/US8751454

Virtual defragmentation in a deduplication vault

Grant · Filed Jan 28, 2014 · Issued Jun 10, 2014 · Nathan S. Bushman · Storagecraft Technology Corporation

Similarly, each of a base backup and multiple incremental backups of the source storage 110 that is stored in the vault storage 108 includes a copy of the FSM ...

Overview · Related · Discuss

www.google.com/patents/US7657582

Using recent activity information to select backup versions ...

Grant · Filed Aug 4, 2005 · Issued Feb 2, 2010 · Paul Cram · Symantec Operating Corporation

In one embodiment, restoration candidates may be selected from among those backup versions that correspond to storage objects that the requesting user modified.

Overview · Related · Discuss

www.google.com/patents/US5765173

High performance backup via selective file saving which can ...

Grant · Filed Jan 11, 1996 · Issued Jun 9, 1998 · David Cane · Connected Corporation

Often only a portion of a large file is modified between backup operations. ... When a recovery operation is requested, a complete version T2 target file ...

Overview · Related · Discuss

www.google.com/patents/US6088694

Continuous availability and efficient backup for externally ...

Grant · Filed Mar 31, 1998 · Issued Jul 11, 2000 · Randal Chilton Burns · International Business Machines Corporation

performing automatic backup of the modified file by providing a copy of the modified reference file to a backup server. 2. A method of appending data to a file ...

Overview · Related · Discuss

Washington DC (Hagerstown MD), Virginia - From your IP address - Update location

Help Send feedback Privacy Terms

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	17123018
	Filing Date	2020-12-15
	First Named Inventor	Bjorn Markus Jakobsson
	Art Unit	2497
	Examiner Name	Andrew J. Steinle
	Attorney Docket Number	MJAKP026

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20170230179		2017-08-10	MANNAN MOHAMMAD	

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17123018
	Filing Date	2020-12-15
	First Named Inventor	Bjorn Markus Jakobsson
	Art Unit	2497
	Examiner Name	Andrew J. Steinle
	Attorney Docket Number	MJAKP026

	1		

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17123018
	Filing Date	2020-12-15
	First Named Inventor	Bjorn Markus Jakobsson
	Art Unit	2497
	Examiner Name	Andrew J. Steinle
	Attorney Docket Number	MJAKP026

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/Yeu-Ting George Cheng/	Date (YYYY-MM-DD)	2022-07-01
Name/Print	Yeu-Ting George Cheng	Registration Number	69408

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

Electronic Acknowledgement Receipt

EFS ID:	46105680
Application Number:	17123018
International Application Number:	
Confirmation Number:	1102
Title of Invention:	AUTHENTICATION TRANSLATION
First Named Inventor/Applicant Name:	Bjorn Markus Jakobsson
Customer Number:	21912
Filer:	Yeu-Ting George Cheng/Elaine Nguyen
Filer Authorized By:	Yeu-Ting George Cheng
Attorney Docket Number:	MJAKP026
Receipt Date:	01-JUL-2022
Filing Date:	15-DEC-2020
Time Stamp:	17:46:20
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	MJAKP026_IDS_04.pdf	1052737 fca794c3333dff90ecab0bdce3a89536a95f2579	no	4

Warnings:

Information:	
Total Files Size (in bytes):	1052737

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.

Application Number	Application/Control No.	Applicant(s)/Patent under Reexamination	
* 17/123,018 *	17/123,018	Jakobsson, Bjorn Markus	
	Examiner	**Art Unit**	
	STEINLE, ANDREW J	2497	

Document Code - DISQ	**Internal Document - DO NOT MAIL**

TERMINAL DISCLAIMER	☑ APPROVED	☐ DISAPPROVED
Date Filed: 17 June 2022	**This patent is subject to a Terminal Disclaimer**	

Approved/Disapproved by:

/LAWANA R HIXON/

Technology Center: OPLC

Telephone: (571)272-6074

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/123,018	12/15/2020	Bjorn Markus Jakobsson	MJAKP026	1102

21912 7590 06/22/2022
VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

EXAMINER	
STEINLE, ANDREW J	

ART UNIT	PAPER NUMBER
2497	

NOTIFICATION DATE	DELIVERY MODE
06/22/2022	ELECTRONIC

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

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

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

usptocorrespondence@ip-patent.com

Applicant-Initiated Interview Summary	**Application No.** 17/123,018	**Applicant(s)** Jakobsson, Bjorn Markus		
	Examiner ANDREW J STEINLE	**Art Unit** 2497	**AIA (First Inventor to File) Status** No	**Page** 1 of 1

All Participants (applicant, applicants representative, PTO personnel)	**Title**	**Type**
ANDREW J STEINLE	Primary Examiner	Telephonic
George Cheng (Reg. No. 69,408)	Attorney of Record	

Date of Interview: 16 June 2022

Issues Discussed:

Proposed Amendment(s)

Examiner stated that both proposed amendments would distinguish over the current rejection. Regarding the first proposed amendment, as it incorporates the previously indicated allowable subject matter, it would likely be in condition for allowance. Regarding the second proposed amendment, it would overcome the current rejection however no agreement on allowability was made at this time as further search and consideration will be required upon receipt of the amendment.

☑ Attachment

/ANDREW J STEINLE/ Primary Examiner, Art Unit 2497	

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

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

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

From: George Cheng
To: Steinle, Andrew
Subject: MJAKP026 (App. No.: 17/123,018) Agenda and Proposed Claim Amendments for 6/16/2022 Interview
Date: Wednesday, June 15, 2022 8:06:28 PM
Attachments: MJAKP026 Interview Request Form - 2022.06.15.pdf
MJAKP026 Interview Request Form - Continuation Sheet - 2022.06.15.docx

CAUTION: This email has originated from a source outside of USPTO. **PLEASE CONSIDER THE SOURCE** before responding, clicking on links, or opening attachments.

Examiner Steinle,

Please find attached an agenda and proposed claim amendments for the 6/16/2022 interview for Application No. 17/123,018. Applicant authorizes communication of this attached interview agenda and these proposed claim amendments by this email. Please continue to send official correspondence via the email address associated with customer number 21912.

Regards,
George

George Cheng

Van Pelt, Yi & James LLP
Intellectual Property Law
10050 N. Foothill Blvd., Suite 200
Cupertino, CA 95014
V: 408-207-4765
F: 408-973-2595
gcheng@ip-patent.com

This email may contain confidential, attorney-client, attorney work product, and/or privileged and confidential information. If you received this message in error, please contact the sender at the above address/number and immediately destroy this and all copies of this message.

Applicant Initiated Interview Request Form

Application No.: 17/123,018 First Named Applicant: Bjorn Markus Jakobsson
Examiner: Andrew J. Steinle Art Unit: 2497 Status of Application: Pending

Tentative Participants:
(1) Examiner Andrew J. Steinle **(2)** Yeu-Ting George Cheng
(3) _____ **(4)** _____

Proposed Date of Interview: Thurs 6/16 **Proposed Time:** 4p ET **(AM/PM)**

Type of Interview Requested:
(1) [✓] Telephonic (2) [ ] Personal (3) [ ] Video Conference

Exhibit To Be Shown or Demonstrated: [ ] YES [✓] NO
If yes, provide brief description: _____

Issues To Be Discussed

Issues (Rej., Obj., etc)	Claims/ Fig. #s	Prior Art	Discussed	Agreed	Not Agreed
(1)	16		[ ]	[ ]	[ ]
(2)			[ ]	[ ]	[ ]
(3)			[ ]	[ ]	[ ]
(4)			[ ]	[ ]	[ ]

[ ] Continuation Sheet Attached [✓] Proposed Amendment or Arguments Attached
Brief Description of Arguments to be Presented: Applicants would like to discuss the attached proposed amendments.

An interview was conducted on the above-identified application on _____

NOTE: This form should be completed and filed by applicant in advance of the interview (see MPEP § 713.01). If this form is signed by a registered practitioner not of record, the Office will accept this as an indication that he or she is authorized to conduct an interview on behalf of the principal (37 CFR 1.32(a)(3)) pursuant to 37 CFR 1.34. This is not a power of attorney to any above named practitioner. See the Instruction Sheet for this form, which is incorporated by reference. By signing this form, applicant or practitioner is certifying that he or she has read the Instruction Sheet. After the interview is conducted, applicant is advised to file a statement of the substance of this interview (37 CFR 1.133(b)) as soon as possible. This application will not be delayed from issue because of applicant's failure to submit a written record of this interview.

/Yeu-Ting George Cheng/
Applicant/Applicant's Representative Signature

Examiner/SPE Signature

Yeu-Ting George Cheng
Typed/Printed Name of Applicant or Representative

69,408
Registration Number, if applicable

This collection of information is required by 37 CFR 1.133. 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 24 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.

MJAKP026 Applicant Initiated Interview Request Form

Continuation Sheet

Application No. 17/123,018

PROPOSED AMENDMENT:

1. (Proposed) A system, comprising:

one or more processors configured to:

receive, at a first device, a request to access a resource external to the first device, wherein the resource external to the first device is associated with a user;

access at least one record stored on the first device, the at least one record including authentication information associated with the user and credential information associated with the external resource to which the user has requested access, wherein the credential information comprises a cryptographic key;

receive authentication input from the user;

determine that the authentication input from the user matches the authentication information associated with the user included in the at least one record stored on the first device;

retrieve at least a portion of the credential information from the at least one record stored on the first device;

facilitate access of the user to the external resource at least in part by transmitting, on behalf of the user, from the first device, output based at least in part on the at least portion of the credential information retrieved from the at least one record, wherein the user of the first device is granted access to the external resource based at least in part on the output transmitted from the first device on behalf of the user; and

<u>based at least in part on the first device being a same brand as a second device,</u> initiate a backup, to [[a]] <u>the</u> second device, of at least a portion of the at least one record; and

a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.

2. (Proposed) A system, comprising:

one or more processors configured to:

receive, at a first device, a request to access a resource external to the first device, wherein the resource external to the first device is associated with a user;

access at least one record stored on the first device, the at least one record including authentication information associated with the user and credential information associated with the external resource to which the user has requested access, wherein the credential information comprises a cryptographic key;

receive authentication input from the user;

determine that the authentication input from the user matches the authentication information associated with the user included in the at least one record stored on the first device;

retrieve at least a portion of the credential information from the at least one record stored on the first device;

facilitate access of the user to the external resource at least in part by transmitting, on behalf of the user, from the first device, output based at least in part on the at least portion of the credential information retrieved from the at least one record, wherein the user of the first device is granted access to the external resource based at least in part on the output transmitted from the first device on behalf of the user; and

based at least in part on the first device and a second device being in a shared MAC address range, initiate a backup, to [[a]] the second device, of at least a portion of the at least one record; and

a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.

The foregoing amendments are not to be taken as an admission of unpatentability of any of the claims prior to the amendments.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.:	17/123,018	Examiner:	Andrew J. Steinle
Filed:	December 15, 2020	Art Unit:	2497
Confirmation No.:	1102	Docket No.:	MJAKP026
First Inventor:	Bjorn Markus Jakobsson		
Title:	AUTHENTICATION TRANSLATION		

TERMINAL DISCLAIMER UNDER 37 C.F.R. § 1.321
TO OBVIATE AN OBVIOUSNESS-TYPE
DOUBLE PATENTING REJECTION

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

Dear Sir:

Applicant(s), RightQuestion, LLC, the owner(s) of the entire interest in the above-identified application hereby disclaim(s), except as provided below, the terminal part of the statutory term of any patent granted on the above-identified application, which would extend beyond the expiration date of the full statutory term defined in 35 U.S.C. 154 and 173 of prior United States Patent No. 9,294,452, of prior United States Patent No. 10,360,351, of prior United States Patent No. 10,521,568, and of prior United States Patent No. 10,929,512 (hereafter "prior patents"), as presently shortened by any terminal disclaimer. The applicant(s)/owner(s) hereby agree(s) that any patent so granted on the above-identified application shall be enforceable only for and during such period that it and the prior patents are commonly owned. This agreement runs with any patent granted on the above-identified application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the applicant(s)/owner(s) do(es) not disclaim the terminal part of any patent granted on the above-identified application that would extend to the expiration date of the full statutory term as defined in 35 U.S.C. 154 and 173 of the prior patents, as presently shortened by any terminal disclaimer, in the event that it later: expires for failure to

pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 C.F.R. 1.321, has all claims canceled by a reexamination certificate, is reissued or is in any matter terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

The undersigned is an agent or attorney of record.

Please charge Deposit Account No. 50-0685 (MJAKP026) in the amount of $170.00 to cover the fee. If the required fees are missing or any additional fees are required during the pendency of the subject application, please charge such fees or credit any overpayment to Deposit Account No. 50-0685 (Order No. MJAKP026).

Respectfully submitted,

Dated: June 17, 2022

/Yeu-Ting George Cheng/
Yeu-Ting George Cheng
Registration No. 69408
408-207-4765

VAN PELT, YI & JAMES LLP
10050 N. Foothill Blvd., Suite 200
Cupertino, CA 95014
Fax 408-973-2595

Electronic Patent Application Fee Transmittal

Application Number:	17123018
Filing Date:	15-Dec-2020
Title of Invention:	AUTHENTICATION TRANSLATION
First Named Inventor/Applicant Name:	Bjorn Markus Jakobsson
Filer:	Yeu-Ting George Cheng/Elaine Nguyen
Attorney Docket Number:	MJAKP026

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
CLAIMS IN EXCESS OF 20	2202	13	50	650
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Extension - 2 months with $0 paid	2252	1	320	320
Miscellaneous:				
STATUTORY OR TERMINAL DISCLAIMER	2814	1	170	170
		Total in USD ($)		**1140**

Electronic Acknowledgement Receipt

EFS ID:	45987700
Application Number:	17123018
International Application Number:	
Confirmation Number:	1102
Title of Invention:	AUTHENTICATION TRANSLATION
First Named Inventor/Applicant Name:	Bjorn Markus Jakobsson
Customer Number:	21912
Filer:	Yeu-Ting George Cheng/Elaine Nguyen
Filer Authorized By:	Yeu-Ting George Cheng
Attorney Docket Number:	MJAKP026
Receipt Date:	17-JUN-2022
Filing Date:	15-DEC-2020
Time Stamp:	15:03:38
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$1140
RAM confirmation Number	E20226GF04060348
Deposit Account	500685
Authorized User	Elaine Nguyen
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.16 (National application filing, search, and examination fees) 37 CFR 1.17 (Patent application and reexamination processing fees)	

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Request for Reconsideration-After Non-Final Rejection	MJAKP026_AMD_B.pdf	126151 03e953750466f84c19d6fbe5de5643db660aecd8	no	10
Warnings:					
Information:					
2	Terminal Disclaimer Filed	MJAKP026_TD.pdf	78613 241134d3f6c606669772f969e3e26cc1470117ae	no	2
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	43049 d84f354509afdc5a1324f861103bbc186df4e236	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	247813		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.:	17/123,018	Examiner:	Andrew J. Steinle
Filed:	December 15, 2020	Art Unit:	2497
Confirmation No.:	1102	Docket No.:	MJAKP026
First Inventor:	Bjorn Markus Jakobsson		
Title:	AUTHENTICATION TRANSLATION		

AMENDMENT B

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

Dear Sir:

This is in response to the Office Action mailed January 28, 2022. The following amendment and remarks are respectfully submitted.

Applicant(s) believe that no (additional) fees are required beyond any fees submitted herewith. If required fees are missing or any additional fees are required during the pendency of the subject application, please charge such fees or credit any overpayment to Deposit Account No. 50-0685 (MJAKP026).

IN THE CLAIMS

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

Listing of Claims:

1. (Currently amended) A system, comprising:

one or more processors configured to:

receive, at a first device, a request to access a resource external to the first device, wherein the resource external to the first device is associated with a user;

access at least one record stored on the first device, the at least one record including authentication information associated with the user and credential information associated with the external resource to which the user has requested access, wherein the credential information comprises a cryptographic key;

receive authentication input from the user;

determine that the authentication input from the user matches the authentication information associated with the user included in the at least one record stored on the first device;

retrieve at least a portion of the credential information from the at least one record stored on the first device;

facilitate access of the user to the external resource at least in part by transmitting, on behalf of the user, from the first device, output based at least in part on the at least portion of the credential information retrieved from the at least one record, wherein the user of the first device is granted access to the external resource based at least in part on the output transmitted from the first device on behalf of the user; and

based at least in part on the first device being a same brand as a second device, initiate a backup, to [[a]] the second device, of at least a portion of the at least one record; and

a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.

2. (Original) The system of claim 1, wherein the second device is used to authenticate the user to one or more external resources.

3. (Original) The system of claim 1, wherein the backup is completed after the first device has performed a verification that the second device conforms to a policy associated with the at least one record stored on the first device.

4. (Original) The system of claim 1, wherein the backup is completed after a secure channel is established by at least one of the first device and the second device.

5. (Original) The system of claim 1, wherein the first device and the second device are configured to complete a pairing process.

6. (Original) The system of claim 5, wherein the pairing process comprises a comparison of data generated from one or more authentication inputs.

7. (Original) The system of claim 1, wherein subsequent to completion of the backup, the second device comprises a first profile associated with the user of the first device, and a second profile associated with a second user different from the user of the first device.

8. (Original) The system of claim 1, wherein the one or more processors are further configured to:

determine that the authentication input from the user does not match authentication information of a first profile; and

subsequent to determining that the authentication input from the user does not match the authentication information of the first profile, determine that the authentication input from the user matches authentication information of a second profile, wherein the first profile is associated with a different user than the second profile.

9. (Currently amended) The system of claim 1, wherein the at least one record stored on the first device is stored in a secure storage, and [[where]] <u>wherein</u> the one or more processors are configured to access the record stored on the secure storage using a restricted interface.

10. (Original) The system of claim 9, wherein the restricted interface comprises a dedicated physical connection.

11. (Original) The system of claim 9, wherein the restricted interface comprises an application programming interface.

12. (Original) The system of claim 1, wherein the backup causes a certificate to be transmitted to the second device.

13. (Original) The system of claim 12, wherein the certificate is generated at least in part by the first device.

14. (Original) The system of claim 1, wherein the authentication input from the user is received using a biometric user input element.

15. (Original) The system of claim 1, wherein the backup comprises copying a modified version of a vault to the second device.

16. (Cancelled)

17. (Currently amended) A method, comprising:

receiving, at a first device, a request to access a resource external to the first device, wherein the resource external to the first device is associated with a user;

accessing at least one record stored on the first device, the at least one record including authentication information associated with the user and credential information associated with the external resource to which the user has requested access, wherein the credential information comprises a cryptographic key;

receiving authentication input from the user;

determining that the authentication input from the user matches the authentication information associated with the user included in the at least one record stored on the first device;

retrieving at least a portion of the credential information from the at least one record stored on the first device;

facilitating access of the user to the external resource at least in part by transmitting, on behalf of the user, from the first device, output based at least in part on the at least portion of the credential information retrieved from the at least one record, wherein the user of the first device is granted access to the external resource based at least in part on the output transmitted from the first device on behalf of the user; and

based at least in part on the first device being a same brand as a second device, initiating a backup, to [[a]] the second device, of at least a portion of the at least one record.

18. (Currently amended) A computer program product embodied in a non-transitory computer readable storage medium and comprising computing instructions for:

receiving, at a first device, a request to access a resource external to the first device, wherein the resource external to the first device is associated with a user;

accessing at least one record stored on the first device, the at least one record including authentication information associated with the user and credential information associated with the external resource to which the user has requested access, wherein the credential information comprises a cryptographic key;

receiving authentication input from the user;

determining that the authentication input from the user matches the authentication information associated with the user included in the at least one record stored on the first device;

retrieving at least a portion of the credential information from the at least one record stored on the first device;

facilitating access of the user to the external resource at least in part by transmitting, on behalf of the user, from the first device, output based at least in part on the at least portion of the credential information retrieved from the at least one record, wherein the user of the first device is granted access to the external resource based at least in part on the output transmitted from the first device on behalf of the user; and

based at least in part on the first device being a same brand as a second device, initiating a backup, to [[a]] the second device, of at least a portion of the at least one record.

19. (Previously Presented) The system of claim 1, wherein the one or more processors are configured to access records associated with at least two different users.

20. (Previously Presented) The system of claim 19, wherein the records associated with the at least two different users are stored on the first device.

21. (Previously Presented) The method of claim 17, comprising accessing records associated with at least two different users.

22. (Previously Presented) The method of claim 21, wherein the records associated with the at least two different users are stored on the first device.

23. (New) The method of claim 17, wherein the second device is used to authenticate the user to one or more external resources.

24. (New) The method of claim 17, wherein the backup is completed after the first device has performed a verification that the second device conforms to a policy associated with the at least one record stored on the first device.

25. (New) The method of claim 17, wherein the backup is completed after a secure channel is established by at least one of the first device and the second device.

26. (New) The method of claim 17, wherein the first device and the second device are configured to complete a pairing process.

27. (New) The method of claim 26, wherein the pairing process comprises a comparison of data generated from one or more authentication inputs.

28. (New) The method of claim 17, wherein subsequent to completion of the backup, the second device comprises a first profile associated with the user of the first device, and a second profile associated with a second user different from the user of the first device.

29. (New) The method of claim 17, further comprising:

determining that the authentication input from the user does not match authentication information of a first profile; and

subsequent to determining that the authentication input from the user does not match the authentication information of the first profile, determining that the authentication input from the user matches authentication information of a second profile, wherein the first profile is associated with a different user than the second profile.

30. (New) The method of claim 17, wherein the at least one record stored on the first device is stored in a secure storage, and further comprising accessing the record stored on the secure storage using a restricted interface.

31. (New) The method of claim 30, wherein the restricted interface comprises a dedicated physical connection.

32. (New) The method of claim 30, wherein the restricted interface comprises an application programming interface.

33. (New) The method of claim 17, wherein the backup causes a certificate to be transmitted to the second device.

34. (New) The method of claim 33, wherein the certificate is generated at least in part by the first device.

35. (New) The method of claim 17, wherein the authentication input from the user is received using a biometric user input element.

36. (New) The method of claim 17, wherein the backup comprises copying a modified version of a vault to the second device.

INTERVIEW SUMMARY

A telephonic interview in the above-referenced case was conducted on June 16, 2022 between the Examiner and the Applicants' undersigned representative. The Office Action mailed on January 28, 2022 was discussed. Specifically, Claim 16 and the proposed amendments set forth herein were discussed with the intent to place the claims in better condition for allowance or appeal.

The Applicants thank the Examiner for the interview.

REMARKS

Claim 16 has been cancelled. Claims 1, 9, 17, and 18 have been amended to clarify the subject matter regarded as the invention. New Claims 23-36 have been added. Claims 1-15 and 17-36 are pending. No new matter has been added.

Subject Matter Indicated as Being Allowable

The Examiner has indicated that Claim 16 contains allowable subject matter. Claim 1 has been amended to include all of the limitations of Claim 16, as well as the base claims and any intervening claims. It is therefore believed that independent Claim 1 is allowable. Independent Claims 17 and 18 have been similarly amended, and are therefore also believed to be allowable for the same reasons described above.

Claims 2-15 and 19-22 depend, either directly or indirectly, from one of the aforementioned independent claims, and are therefore also believed to be allowable for the same reasons described above.

Double Patenting

Claims 1-22 have been rejected under the judicially created doctrine of obviousness-type double patenting. It is believed that the Terminal Disclaimer filed herewith is sufficient to overcome the double patenting rejection.

New Claims

New method dependent Claims 23-36 correspond to system dependent Claims 2-15, respectively. New method dependent Claims 23-36 depend, either directly or indirectly, from independent Claim 17, and are therefore also believed to be allowable for the same reasons described above.

The foregoing amendments are not to be taken as an admission of unpatentability of any of the claims prior to the amendments.

Reconsideration of the application and allowance of all claims are respectfully requested based on the preceding remarks. If at any time the Examiner believes that an interview would be helpful, please contact the undersigned.

Respectfully submitted,

Dated: June 17, 2022

/Yeu-Ting George Cheng/
Yeu-Ting George Cheng
Registration No. 69408
408-207-4765

VAN PELT, YI & JAMES LLP
10050 N. Foothill Blvd., Suite 200
Cupertino, CA 95014
Fax 408-973-2595

UNITED STATES PATENT AND TRADEMARK OFFICE

USPTO Automated Interview Request (AIR)

May 21 2022

This paper requesting to schedule and/or conduct an interview is appropriate because:

This submission is requested to be accepted as an authorization for this interview to communicate via the internet. Recognizing that Internet communications are not secure, I hereby authorize the USPTO to communicate with the undersigned concerning scheduling of the interview via video conference, instant messaging, or electronic mail, and to conduct the interview in accordance with office practice including video conferencing.

Name(s):
Yeu-Ting George Cheng

S-signature:
/YeuTing George Cheng/

Registration Number:
69408

U.S. Application Number:
17123018

Confirmation Number:
1102

E-mail Address:
gcheng@ip-patent.com

Phone Number:
+1 4082074765

Proposed Time of Interview:
5-27-2022 1:00 PM ET

Alternative Proposed Time(s) of Interview:
5-27-2022 1:30 PM ET

Prefered Interview Type:
Telephonic

I am the applicant or applicant's representative for this application.

Topic for Discussion:

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/123,018	12/15/2020	Bjorn Markus Jakobsson	MJAKP026	1102

21912 7590 01/28/2022
VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

EXAMINER	
STEINLE, ANDREW J	

ART UNIT	PAPER NUMBER
2497	

NOTIFICATION DATE	DELIVERY MODE
01/28/2022	ELECTRONIC

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

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

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

usptocorrespondence@ip-patent.com

Office Action Summary	Application No. 17/123,018	Applicant(s) Jakobsson, Bjorn Markus	
	Examiner ANDREW J STEINLE	Art Unit 2497	AIA (FITF) Status No

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

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

Status

1)☑ Responsive to communication(s) filed on 12/15/2020.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

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

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

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

Disposition of Claims*

5) ☑ Claim(s) 1-22 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) 1-22 is/are rejected.

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

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

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

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

11)☑ The drawing(s) filed on 12/15/2020 is/are: a)☑ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

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

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☑ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

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

4) ☐ Other: _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

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

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory double patenting rejection is appropriate where the claims at issue are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the reference application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of

activities undertaken within the scope of a joint research agreement. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The USPTO internet Web site contains terminal disclaimer forms which may be used. Please visit http://www.uspto.gov/forms/. The filing date of the application will determine what form should be used. A web-based eTerminal Disclaimer may be filled out completely online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to http://www.uspto.gov/patents/process/file/efs/guidance/eTD-info-I.jsp.

Claims 1-22 are provisionally rejected on the ground of nonstatutory double patenting as being unpatentable over **Claims 1-5, 8-11, 13, 16-17, 19, 21** of **U.S. Patent 9,294,452, Claims 2, 4-5, 8, 10-11, 13-15, 17, 19-22, and 24-41** of **U.S. Patent 10,360,351, Claims 2-26** of **U.S. Patent 10,521,568,** and **Claims 1-21** of **U.S. Patent 10,929,512.** Although the claims at issue are not identical, they are not patentably distinct from each other because aside from a few minor differences, these claims contain the same limitations and perform the same functions.

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

Claim Rejections - 35 USC § 103

The following is a quotation of pre-AIA 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, 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 negatived by the manner in which the invention was made.

In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

Claims 1-3, 7-9, 11-14, and 17-22 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Shah et al., (US 20080059804 A1) **hereinafter referred to as Shah** in view of Johansson (US 8776214 B1) **hereinafter referred to as Johansson.**

Regarding Claims 1, 17, and 18, Shah discloses ***A system, comprising: one or more processors configured to: receive, at a first device, a request to access a resource external to the first device, wherein the resource external to the first device is associated with a user;*** [paragraph 0014, After the initial setup, users can sign into their workstation, either as they did before, or through a new E-SSO software interface. When users request to connect to applications using their workstation, the E-SSO software automatically populates the user ID and password fields of the applications' login pages]

access at least one record stored on the first device, [paragraph 0014, To implement E-SSO, a copy of the E-SSO software must be installed on each WTRU. User ID and password for every system and application are stored in a local file]

the at least one record including authentication information associated with the user and credential information associated with the external resource to which the user has requested access, [paragraph 0014, After the initial setup, users can sign into their workstation, either as they did before, or through a new E-SSO software interface. When users request to connect to applications using their workstation, the E-SSO software automatically populates the user ID and password fields of the applications' login pages]

receive authentication input from the user; [paragraph 0016, Some E-SSO systems support the use of authentication technologies other than passwords to sign into the workstation and to access a user's credential profile, including smart cards, authentication tokens or biometric samples – user authenticates to the E-SSO system]

determine that the authentication input from the user matches the authentication information associated with the user included in the at least one record stored on the first device; [Claim 1, for comparing said received user authentication data to the stored user authentication data, and forwarding said stored user specific login information if said comparison is positive]

retrieve at least a portion of the credential information from the at least one record stored on the first device; [paragraph 0014, After the initial setup, users can sign into their workstation, either as they did before, or through a new E-SSO software interface. When users request to connect to applications using their workstation, the E-SSO software automatically populates the user ID and password fields of the applications' login pages]

facilitate access of the user to the external resource at least in part by transmitting, on behalf of the user, from the first device, output based at least in part on the at least portion of the credential information retrieved from the at least one record, wherein the user of the first device is granted access to the external resource based at least in part on the output transmitted from the first device on behalf of the user; [paragraph 0014, When users request to connect to applications using their workstation, the E-SSO software automatically populates the user ID and password fields of the applications' login pages]

Shah does not explicitly teach ***wherein the credential information comprises a cryptographic key; and initiate a backup, to a second device, of at least a portion of the at least one record; and a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.***

Johansson teaches ***wherein the credential information comprises a cryptographic key;*** [Column 5, lines 17-23, For example, the user may provide to the authentication manager 124 existing security credentials such as, for example, usernames, passwords, security keys, certificates, and/or other security credentials along with identifying information for the network sites 140 and/or uniform resource locators (URLs) associated with the security credentials – the credential information includes “security keys”]

Before the effective filing date of the claimed invention, it would have been obvious to one with ordinary skill in the art to combine the teachings of Johansson with the disclosure of Shah. The motivation or suggestion would have been to include multiple credential options. (Column 5, lines 12-27)

and initiate a backup, to a second device, of at least a portion of the at least one record; and a memory coupled to the one or more processors and configured to provide the one or more processors with instructions. [Column 5, lines 30-34, the authentication manager 124 may back up the account information to account data 160 located on the remote data server 106, account data 163 located on in the portable data store 118, and/or another location]

Before the effective filing date of the claimed invention, it would have been obvious to one with ordinary skill in the art to combine the teachings of Johansson with the disclosure of Shah. The motivation or suggestion would have been to include multiple credential options. (Column 5, lines 12-27)

Regarding Claim 2, Shah does not explicitly teach ***wherein the second device is used to authenticate the user to one or more external resources.***

Johansson teaches ***wherein the second device is used to authenticate the user to one or more external resources.*** [Column 4, lines 59-63, The portable data store 118 may be configured to store account data 163. The account data 163 may include, for example, security credentials used to access various network sites 140 or network pages 145, information regarding authentication endpoints 139, and/or other information]

Before the effective filing date of the claimed invention, it would have been obvious to one with ordinary skill in the art to combine the teachings of Johansson with the disclosure of Shah. The motivation or suggestion would have been to provide redundancy and to mitigate loss of data.

Regarding Claim 3, Shah does not explicitly teach ***wherein the backup is completed after the first device has performed a verification that the second device conforms to a policy associated with the at least one record stored on the first device.***

Johansson teaches ***wherein the backup is completed after the first device has performed a verification that the second device conforms to a policy associated with the at least one record stored on the first device.*** [Column 5, lines 30-36, the authentication manager 124 may back up the account information to account data 160 located on the remote data server 106, account data 163 located on in the portable data store 118, and/or another location. In some embodiments, the authentication manager 124 may not store the account information on the client 103 at all and may only use other locations – the policy is that the backup cannot be stored on the client]

Before the effective filing date of the claimed invention, it would have been obvious to one with ordinary skill in the art to combine the teachings of Johansson with the disclosure of Shah. The motivation or suggestion would have been to provide redundancy and to mitigate loss of data.

Regarding Claim 7, Shah does not explicitly teach ***wherein subsequent to completion of the backup, the second device comprises a first profile associated with the user of the first device, and a second profile associated with a second user different from the user of the first device.***

Johansson teaches ***wherein subsequent to completion of the backup, the second device comprises a first profile associated with the user of the first***

device, and a second profile associated with a second user different from the user of the first device. [Column 5, lines 43-56, Security credentials may be shared among multiple users of the authentication manager 124. As a non-limiting example, several users in an organization may share an online banking account. A first user may create a username and password for the account using the authentication manager 124. The first user may mark the account as shared and provide a list of users that are authorized to access the account, including a second user. When the account is distributed to account data 130, 160, it is secured such that only the authorized users can access it. When the second user next uses the authentication manager 124, the second user may be given the opportunity to synchronize the new account with account data 163 located in the portable data store 118 belonging to the second user or in some other location] [Column 5, lines 30-34, the authentication manager 124 may back up the account information to account data 160 located on the remote data server 106, account data 163 located on in the portable data store 118, and/or another location]

Before the effective filing date of the claimed invention, it would have been obvious to one with ordinary skill in the art to combine the teachings of Johansson with the disclosure of Shah. The motivation or suggestion would have been to include multiple credential options. (Column 5, lines 12-27)

Regarding Claim 8, Shah does not explicitly teach ***wherein the one or more processors are further configured to: determine that the authentication input from the user does not match authentication information of a first profile; and subsequent to determining that the authentication input from the user does not match the authentication information of the first profile, determine that the***

authentication input from the user matches authentication information of a second profile, wherein the first profile is associated with a different user than the second profile.

Johansson teaches ***wherein the one or more processors are further configured to: determine that the authentication input from the user does not match authentication information of a first profile; and subsequent to determining that the authentication input from the user does not match the authentication information of the first profile, determine that the authentication input from the user matches authentication information of a second profile, wherein the first profile is associated with a different user than the second profile.*** [Column 10, lines 8-15, the authentication manager 124 may give an indication of success or failure and may provide another authentication button 218 in order to log out of the network site 140. If multiple user accounts are present for the network site 140, the authentication manager 124 may provide a drop-down box or other user interface element allowing the user to select one of the accounts for authentication]

Before the effective filing date of the claimed invention, it would have been obvious to one with ordinary skill in the art to combine the teachings of Johansson with the disclosure of Shah. The motivation or suggestion would have been to include multiple credential options. (Column 5, lines 12-27)

Regarding Claim 9, Shah discloses ***wherein the at least one record stored on the first device is stored in a secure storage, and where the one or more processors are configured to access the record stored on the secure storage using a restricted interface.*** [paragraph 0064, The TPM/TSS 815 interacts with both

the SASO proxy unit 810 and the WAA 820 to provide a secure, trusted mechanism to generate, store, and retrieve passwords and SSO credentials]

Regarding Claim 11, Shah discloses ***wherein the restricted interface comprises an application programming interface.*** [paragraph 0064, The TPM/TSS 815 interacts with both the SASO proxy unit 810 and the WAA 820 to provide a secure, trusted mechanism to generate, store, and retrieve passwords and SSO credentials]

Regarding Claim 12, Shah does not explicitly teach ***wherein the backup causes a certificate to be transmitted to the second device.***

Johansson teaches ***wherein the backup causes a certificate to be transmitted to the second device.*** [Column 5, lines 30-34, the authentication manager 124 may back up the account information to account data 160 located on the remote data server 106, account data 163 located on in the portable data store 118, and/or another location]

Before the effective filing date of the claimed invention, it would have been obvious to one with ordinary skill in the art to combine the teachings of Johansson with the disclosure of Shah. The motivation or suggestion would have been to include multiple credential options. (Column 5, lines 12-27)

Regarding Claim 13, Shah discloses ***wherein the certificate is generated at least in part by the first device.*** [paragraph 0072, The USIM could also be configured to generate and store of high-entropy site-specific passwords and also to store SSO password and SSO credentials]

Regarding Claim 14, Shah discloses ***wherein the authentication input from the user is received using a biometric user input element.*** [paragraph 0016, Some

E-SSO systems support the use of authentication technologies other than passwords to sign into the workstation and to access a user's credential profile, including smart cards, authentication tokens or biometric samples]

Regarding Claims 19 and 21, Shah does not explicitly teach ***wherein the one or more processors are configured to access records associated with at least two different users.***

Johansson teaches ***wherein the one or more processors are configured to access records associated with at least two different users.*** [Column 10, lines 8-15, the authentication manager 124 may give an indication of success or failure and may provide another authentication button 218 in order to log out of the network site 140. If multiple user accounts are present for the network site 140, the authentication manager 124 may provide a drop-down box or other user interface element allowing the user to select one of the accounts for authentication]

Before the effective filing date of the claimed invention, it would have been obvious to one with ordinary skill in the art to combine the teachings of Johansson with the disclosure of Shah. The motivation or suggestion would have been to include multiple credential options. (Column 5, lines 12-27)

Regarding Claims 20 and 22, Shah does not explicitly teach ***wherein the records associated with the at least two different users are stored on the first device.***

Johansson teaches ***wherein the records associated with the at least two different users are stored on the first device.*** [Column 5, lines 43-48, Security credentials may be shared among multiple users of the authentication manager 124. As

a non-limiting example, several users in an organization may share an online banking account. A first user may create a username and password for the account using the authentication manager 124] [Column 5, lines 34-36, In some embodiments, the authentication manager 124 may not store the account information on the client 103 at all and may only use other locations – indicates that only in "some embodiments", the authentication manager cannot store account information on the client or the device which means that in other embodiments, it is able to do this]

Before the effective filing date of the claimed invention, it would have been obvious to one with ordinary skill in the art to combine the teachings of Johansson with the disclosure of Shah. The motivation or suggestion would have been to include multiple credential options. (Column 5, lines 12-27)

Claims 4-6 and 10 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Shah in view of Johansson, as applied to **Claims 1, 17, and 18,** respectively, above, and further in view of Owen et al., (US 20070257104 A1) **hereinafter referred to as Owen.**

Regarding Claim 4, the combination of Shah and Johansson does not explicitly teach ***wherein the backup is completed after a secure channel is established by at least one of the first device and the second device.***

Owen teaches ***wherein the backup is completed after a secure channel is established by at least one of the first device and the second device.*** [paragraph 0162, Then, at block 1430, the secure internet portal 70 initiates a private connection 65 with the remote computer 55 by, for example, forming an encrypted VPN connection

between the two computers. In certain embodiments, the encryption level of the connection can be scaled according to the bandwidth of the transmission channel between the two computers]

Before the effective filing date of the claimed invention, it would have been obvious to one with ordinary skill in the art to combine the teachings of Owen with the disclosures of Shah and Johansson. The motivation or suggestion would have been to ensure a secure connection between devices in order to mitigate against nefarious actions]

Regarding Claim 5, the combination of Shah and Johansson does not explicitly teach ***wherein the first device and the second device are configured to complete a pairing process.***

Owen teaches ***wherein the first device and the second device are configured to complete a pairing process.*** [paragraph 0162, Then, at block 1430, the secure internet portal 70 initiates a private connection 65 with the remote computer 55 by, for example, forming an encrypted VPN connection between the two computers. In certain embodiments, the encryption level of the connection can be scaled according to the bandwidth of the transmission channel between the two computers]

Before the effective filing date of the claimed invention, it would have been obvious to one with ordinary skill in the art to combine the teachings of Owen with the disclosures of Shah and Johansson. The motivation or suggestion would have been to ensure a secure connection between devices in order to mitigate against nefarious actions]

Regarding Claim 6, the combination of Shah and Johansson does not explicitly teach ***wherein the pairing process comprises a comparison of data generated from one or more authentication inputs.***

Owen teaches ***wherein the pairing process comprises a comparison of data generated from one or more authentication inputs.*** [paragraph 0162, Then, at block 1430, the secure internet portal 70 initiates a private connection 65 with the remote computer 55 by, for example, forming an encrypted VPN connection between the two computers. In certain embodiments, the encryption level of the connection can be scaled according to the bandwidth of the transmission channel between the two computers]

Before the effective filing date of the claimed invention, it would have been obvious to one with ordinary skill in the art to combine the teachings of Owen with the disclosures of Shah and Johansson. The motivation or suggestion would have been to ensure a secure connection between devices in order to mitigate against nefarious actions]

Regarding Claim 10, the combination of Shah and Johansson does not explicitly teach ***wherein the restricted interface comprises a dedicated physical connection.***

Owen teaches ***wherein the restricted interface comprises a dedicated physical connection.*** [paragraph 0054, the biometrically-secured device is a portable device similar in appearance to a flash drive (e.g., a "jump drive" or a "thumb drive")]

Before the effective filing date of the claimed invention, it would have been obvious to one with ordinary skill in the art to combine the teachings of Owen with the disclosures of Shah and Johansson. The motivation or suggestion would have been to

ensure a secure connection between devices in order to mitigate against nefarious actions]

Claim 15 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Shah in view of Johansson, as applied to **Claim 1,** above, and further in view of Gardner et al., (US 20140250079 A1) **hereinafter referred to as Gardner.**

Regarding Claim 15, the combination of Shah and Johansson does not explicitly teach ***wherein the backup comprises copying a modified version of a vault to the second device.***

Gardner teaches ***wherein the backup comprises copying a modified version of a vault to the second device.*** [paragraph 0004, Using this approach, individual files are backed up if they have been modified since the previous backup]

Before the effective filing date of the claimed invention, it would have been obvious to one with ordinary skill in the art to combine the teachings of Gardner with the disclosures of Shah and Johansson. The motivation or suggestion would have been to ensure the latest files are backed up. (paragraph 0004)

Allowable Subject Matter

Claim 16 is but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims and if the Double Patenting rejection was obviated.

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

Regarding Claim 16, none of the closest prior art of record explicitly teaches nor suggests in detail ***wherein the backup is performed in response to a determination that the first device is of a same brand as the second device*** in view of other limitations of the intervening claims.

Thus the prior arts of record taking singly or in combination do not teach or suggest the above-stated limitations taking wholly in combination with all the elements of each independent claim.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ANDREW J STEINLE whose telephone number is (571)272-9923. The examiner can normally be reached M-F 10am-6pm CT.

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

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Eleni Shiferaw can be reached on (571) 272-3867. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: https://patentcenter.uspto.gov. Visit https://www.uspto.gov/patents/apply/patent-

center for more information about Patent Center and

https://www.uspto.gov/patents/docx for information about filing in DOCX format. For

additional questions, contact the Electronic Business Center (EBC) at 866-217-9197

(toll-free). If you would like assistance from a USPTO Customer Service

Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ANDREW J STEINLE/
Primary Examiner, Art Unit 2497

Notice of References Cited	Application/Control No. 17/123,018	Applicant(s)/Patent Under Reexamination Jakobsson, Bjorn Markus	
	Examiner ANDREW J STEINLE	Art Unit 2497	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20080059804-A1	03-2008	Shah; Yogendra C.	G06F21/41	713/186
*	B	US-8776214-B1	07-2014	Johansson; Jesper M.	H04L63/1433	726/18
*	C	US-20070257104-A1	11-2007	Owen; Kelly	G06Q20/4014	235/380
*	D	US-20140250079-A1	09-2014	Gardner; Andrew Lynn	G06F11/1453	707/646
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

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

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/123,018	Jakobsson, Bjorn Markus
	Examiner	**Art Unit**
	ANDREW J STEINLE	2497

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

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

CLAIM		DATE								
Final	Original	01/25/2022								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								
	22	✓								

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/123,018	Jakobsson, Bjorn Markus
	Examiner	Art Unit
	ANDREW J STEINLE	2497

CPC - Searched*		
Symbol	**Date**	**Examiner**
CPC Classification Search G06F21/10, 121, 128, 31, 32, 44, H04L63 /0861, 10, 20, 0815, 0823, 083, 0869 limited by text	01/24/2022	AS

CPC Combination Sets - Searched*		
Symbol	**Date**	**Examiner**

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	**Date**	**Examiner**
PE2E Search class limited w/text search (see search history)	01/24/2022	AS
PE2E Search inventor and assignee search (see search history)	01/24/2022	AS
PE2E Search text search (see search history)	01/24/2022	AS
NPL Search via Google patents	01/24/2022	AS

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

/ANDREW J STEINLE/ Primary Examiner, Art Unit 2497	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	17123018
Filing Date	2020-12-15
First Named Inventor	Bjorn Markus Jakobsson
Art Unit	2497
Examiner Name	Andrew Steinle
Attorney Docket Number	MJAKP026

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	7780080		2010-08-24	OWEN KELLY	
	2	8776214		2014-07-08	JOHANSSON JESPER M	

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20060085844		2006-04-20	BUER MARK	
	2	20070266256		2007-11-15	SHAH YOGENDRA C	
	3	20080059804		2008-03-06	SHAH YOGENDRA C	
	4	20090191846		2009-07-30	SHI GUANGMING	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17123018
	Filing Date	2020-12-15
	First Named Inventor	Bjorn Markus Jakobsson
	Art Unit	~~xxxxx~~ 2497
	Examiner Name	~~xxxxxxxxxx~~ Andrew Steinle
	Attorney Docket Number	MJAKP026

	5	20110138450		2011-06-09	KESANUPALLI RAMESH			

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	IPR2022-00244 Claim Mapping Table for the '696 Patent. November 30, 2021	
	2	IPR2022-00244 Petition for Inter Partes Review of U.S. Patent No. 10,824,696. November 30, 2021	
	3	IPR2022-00251 Claim Mapping Table for the '512 Patent. December 1, 2021	
	4	IPR2022-00251 Petition for Inter Partes Review of U.S. Patent No. 10,929,512. December 1, 2021	

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

EXAMINER SIGNATURE

Examiner Signature	/ANDREW J STEINLE/	Date Considered	01/22/2022

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

EFS Web 2.1.18

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

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L1	281	((("Jakobsson") near3 ("Bjorn") near3 ("Markus"))).INV.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2022/01/22 08:42 PM
L2	431	((("Jakobsson") near3 ("Bjorn") near3 ("Markus"))).INV.	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/01/22 08:42 PM
L3	13	(RightQuestion).as.	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/01/22 08:43 PM
L94	46	(("(H01836") or ("20110066858") or ("20110066858") or ("6055637") or ("20030084171") or ("20030140230") or ("20060157559") or ("5832211") or ("5862323") or ("5659165") or ("5825003") or ("6446218") or ("20020099671") or ("20040002878") or ("20070044144") or ("7450584") or ("20050058132") or	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 09:36 PM

		("6006018") or ("20090113522") or ("4924515") or ("8599267") or ("20090096871") or ("6668327") or ("6067623") or ("7089584") or ("7210167") or ("20030065940") or ("20060075224") or ("20050108546") or ("20100228967") or ("8094634") or ("20090122770") or ("7085840") or ("7275260") or ("7496751") or ("7903611") or ("7903611") or ("20030084170") or ("20030084172") or ("20030084288") or ("20030084302") or ("20080117879") or ("5594789") or ("5850450") or ("6061799") or ("6061799") or ("6078805") or ("6108789") or ("6134327") or ("6141752") or (").pn.")).PN.					
L95	10427	(bjorn jakobsson).in.	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 09:36 PM
L96	741	(bjorn jakobsson).in. and authentication	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 09:36 PM
L97	108	(bjorn jakobsson).in. and authentication and translation	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 09:36 PM
L98	21	authentication adj translator	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 09:36 PM
L99	198	(proxy intermediate intermediary behalf adj2 of) near4 (cookie certificate ticket credential) with (transaction bank merchant) and biometric	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 09:36 PM
L100	201	(proxy intermediate intermediary behalf adj2 of) near4 (cookie certificate ticket credential) with	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 09:36 PM

		(transaction bank merchant vendor) and biometric					
L101	3	(proxy intermediate intermediary behalf adj2 of) near4 (cookie certificate ticket credential) with (transaction bank merchant vendor) and biometric and (726/5-7,10,18-19,28 713/170,172,185-186 382/115).ccls.	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 09:36 PM
L102	386	(forward$3) near4 (cookie certificate ticket credential) with (transaction bank merchant vendor) and biometric	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 09:36 PM
L103	400	biometric with authenticat$ with (proxy$4 intermediate intermediary)	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 09:36 PM
L104	162	(biometric fingerprint retinal) with (authenticat$ authoriz$ valid$ verif$ confirm$4 near3 identity) near2 (proxy$4 intermediate intermediary)	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 09:36 PM
L105	15	L14 AND ((713/186).CCLS.)	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 09:36 PM
L106	39	(biometric or fingerprint or retinal) with (authenticat$ authoriz$ valid$ verif$ confirm$4 near3 identity) near2 (proxy$4 intermediate intermediary)	(FPRS; EPO; JPO; DERWENT)	OR	ON	ON	2022/01/23 09:36 PM
L107	1	"20090100269".pn. and (proxy intermediate intermediary behalf adj2 cookie certificate ticket credential transaction bank merchant biometric)	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 09:36 PM
L108	1	"20090100269".pn. and (proxy intermediate intermediary behalf adj2 cookie certificate ticket credential transaction bank merchant biometric authentication)	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 09:36 PM

L109	1	"20080120707".pn. and (proxy intermediate intermediary behalf adj2 cookie certificate ticket credential transaction bank merchant biometric authentication)	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 09:36 PM
L110	386	(forward$3) near4 (cookie certificate ticket credential) with (transaction bank merchant vendor) and biometric	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 09:36 PM
L111	400	biometric with authenticat$ with (proxy$4 intermediate intermediary)	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 09:36 PM
L112	3	L21 and renegotiat$3	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 09:36 PM
L113	1	"20110205016".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 09:36 PM
L114	2	("20120110341" "20100242102").pn.	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 09:36 PM
L115	1	"20110231652".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 09:36 PM
L116	10	(US-20090100269-$ or US-20110231651-$ or US-20050198348-$ or US-20060247982-$ or US-20110205016-$ or US-20120110341-$ or US-20100242102-$).did. or (US-7512965-$ or US-7950051-$ or US-8549300-$).did.	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 09:36 PM
L117	3	L26 and cookie	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 09:36 PM
L118	10	(US-20090100269-$ or US-20110231651-$ or US-20050198348-$ or US-20060247982-$ or US-20110205016-$ or US-20120110341-$ or US-20100242102-$).did. or (US-7512965-$ or US-7950051-$ or US-8549300-$).did.	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 09:36 PM
L119	10	(US-20090100269-$ or US-20110231651-$ or US-20050198348-$ or US-20060247982-$ or US-20110205016-$ or US-20120110341-$ or US-20100242102-	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 09:36 PM

		$).did. or (US-7512965-$ or US-7950051-$ or US-8549300-$).did.					
L120	16	("20040107170"|"20040236632"|"20050198348"|"20090100269"|"20100242102"|"20110205016"|"20110231651"|"20120110341"|"20120167193"|"6016476"|"7512965"|"7950051"|"8549300"|"8577813"|"8856539"|"9100826").PN.	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 09:36 PM
L121	7	L30 and credential	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 09:36 PM
L122	5	L31 and login	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 09:36 PM
L123	0	L32 and backup	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 09:36 PM
L184	10	(US-20090100269-$ or US-20110231651-$ or US-20050198348-$ or US-20060247982-$ or US-20110205016-$ or US-20120110341-$ or US-20100242102-$).did. or (US-7512965-$ or US-7950051-$ or US-8549300-$).did.	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 10:15 PM
L185	1	L34 and (password same change)	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 10:15 PM
L186	9055072	@ad<="20111209"	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 10:15 PM
L187	8	L36 and ((password near3 change) same (without near3 (user adj (input knowledge notification))))	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 10:15 PM
L188	1	"20090132807".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 10:15 PM
L189	42	@ad<="20111209" and renegotiation same proxy	(US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/01/23 10:15 PM
L190	3	@ad<="20111209" and (non-security adj transparent adj proxy)	(US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/01/23 10:15 PM
L191	3	"20130205360"	(US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/01/23 10:15 PM
L192	3	"20090132807"	(US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/01/23 10:15 PM
L193	2	"20110231651".pn.	(US-PGPUB; USPAT;	OR	ON	ON	2022/01/23

			EPO; JPO; DERWENT; IBM_TDB)				10:15 PM
L194	17	ssl adj renegotiation	(US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/01/23 10:15 PM
L195	12740	@ad<="20111209" and restricted adj access	(US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/01/23 10:15 PM
L196	4396	@ad<="20111209" and authenticat$ and (restricted adj access)	(US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/01/23 10:15 PM
L197	1191	@ad<="20111209" and authenticat$ and biometric and (restricted adj access)	(US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/01/23 10:15 PM
L198	341	@ad<="20111209" and authenticat$ and biometric and (restricted adj access) and proxy	(US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/01/23 10:15 PM
L199	2	("6178505" | "6453419").PN.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2022/01/23 10:15 PM
L200	78	@ad<="20111209" and (authenticat$ adj server) and (restricted adj access) and (access adj control adj policy)	(US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/01/23 10:15 PM
L201	82	@ad<="20111209" and (authenticat$ adj server) and (restricted adj access or partial adj access) and (access adj control adj policy)	(US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/01/23 10:15 PM
L202	32	@ad<="20111209" and (authenticat$3 adj server) and remot$3 and password adj (updat$3 chang$3) and biometric and legacy	(US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/01/23 10:15 PM
L203	32	@ad<="20111209" and (authenticat$3 adj server) and password adj (updat$3 chang$3) and biometric and legacy	(US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/01/23 10:15 PM
L204	5	@ad<="20111209" and updat$3 near3 (password) with (automatic automatically) with expir$3	(US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/01/23 10:15 PM
L205	15	("2007/0124807").URPN.	(USPAT)	OR	ON	ON	2022/01/23 10:15 PM
L206	1210	@ad<="20111209" and (use adj condition)	(US-PGPUB; USPAT; EPO; JPO;	OR	ON	ON	2022/01/23 10:15 PM

		near3 information	DERWENT; IBM_TDB)				
L207	121	biometric with (authenticat$ authoriz$ valid$ verif$ confirm$4 near3 identity) near2 (proxy$4 intermediate intermediary)	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 10:15 PM
L208	20748	@ad<="20111209" and 713/186,168,155,152.ccls.	(US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/01/23 10:15 PM
L209	18	(biometric or fingerprint or retinal) with (authenticat$ authoriz$ valid$ verif$ confirm$4 near3 identity) near2 (proxy$4 intermediate intermediary) and @ad<="20111209" and 713/186,168,155,152.ccls.	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 10:15 PM
L210	1	"8549300".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 10:15 PM
L211	8	(biometric or fingerprint or retinal) with (authenticat$ authoriz$ valid$ verif$ confirm$4 near3 identity) near2 (proxy$4 intermediate intermediary) and @ad<="20111209" and 726/1,5,4,21,26.ccls.	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 10:15 PM
L212	7	(biometric or fingerprint or retinal) with (authenticat$ authoriz$ valid$ verif$ confirm$4 near3 identity) near2 (proxy$4 intermediate intermediary) and @ad<="20111209" and 705/38,3,8,141,67.ccls.	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 10:15 PM
L213	1	"20080071545".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/23 10:16 PM
L214	162	(biometric or fingerprint or retinal) with (authenticat$ authoriz$ valid$ verif$ confirm$4 near3 identity) near2 (proxy$4 intermediate intermediary)	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/24 12:17 AM
L215	39	("2011/0289314").URPN.	(USPAT)	OR	ON	ON	2022/01/24 12:17 AM
L216	14958	@ad<="20111209" and authenticat$ and cookie	(US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/01/24 12:17 AM

L217	77	(proxy intermediate intermediary behalf adj2 of) near4 cookie and biometric	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/24 12:17 AM
L218	36968	@ad<="20111209" and biometric and (authenticat$ authoriz$ valid$ verif$ confirm$4) and (transmit transmission)	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/24 12:17 AM
L219	36968	@ad<="20111209" and biometric and (authenticat$ authoriz$ valid$ verif$ confirm$4) and (transmit transmission)	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/24 12:17 AM
L220	5135	@ad<="20111209" and biometric same (authenticat$ authoriz$ valid$ verif$ confirm$4) same (transmit transmission)	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/24 12:17 AM
L221	1395	@ad<="20111209" and biometric with (authenticat$ authoriz$ valid$ verif$ confirm$4) with (transmit transmission)	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/24 12:17 AM
L222	358	@ad<="20111209" and biometric with (authenticat$ authoriz$ valid$ verif$ confirm$4) with (transmit transmission) and (proxy intermediate intermediary behalf adj2 of)	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/24 12:17 AM
L223	1	"7107220".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/24 12:17 AM
L224	0	@ad<="20111209" and (identify identifier id) adj of adj a near2 requesting near2 (service site website resource application app)	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/24 12:17 AM
L225	1562	@ad<="20111209" and (identify identifier id) near3 requesting near2 (service site website resource application app)	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/24 12:17 AM
L226	114	@ad<="20111209" and (identify identifier id) near3 requesting near2	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/24 12:17 AM

		(service site website resource application app) and biometric					
L227	6	(US-20120110341-$ or US-20110231651-$ or US-20100242102-$).did. or (US-8549300-$ or US-7950051-$ or US-7512965-$).did.	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/24 12:17 AM
L228	1	L76 and cookie	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/24 12:17 AM
L229	2	(US-20120110341-$).did. or (US-8549300-$).did.	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/24 12:17 AM
L230	0	L78 and cooki	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/24 12:17 AM
L231	10	(US-20120110341-$ or US-20110231651-$ or US-20110205016-$ or US-20090100269-$ or US-20060247982-$ or US-20100242102-$ or US-20050198348-$).did. or (US-8549300-$ or US-7950051-$ or US-7512965-$).did.	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/24 12:17 AM
L232	0	L80 and cooki	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/24 12:17 AM
L233	6	("6016476" "8577813" "8856539" "9100826" "20040107170" "20040236632").pn.	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/24 12:17 AM
L234	564950	"6" and authentication	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/24 12:17 AM
L235	5	L82 and authentication	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/24 12:17 AM
L236	5	L84 and key	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/24 12:17 AM
L237	0	L85 and cookie	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/24 12:17 AM
L238	11	(US-20090100269-$ or US-20110231651-$ or US-20050198348-$ or US-20060247982-$ or US-20110205016-$ or US-20120110341-$ or US-20100242102-$ or US-20120167193-$).did. or (US-7512965-$ or US-7950051-$ or US-8549300-$).did.	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/24 12:17 AM
L239	38419	(G06F21/31,32,44).cpc.	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/24 12:17 AM

L240	15	L88 and authentication adj translator	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/01/24 12:17 AM
L241	79	L88 and (credential and (external adj resource) and login)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/01/24 12:17 AM
L242	31	L90 and backup	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/01/24 12:18 AM
L243	4	("7697729" "8145916" "8984596" "20110078771").pn.	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/24 12:18 AM
L244	1	L92 and backup	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/24 12:18 AM
L245	31	("20060085844" OR "20070266256" OR "20080059804" OR "20090191846" OR "20110138450" OR "7780080" OR "8776214" OR "10872152" OR "5010571" OR "5499298" OR "20040107170" OR "20040236632" OR "20050198348" OR "20090100269" OR "20100242102" OR "20110078771" OR "20110205016" OR "20110231651" OR "20120110341" OR "20120167193" OR "6016476" OR "6691232" OR "7512965" OR "7697729" OR "7950051" OR "8145916" OR "8549300" OR "8577813" OR "8856539" OR "8984596" OR "9100826").pn.	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/24 02:39 PM
L246	1	"20070257104".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2022/01/24 04:33 PM
L247	1	243 AND (backup (back ADJ up))	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB,	OR	ON	ON	2022/01/24 06:03 PM

			HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L248	17	((US-20090100269-A1 OR US-20110231651-A1 OR US-20050198348-A1 OR US-20060247982-A1 OR US-20110205016-A1 OR US-20120110341-A1 OR US-20100242102-A1 OR US-20120167193-A1 OR US-20080059804-A1 OR US-20090191846-A1 OR US-20060085844-A1 OR US-20070257104-A1).did. AND PGPB.dbnm.) OR ((US-7512965-B1 OR US-7950051-B1 OR US-8549300-B1 OR US-8776214-B1 OR US-7780080-B2).did. AND USPT.dbnm.)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/01/24 06:03 PM
L249	1	243 AND (pair$3)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/01/24 06:09 PM
L250	17	((US-20090100269-A1 OR US-20110231651-A1 OR US-20100242102-A1 OR US-20120110341-A1 OR US-20110205016-A1 OR US-20060247982-A1 OR	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DK, EA, EE, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV,	OR	ON	ON	2022/01/25 01:36 AM

APPL-1002
APPLE INC. / Page 120 of 419

		US-20050198348-A1 OR US-20120167193-A1 OR US-20080059804-A1 OR US-20090191846-A1 OR US-20060085844-A1 OR US-20070257104-A1).did. AND PGPB.dbnm.) OR ((US-8549300-B1 OR US-7950051-B1 OR US-7512965-B1 OR US-8776214-B1 OR US-7780080-B2).did. AND USPT.dbnm.)	MA, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L251	0	250 AND (copy$3 SAME (modif$3 modification, alter$3 edit$3) SAME (backup (back ADJ up)))	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DK, EA, EE, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/01/25 01:38 AM
L252	186	239 AND (copy$3 SAME (modif$3 modification, alter$3 edit$3) SAME (backup (back ADJ up)))	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DK, EA, EE, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/01/25 01:38 AM
L253	3	252 AND ((backup (back ADJ up)) SAME brand)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DK, EA, EE, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR,	OR	ON	ON	2022/01/25 01:39 AM

			TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L254	1	"20140250079".pn.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2022/01/25 01:42 AM
L257	97360	(G06F21/10,121,128,31,32,44, H04L63/0861,10,20).cpc.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2022/01/25 02:11 AM
L258	67920	(H04L63/08,0815,0823,083,0281,0869).cpc.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2022/01/25 02:11 AM
L259	748	(257 258) AND (copy$3 SAME (modif$3 modification, alter$3 edit$3) SAME (backup (back ADJ up)))	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DK, EA, EE, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/01/25 02:12 AM
L260	31	259 AND ((backup (back ADJ up)) SAME brand)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DK, EA, EE, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/01/25 02:12 AM

PE2E SEARCH - Search History (Interference)

There are no Interference searches to show.

APPL-1002
APPLE INC. / Page 122 of 419

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

BIB DATA SHEET

CONFIRMATION NO. 1102

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
17/123,018	12/15/2020 RULE	216	2497	MJAKP026

APPLICANTS
RightQuestion, LLC, Portola Valley, CA

INVENTORS
Bjorn Markus Jakobsson, Portola Valley, CA;

**** CONTINUING DATA ***************************
This application is a CIP of 17/027,481 09/21/2020
which is a CON of 16/773,767 01/27/2020 PAT 10929512
which is a CON of 16/563,715 09/06/2019 PAT 10824696
which is a CON of 16/273,797 02/12/2019 PAT 10521568
which is a CON of 15/042,636 02/12/2016 PAT 10360351
which is a CON of 13/706,254 12/05/2012 PAT 9294452
which claims benefit of 61/587,387 01/17/2012
and claims benefit of 61/569,112 12/09/2011

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
12/30/2020

Foreign Priority claimed	❑ Yes ☑ No	❑ Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
35 USC 119(a-d) conditions met	❑ Yes ☑ No		CA	15	22	3
Verified and Acknowledged	/ANDREW J STEINLE/ Examiner's Signature	Initials				

ADDRESS
VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014
UNITED STATES

TITLE
AUTHENTICATION TRANSLATION

FILING FEE RECEIVED	FEES: Authority has been given in Paper	
1010	No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	❑ All Fees ❑ 1.16 Fees (Filing) ❑ 1.17 Fees (Processing Ext. of time) ❑ 1.18 Fees (Issue) ❑ Other _____ ❑ Credit

BIB (Rev. 05/07).

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17123018
Filing Date	2020-12-15
First Named Inventor	Bjorn Markus Jakobsson
Art Unit	1718xx 2497
Examiner Name	~~Not Assigned~~ Andrew Steinle
Attorney Docket Number	MJAKP026

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5010571		1991-04-23	KATZNELSON RON D	
	2	5499298		1996-03-12	NARASIMHALU ARCOT D	
	3	10872152		2020-12-22	MARTEL PIERRE OLIVIER	

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17123018
	Filing Date	2020-12-15
	First Named Inventor	Bjorn Markus Jakobsson
	Art Unit	2497
	Examiner Name	Andrew Steinle
	Attorney Docket Number	MJAKP026

If you wish to add additional Foreign Patent Document citation information please click the Add button [Add]

NON-PATENT LITERATURE DOCUMENTS [Remove]

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

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

EXAMINER SIGNATURE

Examiner Signature	/ANDREW J STEINLE/	Date Considered	01/22/2022

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

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

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

Google backup a modified version of the vault

All Videos Shopping News More Settings Tools

About 4,670 results (0.39 seconds)

www.google.com/patents/US8099605

Intelligent storage device for backup system

Grant · Filed Jun 1, 2007 · Issued Jan 17, 2012 · Leif Olov Billström · InventSec AB
The device offers high protection against destruction or **modification** of already ... By using this method, there is always a **copy** in the **vault** and there is ...
Overview · Related · Discuss

www.google.com/patents/US8874527

Local seeding of a restore storage for restoring a backup ...

Grant · Filed Mar 1, 2013 · Issued Oct 28, 2014 · Andrew Lynn Gardner · Storagecraft Technology Corporation
The remote **vault** storage is remote from the restore storage and the local ... files are backed up if they have been **modified** since the previous **backup**.
Overview · Related · Discuss

www.google.com/patents/US8751454

Virtual defragmentation in a deduplication vault

Grant · Filed Jan 28, 2014 · Issued Jun 10, 2014 · Nathan S. Bushman · Storagecraft Technology Corporation
Similarly, each of a base **backup** and multiple incremental **backups** of the source storage 110 that is stored in the **vault** storage 108 includes a **copy** of the ...
Overview · Related · Discuss

www.google.com/patents/US20040030852

System and method for data backup

App. · Filed Mar 18, 2003 · Published Feb 12, 2004 · David Coombs · Coombs David Lawrence
Each full **backup** comprises a **copy** of the data selected from the first storage device in accordance with a first criteria and attribute data representative ...
Overview · Related · Discuss

www.google.com/patents/US8151139

Preventing data loss from restore overwrites

Grant · Filed Mar 27, 2009 · Issued Apr 3, 2012 · Paul T. Gordon · Symantec Corporation
One such method and system copies data to a restore **backup** of a working **copy**, ... Further, a **modified version** of a logical data object is a **version** of that ...
Overview · Related · Discuss

www.google.com/patents/US20160210198

One-click backup in a cloud-based disaster recovery system

App. · Filed Jul 18, 2014 · Published Jul 21, 2016 · Sachin Baban Durge · Sachin Baban Durge
It is determined that a **modification** occurs to a data block in the local ... be **backup** of computer data by automatically saving a **copy** of every change made ...
Overview · Related · Discuss

www.google.com/patents/US6785786

Data backup and recovery systems

Grant · Filed Aug 28, 1998 · Issued Aug 31, 2004 · Stephen Gold · Hewlett Packard Development Company, L.P.
2 is a diagram of a computer network **modified** to operate in accordance with the ... In order to ensure that a **backup copy** of a file does not contain a ...
Overview · Related · Discuss

www.google.com/patents/EP0650122B1?cl=en

Remote back-up device and method for numerical data

Grant · Filed Oct 19, 1994 · Issued Mar 25, 1998 · Christian Ferrand · Christian Ferrand
The archiving means 2 is **adapted** to receive, process, store and transmit ... some of the old versions files that have been transmitted in the last backups by ...

Help Send feedback Privacy Terms

APPL-1002
APPLE INC. / Page 126 of 419

www.google.com/patents/US5276860

Digital data processor with improved backup storage

Grant · Filed Dec 19, 1989 · Issued Jan 4, 1994 · Richard W. Fortier · Epoch Systems, Inc.

It does, however, **copy** the attributes of those files to the full/incremental **backup** volumes. This enables the system to treat baseline **backup** copies as current ...

Overview · Related · Discuss

www.google.com/patents/US20070100913

Method and system for data backup

App. · Filed Oct 12, 2006 · Published May 3, 2007 · Gary Sumner · Sumner Gary S

9 illustrates operations performed by the data-**vault** application related to ... file and the subsequent, altered or **modified version** of the original file.

Overview · Related · Discuss

1 2 3 4 5 6 7 8 9 10 Next

APPL-1002
APPLE INC. / Page 127 of 419

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	17123018
Filing Date	2020-12-15
First Named Inventor	Bjorn Markus Jakobsson
Art Unit	N/Axx 2497
Examiner Name	N/Axx Andrew Steinle
Attorney Docket Number	MJAKP026

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6016476		2000-01-18	MAES STEPHANE HERMAN	
	2	6691232		2004-02-10	WOOD DAVID L	
	3	7512965		2009-03-31	AMDUR EUGENE	
	4	7697729		2010-04-13	HOWELL MARK J	
	5	7950051		2011-05-24	SPITZ SEAN T	
	6	8145916		2012-03-27	BOSHRA MICHAEL	
	7	8549300		2013-10-01	KUMAR KARTIK	
	8	8577813		2013-11-05	WEISS KENNETH P	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17123018
	Filing Date	2020-12-15
	First Named Inventor	Bjorn Markus Jakobsson
	Art Unit	~~N/A~~ 2497
	Examiner Name	~~N/A~~ Andrew Steinle
	Attorney Docket Number	MJAKP026

	9	8856539		2014-10-07	WEISS KENNETH	
	10	8984596		2015-03-17	GRIFFIN STEPHANIE	
	11	9100826		2015-08-04	WEISS KENNETH P	

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20040107170		2004-06-03	LABROU YANNIS	
	2	20040236632		2004-11-25	MARITZEN MICHAEL L	
	3	20050198348		2005-09-08	YEATES ANTHONY J	
	4	20090100269		2009-04-16	NACCACHE DAVID	
	5	20100242102		2010-09-23	CROSS DAVID B	
	6	20110078771		2011-03-31	GRIFFIN STEPHANIE	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17123018
	Filing Date	2020-12-15
	First Named Inventor	Bjorn Markus Jakobsson
	Art Unit	~~N/A~~ 2497
	Examiner Name	~~N/A~~ Andrew Steinle
	Attorney Docket Number	MJAKP026

	7	20110205016		2011-08-25	AL-AZEM SAMER	
	8	20110231651		2011-09-22	BOLLAY BENN SAPIN	
	9	20120110341		2012-05-03	BEIGI HOMAYOON	
	10	20120167193		2012-06-28	GARGARO GIANLUCA	

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2004051585	WO		2004-06-17	JAKOBSSON MARKUS		
	2	2005001751	WO		2005-01-06	REGENTS OF THE UNIVERSITY OF CALIFORNIA		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	"Managing Authorization and Access Control", Author: unknown, Published November 3, 2005, pp. 1-12, URL: http://technet.microsoft.com/en-us/library/bb457115.aspx	

EFS Web 2.1.18

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17123018
	Filing Date	2020-12-15
	First Named Inventor	Bjorn Markus Jakobsson
	Art Unit	N/Axx 2497
	Examiner Name	N/Axx Andrew Steinle
	Attorney Docket Number	MJAKP026

	2	BRANDS ET AL. Distance-Bounding Protocols. January 28, 1994: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.51.6437&rep=rep1&type=pdf	
	3	Hammer-Lahav, Ed. "The OAuth 1.0 Protocol", from https://tools.ietf.org/html/rfc5849, April 2010.	
	4	JAKOBSSON ET AL. Proving Without Knowing: On Oblivious, Agnostic and Blindfolded Provers. July 24, 1996: http://markus-jakobsson.com/papers/jakobsson-crypto96.pdf	
	5	MONROSE ET AL. Using Voice to Generate Cryptographic Keys. May 13, 2001: https://www.cs.unc.edu/~fabian/papers/odyssey.pdf	
	6	SESHADRI ET AL. Pioneer: Verifying Code Integrity and Enforcing Untampered Code Execution on Legacy Systems. October 23, 2005: https://netsec.ethz.ch/publications/papers/pioneer.pdf	

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

EXAMINER SIGNATURE

Examiner Signature	/ANDREW J STEINLE/	Date Considered	01/22/2022

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

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

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

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	17123018
Filing Date	2020-12-15
First Named Inventor	Bjorn Markus Jakobsson
Art Unit	OPAP
Examiner Name	Docket Central
Attorney Docket Number	MJAKP026

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	7780080		2010-08-24	OWEN KELLY	
	2	8776214		2014-07-08	JOHANSSON JESPER M	

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20060085844		2006-04-20	BUER MARK	
	2	20070266256		2007-11-15	SHAH YOGENDRA C	
	3	20080059804		2008-03-06	SHAH YOGENDRA C	
	4	20090191846		2009-07-30	SHI GUANGMING	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17123018
	Filing Date	2020-12-15
	First Named Inventor	Bjorn Markus Jakobsson
	Art Unit	OPAP
	Examiner Name	Docket Central
	Attorney Docket Number	MJAKP026

	5	20110138450		2011-06-09	KESANUPALLI RAMESH			

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	IPR2022-00244 Claim Mapping Table for the '696 Patent. November 30, 2021	
	2	IPR2022-00244 Petition for Inter Partes Review of U.S. Patent No. 10,824,696. November 30, 2021	
	3	IPR2022-00251 Claim Mapping Table for the '512 Patent. December 1, 2021	
	4	IPR2022-00251 Petition for Inter Partes Review of U.S. Patent No. 10,929,512. December 1, 2021	

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

EFS Web 2.1.18

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17123018
	Filing Date	2020-12-15
	First Named Inventor	Bjorn Markus Jakobsson
	Art Unit	OPAP
	Examiner Name	Docket Central
	Attorney Docket Number	MJAKP026

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17123018
	Filing Date	2020-12-15
	First Named Inventor	Bjorn Markus Jakobsson
	Art Unit	OPAP
	Examiner Name	Docket Central
	Attorney Docket Number	MJAKP026

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/Yeu-Ting George Cheng/	Date (YYYY-MM-DD)	2021-12-23
Name/Print	Yeu-Ting George Cheng	Registration Number	69408

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

Electronic Acknowledgement Receipt

EFS ID:	44604864
Application Number:	17123018
International Application Number:	
Confirmation Number:	1102
Title of Invention:	AUTHENTICATION TRANSLATION
First Named Inventor/Applicant Name:	Bjorn Markus Jakobsson
Customer Number:	21912
Filer:	Yeu-Ting George Cheng/Elaine Nguyen
Filer Authorized By:	Yeu-Ting George Cheng
Attorney Docket Number:	MJAKP026
Receipt Date:	23-DEC-2021
Filing Date:	15-DEC-2020
Time Stamp:	17:41:38
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	MJAKP026_IDS_03_SB08.pdf	1053570 683ae19d30d19d2a30698893babc23e1f5974028	no	5

Warnings:

Information:					
2	Non Patent Literature	IPR2022-00244_Claim_Mapping_Table_for_the_696_Patent.pdf	770926 5f33603fece7760236c03d97a53bbc92cbd22e24	no	5
Warnings:					
Information:					
3	Non Patent Literature	IPR2022-00244_Petition_for_Inter_Partes_Review_of_US_Patent_No_10824696.pdf	746238 dc0a54ce9eeb861c8f2c1c0cb4ae83ce5b62c3c5	no	82
Warnings:					
Information:					
4	Non Patent Literature	IPR2022-00251_Claim_Mapping_Table_for_the_512_Patent.pdf	787926 2477e2bebedb1c07a7d85c945f3d2c3a34d20cce	no	6
Warnings:					
Information:					
5	Non Patent Literature	IPR2022-00251_Petition_for_Inter_Partes_Review_of_US_Patent_No_10929512.pdf	706385 4296e6fd8f650482b52813c43474b8dbeb65a1e1	no	80
Warnings:					
Information:					
		Total Files Size (in bytes):	4065045		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
17/123,018	12/15/2020	Bjorn Markus Jakobsson	MJAKP026

CONFIRMATION NO. 1102

21912
VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

PUBLICATION NOTICE

OC000000126219959

Title:AUTHENTICATION TRANSLATION

Publication No.US-2021-0173897-A1
Publication Date:06/10/2021

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Public Records Division. The Public Records Division can be reached by telephone at (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, by mail addressed to the United States Patent and Trademark Office, Public Records Division, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently https://portal.uspto.gov/pair/PublicPair. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
17/123,018	12/15/2020	1713	1010	MJAKP026	22	3

CONFIRMATION NO. 1102

UPDATED FILING RECEIPT

21912
VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

OC000000123788810

Date Mailed: 03/04/2021

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

Bjorn Markus Jakobsson, Portola Valley, CA;

Applicant(s)

RightQuestion, LLC, Portola Valley, CA

Power of Attorney: The patent practitioners associated with Customer Number 21912

Domestic Priority data as claimed by applicant

This application is a CIP of 17/027,481 09/21/2020
which is a CON of 16/773,767 01/27/2020 PAT 10929512
which is a CON of 16/563,715 09/06/2019 PAT 10824696
which is a CON of 16/273,797 02/12/2019 PAT 10521568
which is a CON of 15/042,636 02/12/2016 PAT 10360351
which is a CON of 13/706,254 12/05/2012 PAT 9294452
which claims benefit of 61/587,387 01/17/2012
and claims benefit of 61/569,112 12/09/2011

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 12/30/2020
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 17/123,018**
Projected Publication Date: 06/10/2021
Non-Publication Request: No
Early Publication Request: No
**** SMALL ENTITY ****
Title

AUTHENTICATION TRANSLATION

Preliminary Class

216

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative,

this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop

technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 17/123,018

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	80		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	350		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	400		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	22 minus 20 =	* 2	x 50 =	100	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*	x 240 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	930		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

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

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
17/123,018	12/15/2020	Bjorn Markus Jakobsson	MJAKP026

CONFIRMATION NO. 1102

21912
VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

POA ACCEPTANCE LETTER

OC000000123786973

Date Mailed: 03/04/2021

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 03/01/2021.

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.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/zabraha/

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.:	17/123,018	Examiner:	Not Assigned
Filed:	December 15, 2020	Art Unit:	1713
Confirmation No.:	1102	Docket No.:	MJAKP026
First Inventor:	Bjorn Markus Jakobsson		
Title:	AUTHENTICATION TRANSLATION		

RESPONSE TO NOTICE TO FILE MISSING PARTS

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

Sir:

This is a Response to the Notice to File Missing Parts mailed December 31, 2020.

Application Elements:

☒ Declaration
- ☒ Newly executed (original or copy)
- ☐ Copy from a prior application (37 CFR 1.63(d) for a continuation or divisional). The entire disclosure of the prior application from which a copy of the declaration is herein supplied is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.
- ☐ Deletion of inventors Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).

Accompanying Application Parts:

☐ Information Disclosure Statement with Form PTO/SB/08 ☐ Copies of IDS Citations
☒ Preliminary Amendment (*New claims numbered after highest original claim in prior application.*)
☒ Power of Attorney with ☒ Transmittal ☐ Statement Under 37 CFR 3.73
☒ Other: Replacement Drawings

Amendments

☐ Cancel in this application original claims _____ of the prior application before calculating the filing fee. (*At least one original independent claim must be retained.*)

Fee Calculation (37 CFR § 1.16)

				Small Entity			Large Entity	
				Rate	Fee		Rate	Fee
Filing Fees				x $80=$	80	OR	x $320=$	
Search Fees				x $350=$	350	OR	x $700=$	
Examination Fees				x $400=$	400	OR	x $800=$	
CLAIMS	Filed		Extra					
Total	22	Less 20	2	X $50= $	100	OR	x $100=$	
Independent	3	Less 3	0	x $240=$	0	OR	x $480=$	
Multiple Dependent Claims			-0-	x $430=$	0	OR	x $860=$	
Declaration and Surcharge Fee				x $80=$	80	OR	x $160=$	
Processing fee under Rule 1.17(i) to correct inventorship				x $70=$	0	OR	x $140=$	
				TOTAL FILING FEE $	**1,010**		TOTAL FILING FEE $	

☐ Applicants petition for an extension of time to respond under 37 CFR § 1.136(a) as follows:

	SMALL ENTITY			LARGE ENTITY	
	Rate	Add'l Fee		Rate	Add'l Fee
☐ Extension for Response within FIRST month	x $110=$		OR	x $220=$	
☐ Extension for Response within SECOND month	x $320=$		OR	x $640=$	
☐ Extension for Response within THIRD month	x $740=$		OR	x $1480=$	
☐ Extension for Response within FOURTH month	x $1160=$		OR	x $2320=$	
☐ Extension for Response within FIFTH month	x $1580=$		OR	x $3160=$	

☒ Please charge Deposit Account No. 50-0685 (MJAKP026) in the amount of $1,010.00 to cover the filing fees, the additional claim fee, if any, and/or extension of time fees.

General Authorizations

☒ Applicants hereby make and generally authorize any Petitions for Extensions of Time as needed for this or any subsequent filings. The Commissioner is also authorized to charge any extension fees under 37 CFR §1.17 as needed to Deposit Account No. 50-0685 (Order No. MJAKP026).

☒ The Commissioner is given general authorization to charge any fees or to credit any overpayment during the pendency of this application to Deposit Account No. 50-0685 (Order No. MJAKP026).

☒ Please send correspondence to the following address:

Customer No. 21912
VAN PELT, YI & JAMES LLP
10050 N. Foothill Blvd., Suite 200
Cupertino, CA 95014

Dated: March 1, 2021

/Yeu-Ting George Cheng/
Yeu-Ting George Cheng
Registration No. 69408

DECLARATION
FOR ORIGINAL U.S. PATENT APPLICATION

Attorney's Docket No. MJAKP026

As a below-named inventor, I hereby declare that:

I believe that I am the original inventor (if only one name is listed below) or an original joint inventor (if plural names are listed below) of a claimed invention in the application entitled: **AUTHENTICATION TRANSLATION**, the specification of which,

(check one) 1. ☐ is attached hereto.

2. ☒ was filed on December 15, 2020 as
U.S. Application No. 17/123,018
and was amended on _____.

3. ☐ was filed on _____ as
International PCT Application No. _____
and was amended on _____.

I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

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

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR § 1.56.

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 I acknowledge that any willful false statement made in this declaration is punishable under 18 USC 1001 by fine or imprisonment of not more than five (5) years, or both.

Full name of inventor	Bjorn Markus Jakobsson	
Signature of inventor	/_____/	Date: 6/4/21

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

PTO/AIA/82A (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

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

Application Number	17/123,018
Filing Date	December 15, 2020
First Named Inventor	Bjorn Markus Jakobsson
Title	AUTHENTICATION TRANSLATION
Art Unit	1713
Examiner Name	Not Assigned
Attorney Docket Number	MJAKP026

SIGNATURE of Applicant or Patent Practitioner

Signature	/Yeu-Ting George Cheng/	Date (Optional)	
Name	Yeu-Ting George Cheng	Registration Number	69408
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)			

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

☑ *Total of 1 forms are submitted.

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

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

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

PTO/AIA/82B (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

POWER OF ATTORNEY BY APPLICANT

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

Application Number	Filing Date

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

☑ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: 21912

OR

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

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

☑ The address associated with the above-mentioned Customer Number

OR

☐ The address associated with Customer Number:

OR

Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

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

RightQuestion, LLC

☐ Inventor or Joint Inventor (title not required below)

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

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

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

SIGNATURE of Applicant for Patent

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

Signature		Date (Optional)	
Name	Bjorn Markus Jakobsson		
Title	Manager		

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

☐ Total of forms are submitted.

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

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

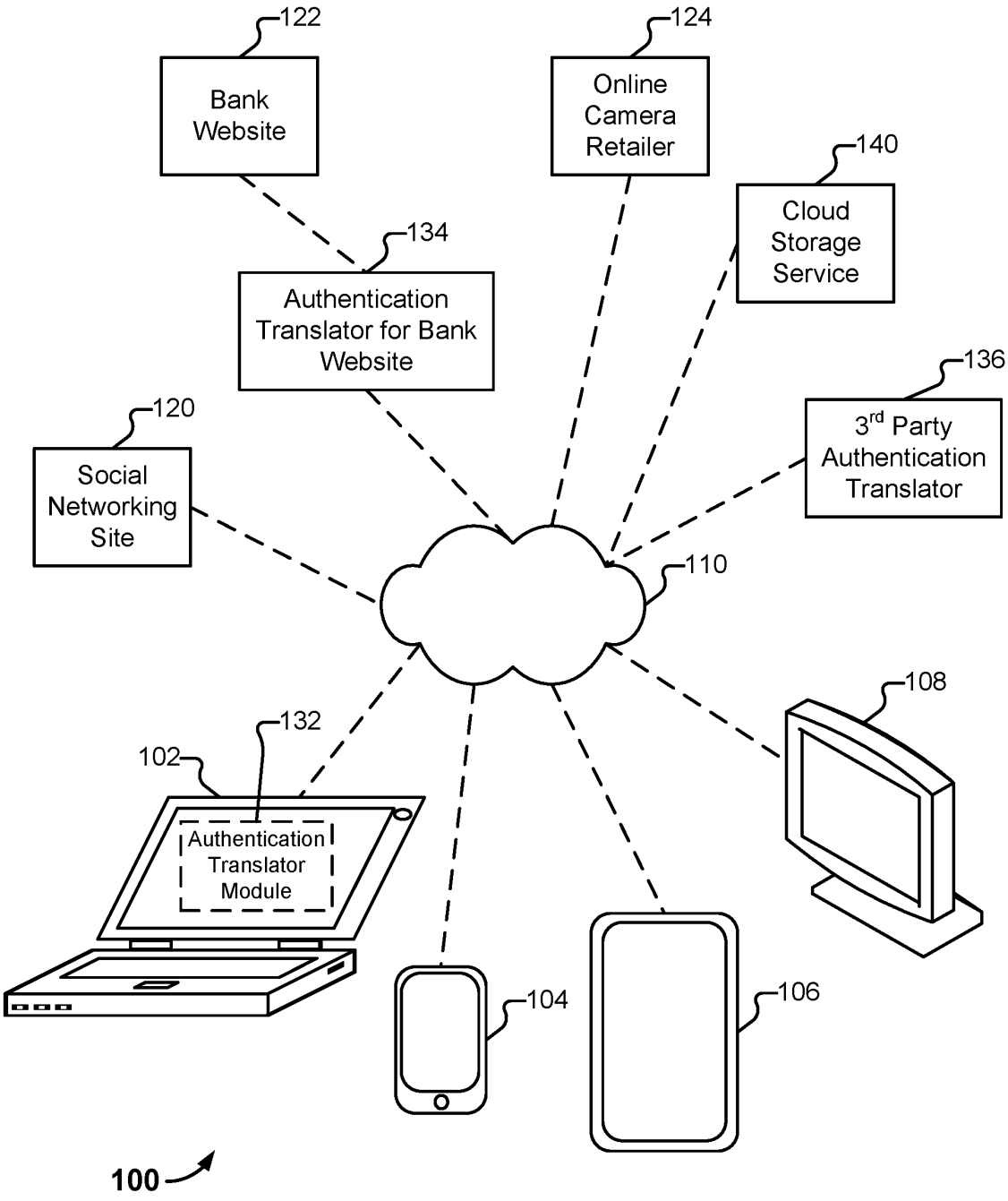

122
Bank Website
124
Online Camera Retailer
140
Cloud Storage Service
134
Authentication Translator for Bank Website
136
3rd Party Authentication Translator
120
Social Networking Site
110
108
132
102
Authentication Translator Module
104
106
100

FIG. 1

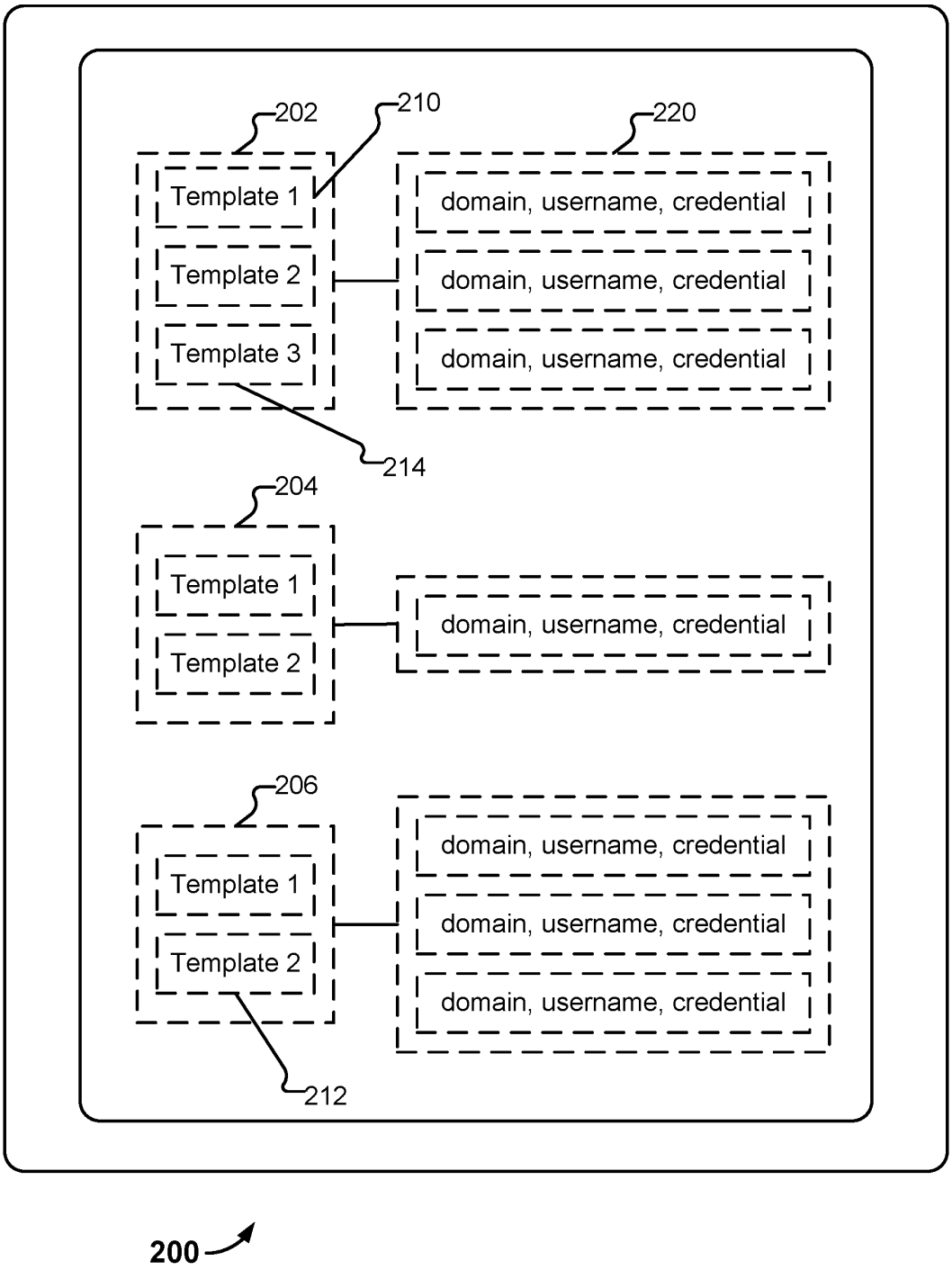

202
210
220
Template 1
Template 2
Template 3
domain, username, credential
domain, username, credential
domain, username, credential
214
204
Template 1
Template 2
domain, username, credential
206
Template 1
Template 2
domain, username, credential
domain, username, credential
domain, username, credential
212
200

FIG. 2

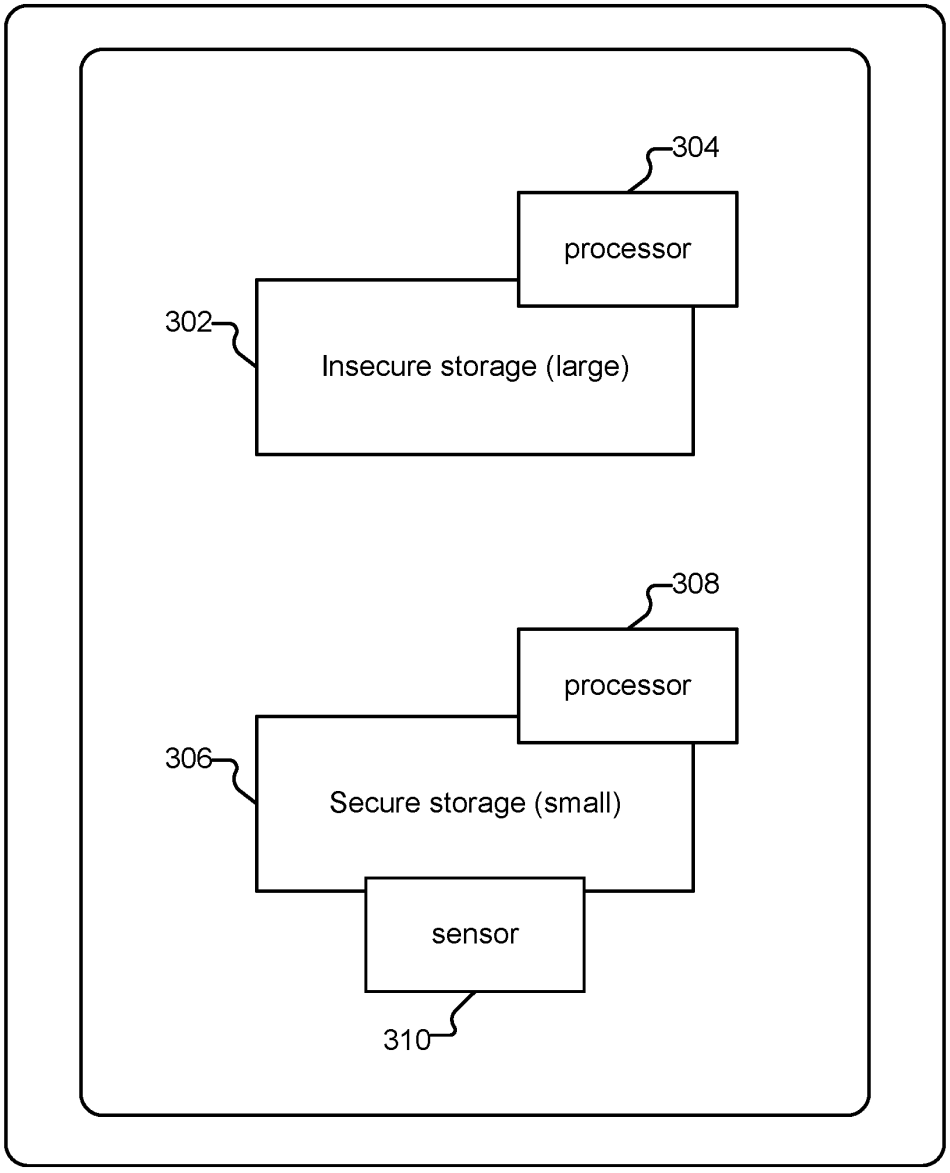

304
processor
302
Insecure storage (large)
308
processor
306
Secure storage (small)
sensor
310
300

FIG. 3

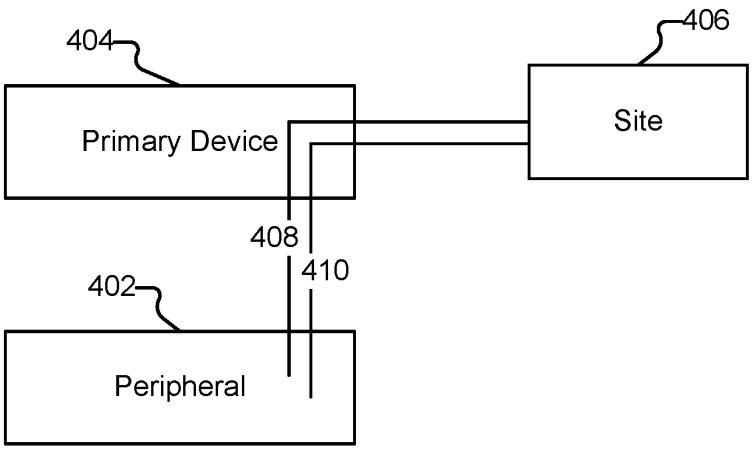


FIG. 4

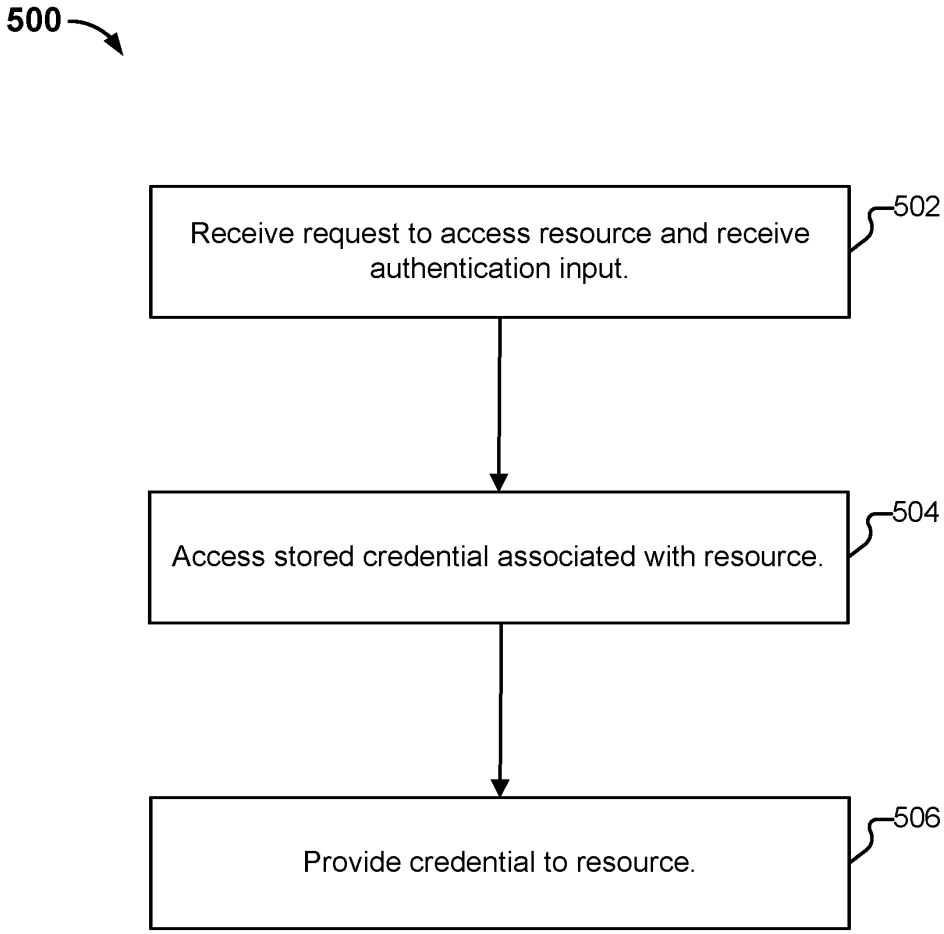

500
Receive request to access resource and receive authentication input.
502
Access stored credential associated with resource.
504
Provide credential to resource.
506

FIG. 5

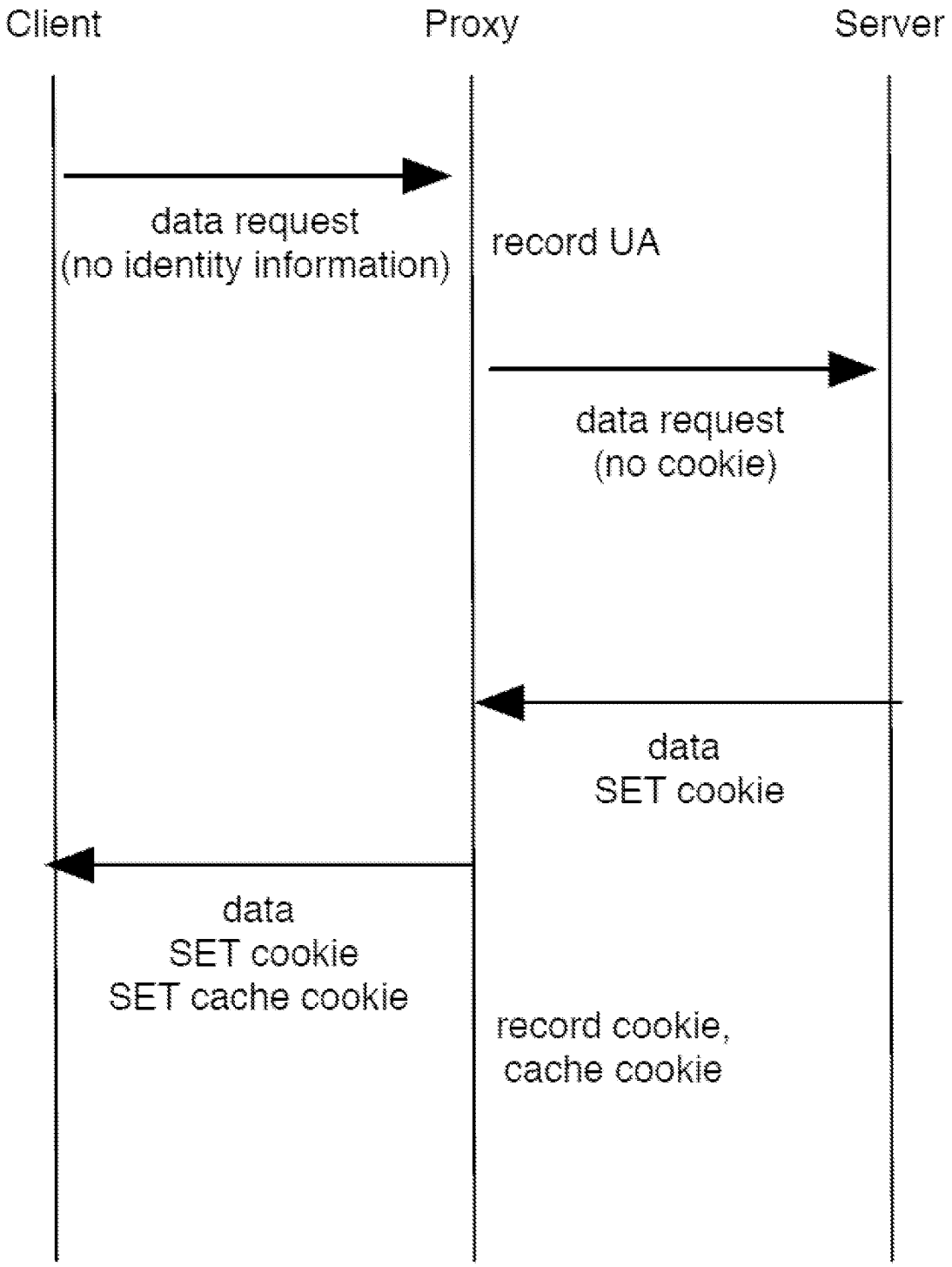

Client
Proxy
Server
data request
(no identity information)
record UA
data request
(no cookie)
data
SET cookie
data
SET cookie
SET cache cookie
record cookie,
cache cookie

FIG. 6

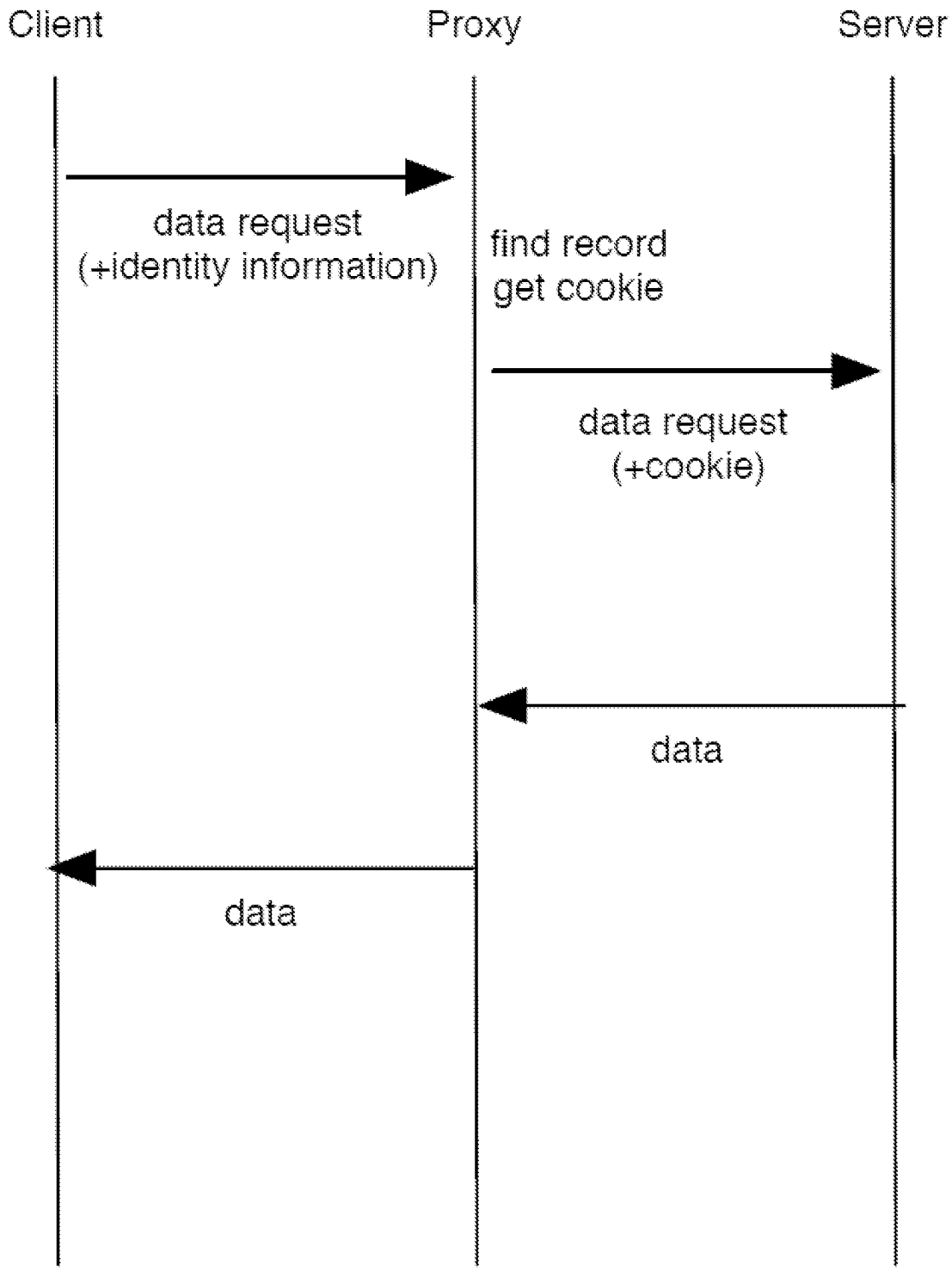

Client
Proxy
Server
data request
(+identity information)
find record
get cookie
data request
(+cookie)
data
data

FIG. 7

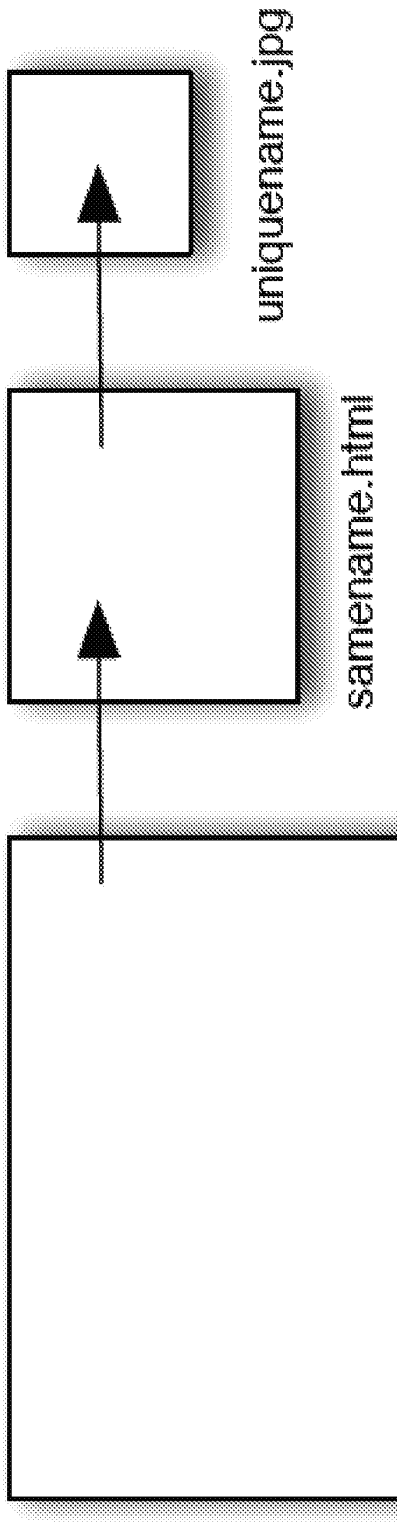


FIG. 8

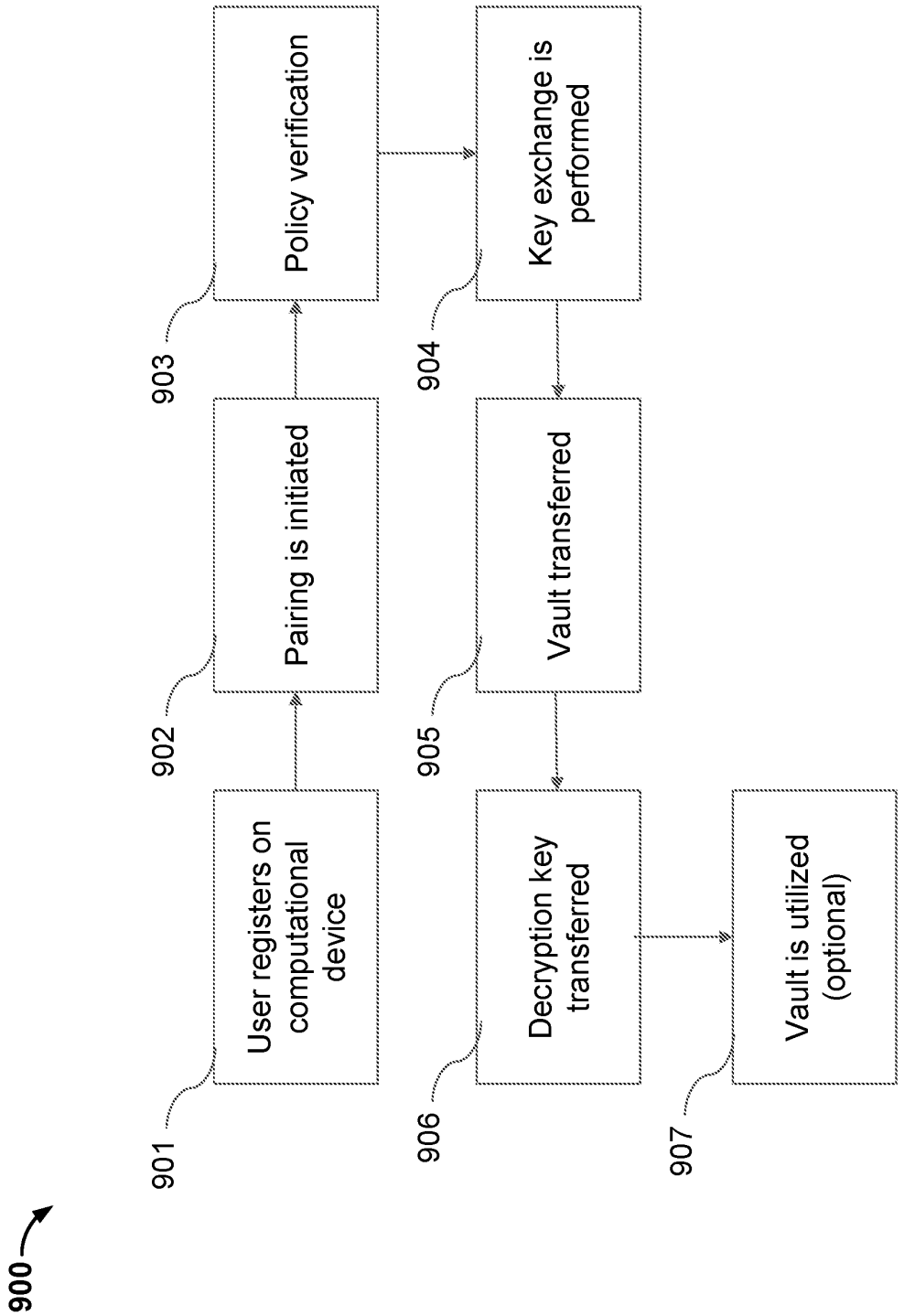

900
901
User registers on computational device
902
Pairing is initiated
903
Policy verification
904
Key exchange is performed
905
Vault transferred
906
Decryption key transferred
907
Vault is utilized (optional)

FIG. 9

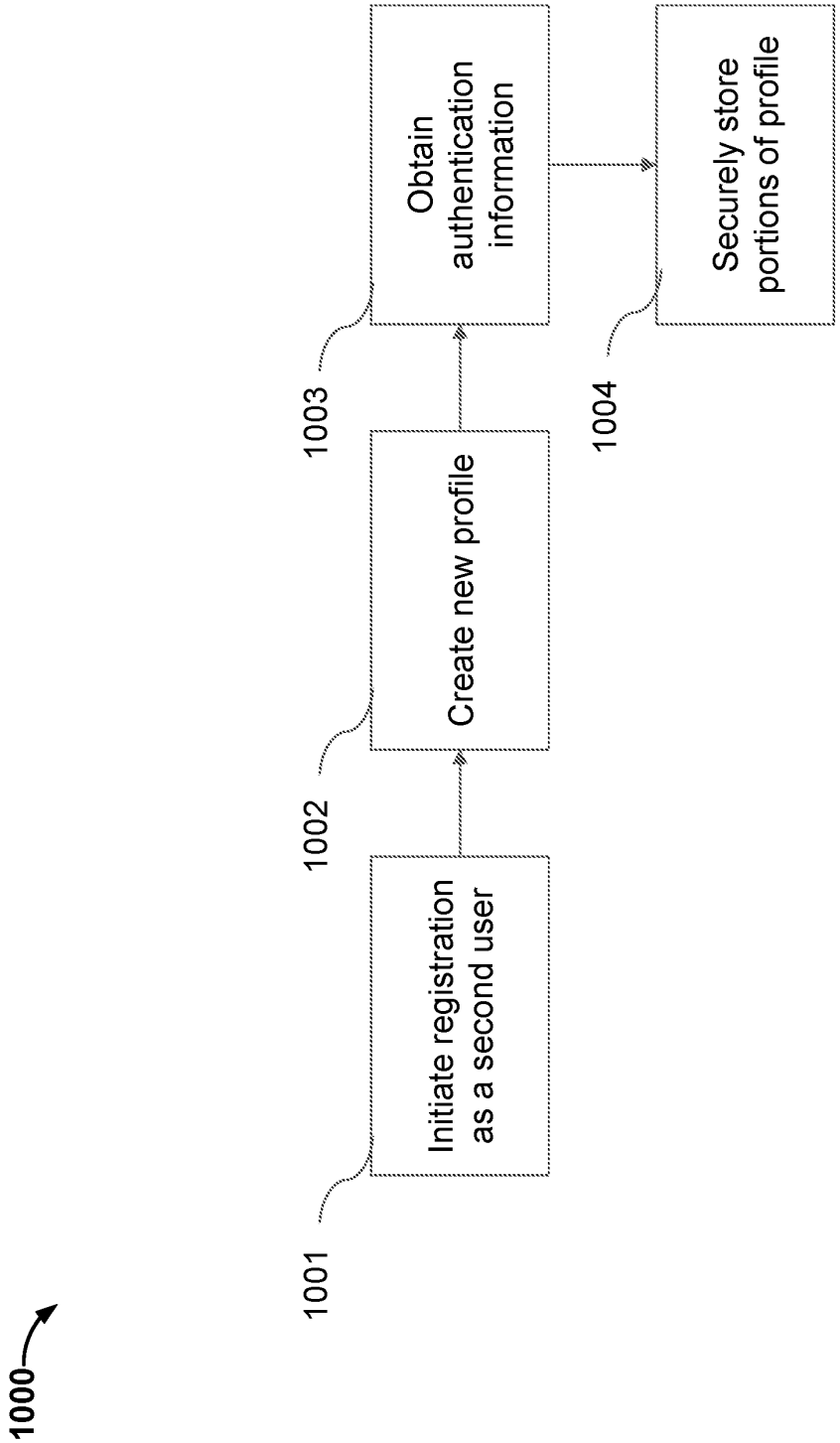

1000
1001
Initiate registration as a second user
1002
Create new profile
1003
Obtain authentication information
1004
Securely store portions of profile

FIG. 10

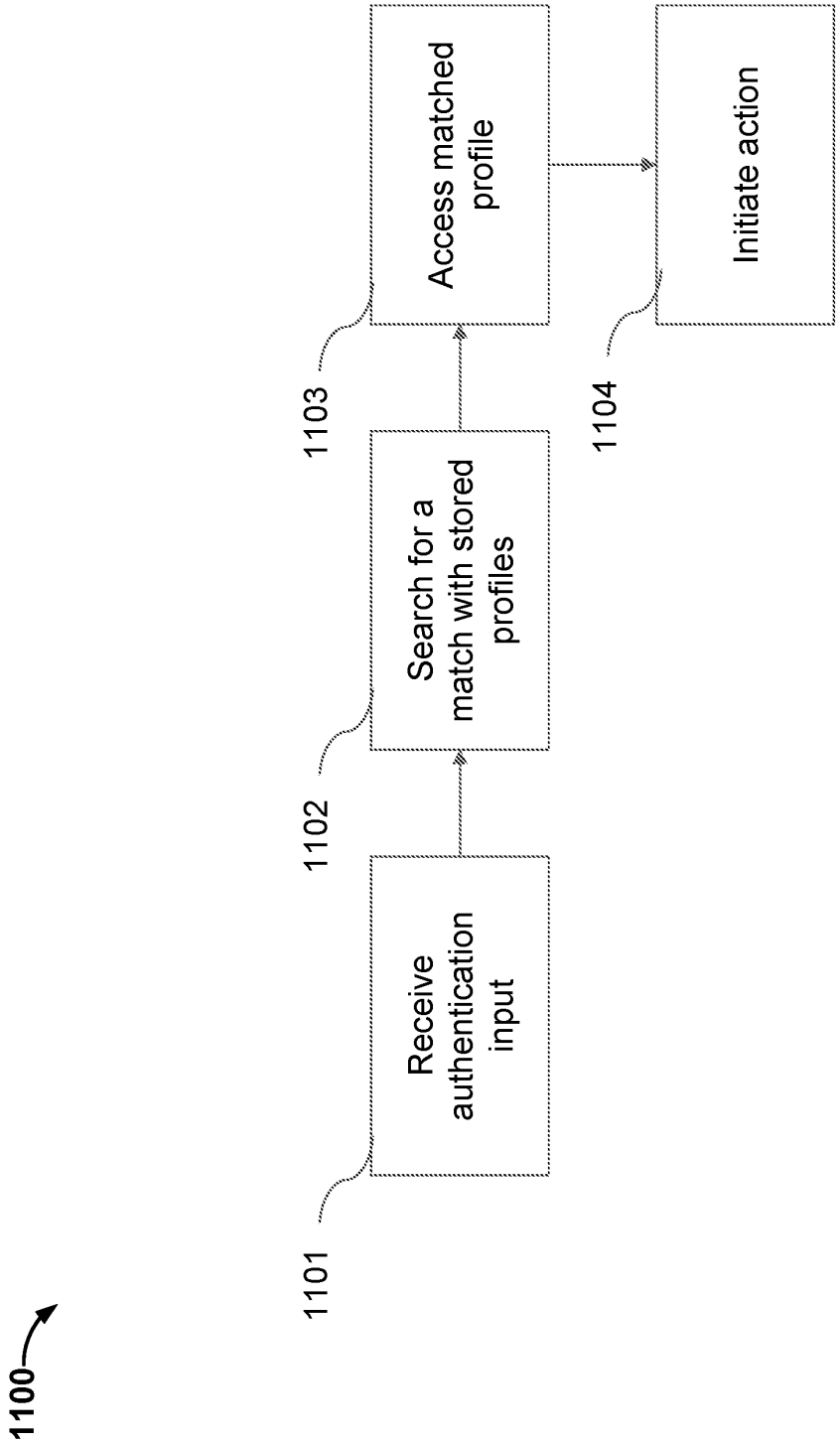

1100
1101
Receive authentication input
1102
Search for a match with stored profiles
1103
Access matched profile
1104
Initiate action

FIG. 11

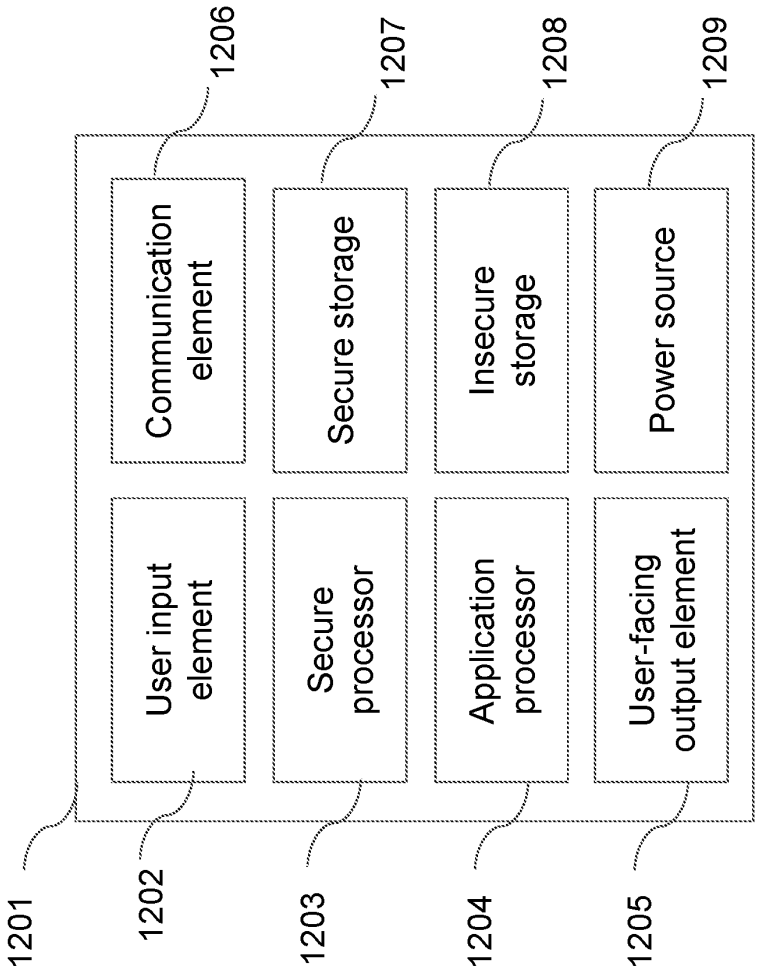

1201
1202
1203
1204
1205
1206
1207
1208
1209
User input element
Secure processor
Application processor
User-facing output element
Communication element
Secure storage
Insecure storage
Power source

FIG. 12

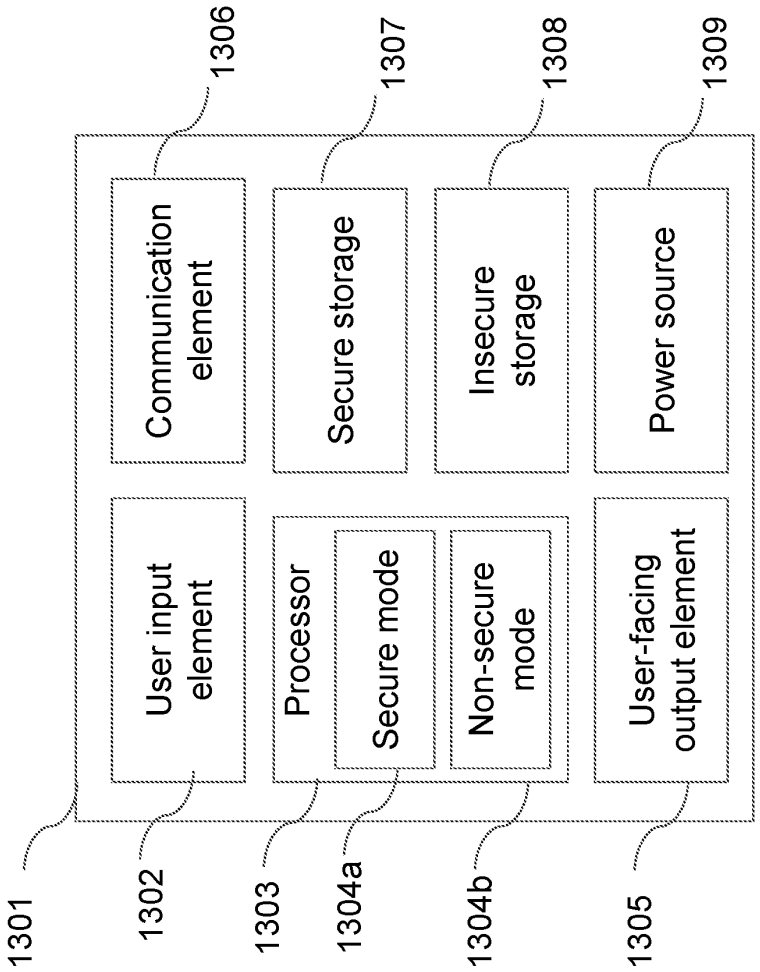

1301
1302
1303
1304a
1304b
1305
1306
1307
1308
1309
User input element
Processor
Secure mode
Non-secure mode
User-facing output element
Communication element
Secure storage
Insecure storage
Power source

FIG. 13

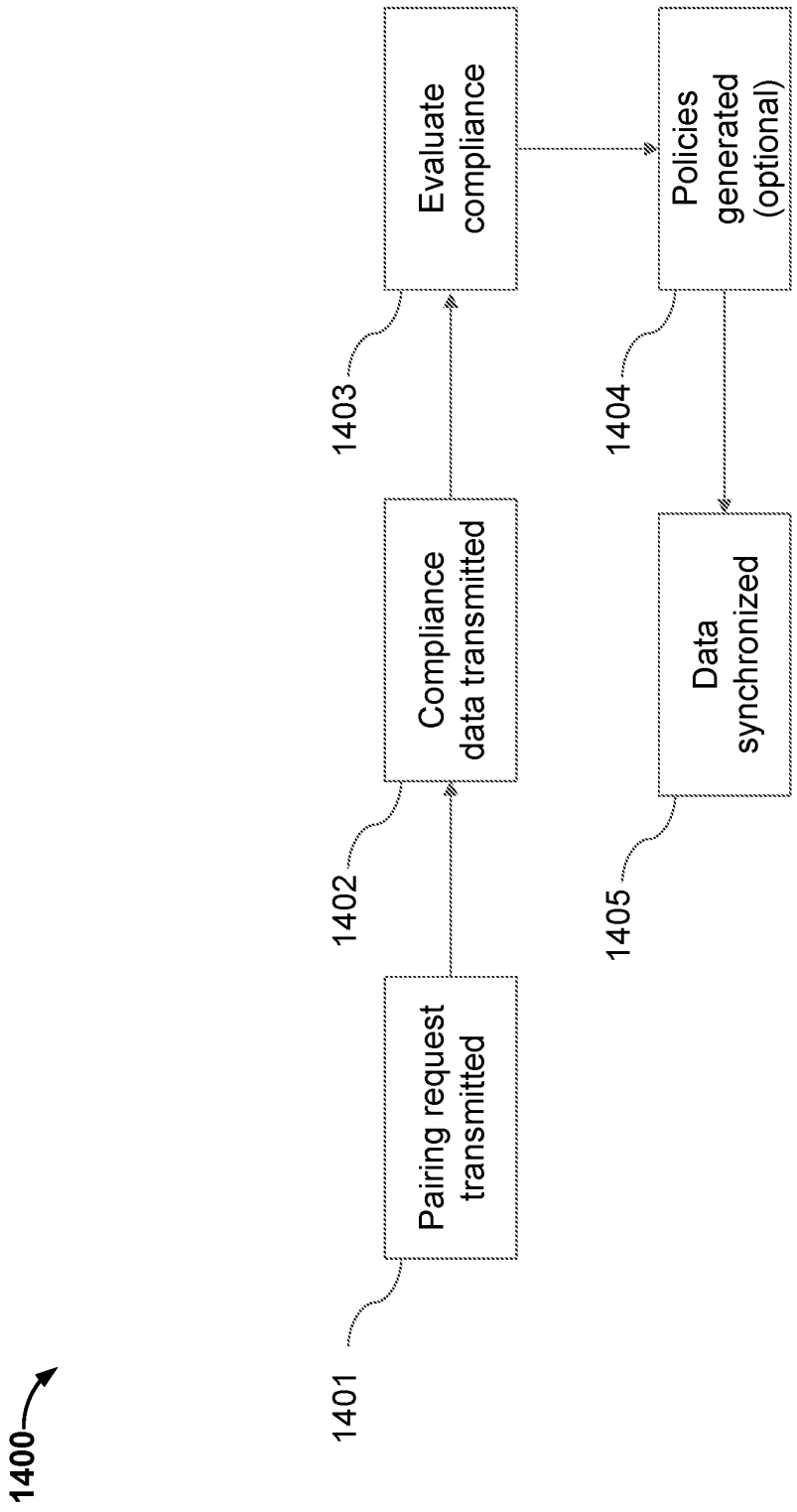

1400
1401
Pairing request transmitted
1402
Compliance data transmitted
1403
Evaluate compliance
1404
Policies generated (optional)
1405
Data synchronized

FIG. 14

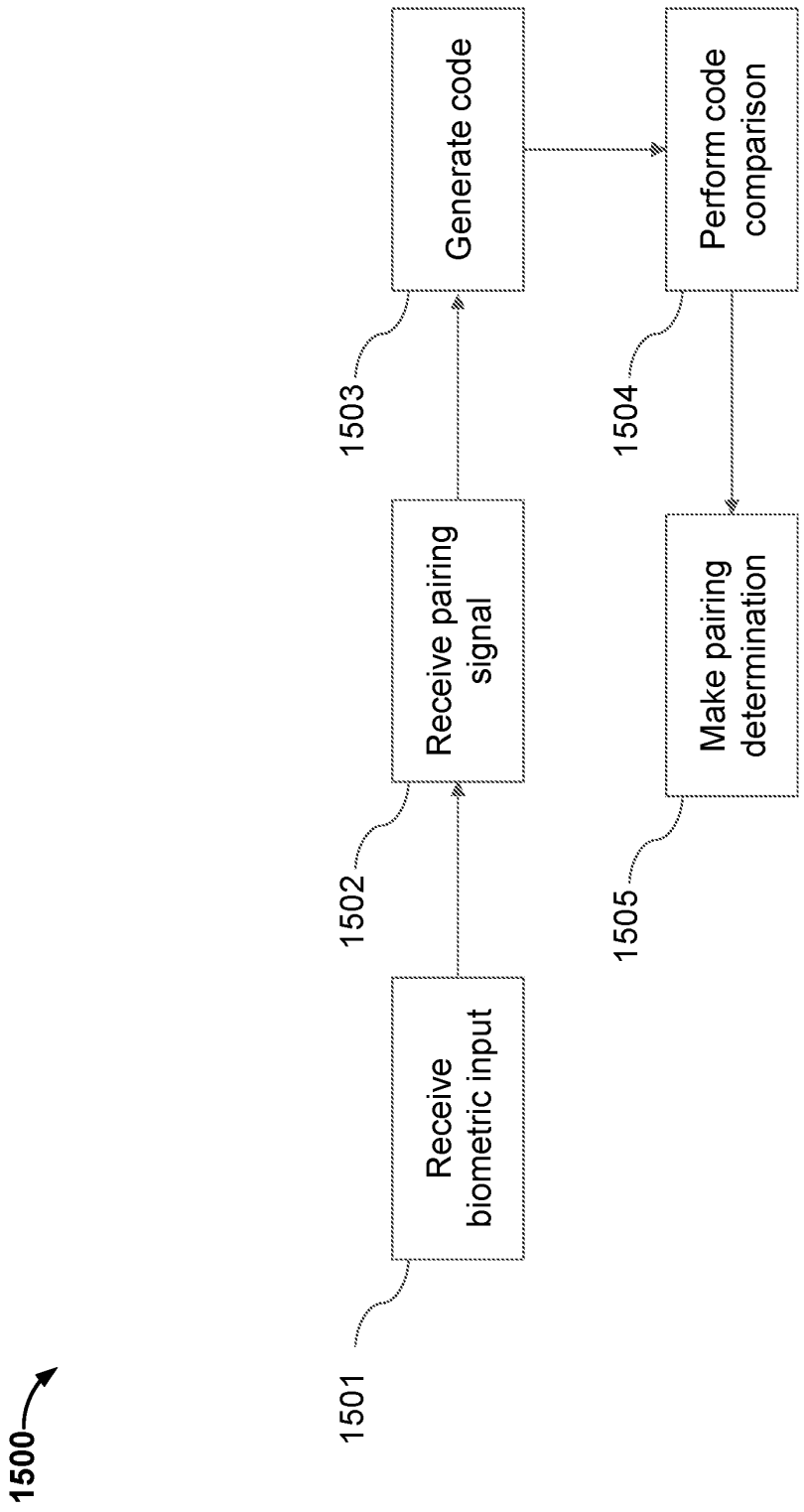

1500
1501
Receive biometric input
1502
Receive pairing signal
1503
Generate code
1504
Perform code comparison
1505
Make pairing determination

FIG. 15

Electronic Patent Application Fee Transmittal

Application Number:	17123018
Filing Date:	15-Dec-2020
Title of Invention:	AUTHENTICATION TRANSLATION
First Named Inventor/Applicant Name:	Bjorn Markus Jakobsson
Filer:	Yeu-Ting George Cheng/Elaine Nguyen
Attorney Docket Number:	MJAKP026

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
UTILITY FILING FEE (ELECTRONIC FILING)	4011	1	80	80
UTILITY SEARCH FEE	2111	1	350	350
UTILITY EXAMINATION FEE	2311	1	400	400
Pages:				
Claims:				
CLAIMS IN EXCESS OF 20	2202	2	50	100
Miscellaneous-Filing:				
LATE FILING FEE FOR OATH OR DECLARATION	2051	1	80	80

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**1010**

Electronic Acknowledgement Receipt

EFS ID:	42054868
Application Number:	17123018
International Application Number:	
Confirmation Number:	1102
Title of Invention:	AUTHENTICATION TRANSLATION
First Named Inventor/Applicant Name:	Bjorn Markus Jakobsson
Customer Number:	21912
Filer:	Yeu-Ting George Cheng/Elaine Nguyen
Filer Authorized By:	Yeu-Ting George Cheng
Attorney Docket Number:	MJAKP026
Receipt Date:	01-MAR-2021
Filing Date:	15-DEC-2020
Time Stamp:	18:55:53
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$1010
RAM confirmation Number	E202131I56240584
Deposit Account	500685
Authorized User	Elaine Nguyen
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.16 (National application filing, search, and examination fees) 37 CFR 1.17 (Patent application and reexamination processing fees)	

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Applicant Response to Pre-Exam Formalities Notice	MJAKP026_MP_Transmittal.pdf	106102 b8797a9424db80fa252c93a66852c43693a5618f	no	2
Warnings:					
Information:					
2	Oath or Declaration filed	MJAKP026_Executed_Dec.pdf	1411597 4db876d5cc325e52075605f9213d66a1fa02a8b5	no	1
Warnings:					
Information:					
3	Power of Attorney	MJAKP026_POA_AIA82A.pdf	168559 522394a20c4849f5027e3912c726727490c94570	no	1
Warnings:					
Information:					
4	Power of Attorney	MJAK_Executed_POA_AIA82B_RightQuestionLLC.pdf	387899 a756b6df61aa99188ddec71473eefbe19a844b6f	no	1
Warnings:					
Information:					
5	Preliminary Amendment	MJAKP026_AMD_A_PRE.pdf	118140 4e3a3b361263d5951fb0a93224b18643cd03231c	no	7
Warnings:					
Information:					
6	Drawings-only black and white line drawings	MJAKP026_MP_Figures.pdf	759298 94fe61cb5fef86c45680d62a1d6e89cf49df21ab	no	15
Warnings:					
Information:					

7	Fee Worksheet (SB06)	fee-info.pdf	38594 bb6319389131fcf8942eac0c979af4fffad785c5	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	2990189	

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.:	17/123,018	Examiner:	Not Assigned
Filed:	December 15, 2020	Art Unit:	1713
Confirmation No.:	1102	Docket No.:	MJAKP026
First Inventor:	Bjorn Markus Jakobsson		
Title:	AUTHENTICATION TRANSLATION		

PRELIMINARY AMENDMENT A

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

Dear Sir:

Prior to the examination of the application on the merits, please amend the application as follows:

Applicant(s) believe that no (additional) fees are required beyond any fees submitted herewith. If required fees are missing or any additional fees are required during the pendency of the subject application, please charge such fees or credit any overpayment to Deposit Account No. 50-0685 (MJAKP026).

IN THE CLAIMS

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

Listing of Claims:

1. (Original) A system, comprising:

one or more processors configured to:

receive, at a first device, a request to access a resource external to the first device, wherein the resource external to the first device is associated with a user;

access at least one record stored on the first device, the at least one record including authentication information associated with the user and credential information associated with the external resource to which the user has requested access, wherein the credential information comprises a cryptographic key;

receive authentication input from the user;

determine that the authentication input from the user matches the authentication information associated with the user included in the at least one record stored on the first device;

retrieve at least a portion of the credential information from the at least one record stored on the first device;

facilitate access of the user to the external resource at least in part by transmitting, on behalf of the user, from the first device, output based at least in part on the at least portion of the credential information retrieved from the at least one record, wherein the user of the first device is granted access to the external resource based at least in part on the output transmitted from the first device on behalf of the user; and

initiate a backup, to a second device, of at least a portion of the at least one record; and

a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.

2. (Original) The system of claim 1, wherein the second device is used to authenticate the user to one or more external resources.

3. (Original) The system of claim 1, wherein the backup is completed after the first device has performed a verification that the second device conforms to a policy associated with the at least one record stored on the first device.

4. (Original) The system of claim 1, wherein the backup is completed after a secure channel is established by at least one of the first device and the second device.

5. (Original) The system of claim 1, wherein the first device and the second device are configured to complete a pairing process.

6. (Original) The system of claim 5, wherein the pairing process comprises a comparison of data generated from one or more authentication inputs.

7. (Original) The system of claim 1, wherein subsequent to completion of the backup, the second device comprises a first profile associated with the user of the first device, and a second profile associated with a second user different from the user of the first device.

8. (Original) The system of claim 1, wherein the one or more processors are further configured to:

determine that the authentication input from the user does not match authentication information of a first profile; and

subsequent to determining that the authentication input from the user does not match the authentication information of the first profile, determine that the authentication input from the user matches authentication information of a second profile, wherein the first profile is associated with a different user than the second profile.

9. (Original) The system of claim 1, wherein the at least one record stored on the first device is stored in a secure storage, and where the one or more processors are configured to access the record stored on the secure storage using a restricted interface.

10. (Original) The system of claim 9, wherein the restricted interface comprises a dedicated physical connection.

11. (Original) The system of claim 9, wherein the restricted interface comprises an application programming interface.

12. (Original) The system of claim 1, wherein the backup causes a certificate to be transmitted to the second device.

13. (Original) The system of claim 12, wherein the certificate is generated at least in part by the first device.

14. (Original) The system of claim 1, wherein the authentication input from the user is received using a biometric user input element.

15. (Original) The system of claim 1, wherein the backup comprises copying a modified version of a vault to the second device.

16. (Original) The system of claim 1, wherein the backup is performed in response to a determination that the first device is of a same brand as the second device.

17. (Original) A method, comprising:

receiving, at a first device, a request to access a resource external to the first device, wherein the resource external to the first device is associated with a user;

accessing at least one record stored on the first device, the at least one record including authentication information associated with the user and credential information associated with the external resource to which the user has requested access, wherein the credential information comprises a cryptographic key;

receiving authentication input from the user;

determining that the authentication input from the user matches the authentication information associated with the user included in the at least one record stored on the first device;

retrieving at least a portion of the credential information from the at least one record stored on the first device;

facilitating access of the user to the external resource at least in part by transmitting, on behalf of the user, from the first device, output based at least in part on the at least portion of the credential information retrieved from the at least one record, wherein the user of the first device is granted access to the external resource based at least in part on the output transmitted from the first device on behalf of the user; and

initiating a backup, to a second device, of at least a portion of the at least one record.

18. (Original) A computer program product embodied in a non-transitory computer readable storage medium and comprising computing instructions for:

receiving, at a first device, a request to access a resource external to the first device, wherein the resource external to the first device is associated with a user;

accessing at least one record stored on the first device, the at least one record including authentication information associated with the user and credential information associated with the external resource to which the user has requested access, wherein the credential information comprises a cryptographic key;

receiving authentication input from the user;

determining that the authentication input from the user matches the authentication information associated with the user included in the at least one record stored on the first device;

retrieving at least a portion of the credential information from the at least one record stored on the first device;

facilitating access of the user to the external resource at least in part by transmitting, on behalf of the user, from the first device, output based at least in part on the at least portion of the credential information retrieved from the at least one record, wherein the user of the first device is granted access to the external resource based at least in part on the output transmitted from the first device on behalf of the user; and

initiating a backup, to a second device, of at least a portion of the at least one record.

19. (New) The system of claim 1, wherein the one or more processors are configured to access records associated with at least two different users.

20. (New) The system of claim 19, wherein the records associated with the at least two different users are stored on the first device.

21. (New) The method of claim 17, comprising accessing records associated with at least two different users.

22. (New) The method of claim 21, wherein the records associated with the at least two different users are stored on the first device.

AMENDMENTS TO THE DRAWINGS

The attached sheet of drawings, which includes Figures 1-15, replaces the original sheet including Figures 1-15.

Attachment: Replacement Sheet

REMARKS

New Claims 19-22 have been added. Claims 1-22 are pending. No new matter has been added.

New Claims

Support for new Claims 19-22 may be found, without limitation, in Paragraph [0085] of the Specification.

The foregoing amendments are not to be taken as an admission of unpatentability of any of the claims prior to the amendments.

Reconsideration of the application and allowance of all claims are respectfully requested based on the preceding remarks. If at any time the Examiner believes that an interview would be helpful, please contact the undersigned.

Respectfully submitted,

Dated: March 1, 2021

/Yeu-Ting George Cheng/
Yeu-Ting George Cheng
Registration No. 69408
408-207-4765

VAN PELT, YI & JAMES LLP
10050 N. Foothill Blvd., Suite 200
Cupertino, CA 95014
Fax 408-973-2595

DocCode – SCORE

SCORE Placeholder Sheet for IFW Content

Application Number: 17123018 Document Date: 03/01/2021

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

- Drawing

At the time of document entry (noted above):

- USPTO employees may access SCORE content via DAV or via the SCORE web page.
- External customers may access SCORE content via PAIR using the Supplemental Content tab.

Form Revision Date: March 1, 2019

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	17123018
Filing Date	2020-12-15
First Named Inventor	Bjorn Markus Jakobsson
Art Unit	1713
Examiner Name	Not Assigned
Attorney Docket Number	MJAKP026

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5010571		1991-04-23	KATZNELSON RON D	
	2	5499298		1996-03-12	NARASIMHALU ARCOT D	
	3	10872152		2020-12-22	MARTEL PIERRE OLIVIER	

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17123018
	Filing Date	2020-12-15
	First Named Inventor	Bjorn Markus Jakobsson
	Art Unit	1713
	Examiner Name	Not Assigned
	Attorney Docket Number	MJAKP026

If you wish to add additional Foreign Patent Document citation information please click the Add button			Add
NON-PATENT LITERATURE DOCUMENTS			Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		
If you wish to add additional non-patent literature document citation information please click the Add button			Add

EXAMINER SIGNATURE			
Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17123018
	Filing Date	2020-12-15
	First Named Inventor	Bjorn Markus Jakobsson
	Art Unit	1713
	Examiner Name	Not Assigned
	Attorney Docket Number	MJAKP026

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/Yeu-Ting George Cheng/	Date (YYYY-MM-DD)	2021-01-07
Name/Print	Yeu-Ting George Cheng	Registration Number	69408

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

Electronic Acknowledgement Receipt

EFS ID:	41585535
Application Number:	17123018
International Application Number:	
Confirmation Number:	1102
Title of Invention:	AUTHENTICATION TRANSLATION
First Named Inventor/Applicant Name:	Bjorn Markus Jakobsson
Customer Number:	21912
Filer:	Yeu-Ting George Cheng/Elaine Nguyen
Filer Authorized By:	Yeu-Ting George Cheng
Attorney Docket Number:	MJAKP026
Receipt Date:	07-JAN-2021
Filing Date:	15-DEC-2020
Time Stamp:	16:28:10
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	MJAKP026_IDS_02_SB08.pdf	1052875 8bd3ca64f3509b358a29497004c156c6e8692a5a	no	4

Warnings:

Information:	
Total Files Size (in bytes):	1052875

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
17/123,018	12/15/2020	1713	0.00	MJAKP026	18	3

CONFIRMATION NO. 1102

21912
VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

FILING RECEIPT



Date Mailed: 12/31/2020

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

Bjorn Markus Jakobsson, Portola Valley, CA;

Applicant(s)

RightQuestion, LLC, Portola Valley, CA

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CIP of 17/027,481 09/21/2020
which is a CON of 16/773,767 01/27/2020
which is a CON of 16/563,715 09/06/2019 PAT 10824696
which is a CON of 16/273,797 02/12/2019 PAT 10521568
which is a CON of 15/042,636 02/12/2016 PAT 10360351
which is a CON of 13/706,254 12/05/2012 PAT 9294452
which claims benefit of 61/587,387 01/17/2012
and claims benefit of 61/569,112 12/09/2011

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 12/30/2020
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 17/123,018**
Projected Publication Date: To Be Determined - pending completion of Missing Parts
Non-Publication Request: No
Early Publication Request: No
**** SMALL ENTITY ****
Title

AUTHENTICATION TRANSLATION

Preliminary Class

216

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative,

this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop

technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 17/123,018

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	80		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	350		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	400		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	18 minus 20 =	*	x 50 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*	x 240 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	830		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

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

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
17/123,018	12/15/2020	Bjorn Markus Jakobsson	MJAKP026

CONFIRMATION NO. 1102

21912
VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

FORMALITIES LETTER

OC000000122344335

Date Mailed: 12/31/2020

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 application is informal since it does not comply with the regulations for the reason(s) indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- Replacement drawings in compliance with 37 CFR 1.84 and 37 CFR 1.121(d) are required. The drawings submitted are not acceptable because:
  - More than one figure is present and one or more figure appears to be unnumbered or misnumbered in comparison to the brief description of the figures. See Figure(s) 14. The figures must be labeled "Fig." with a consecutive Arabic numeral (1, 2, etc.) or an Arabic numeral and capital letter in the English alphabet (A, B, etc.) and correspond with a brief description having the same figure number. See 37 CFR 1.84(u)(1).
    (1) To correct the figure numbering, replacement figures must be submitted.
    (2) To add a brief description of an unnumbered figure, or correct the reference in the specification to the figures, a proper substitute specification in compliance with 37 CFR 1.121(b)(3) and 1.125, providing a brief description of each drawing figure presented, added or amended to correspond to the corrected numbering of the figures, must be submitted. See also 37 CFR 1.77(b)(9).

Applicant is cautioned that correction of the above items may cause the specification and drawings page count to exceed 100 pages. If the specification and drawings exceed 100 pages, applicant will need to submit the required application size fee.

- The statutory basic filing fee is missing.

- The application search fee must be submitted.
- The application examination fee must be submitted.
- Surcharge as set forth in 37 CFR 1.16(f) must be submitted.
  The surcharge is due for any one of:
  - late submission of the basic filing fee, search fee, or examination fee,
  - late submission of inventor's oath or declaration,
  - filing an application that does not contain at least one claim on filing, or
  - submission of an application filed by reference to a previously filed application.

SUMMARY OF FEES DUE:

The fee(s) required within **TWO MONTHS** from the date of this Notice to avoid abandonment is/are itemized below. Small entity discount is in effect. If applicant is qualified for micro entity status, an acceptable Certification of Micro Entity Status must be submitted to establish micro entity status. (See 37 CFR 1.29 and forms PTO/SB/15A and 15B.)

- $ **80** basic filing fee.
- $ **80** surcharge.
- $ **350** search fee.
- $ **400** examination fee.
- $(**0**) previous unapplied payment amount.
- $ **910** TOTAL FEE BALANCE DUE.

Items Required To Avoid Processing Delays:

Applicant is notified that the above-identified application contains the deficiencies noted below. No period for reply is set forth in this notice for correction of these deficiencies. However, if a deficiency relates to the inventor's oath or declaration, the applicant must file an oath or declaration in compliance with 37 CFR 1.63, or a substitute statement in compliance with 37 CFR 1.64, executed by or with respect to each actual inventor no later than the expiration of the time period set in the "Notice of Allowability" to avoid abandonment. See 37 CFR 1.53(f).

- A properly executed inventor's oath or declaration has not been received for the following inventor(s):
  Bjorn Markus Jakobsson

Replies must be received in the USPTO within the set time period or must include a proper Certificate of Mailing or Transmission under 37 CFR 1.8 with a mailing or transmission date within the set time period. For more information and a suggested format, see Form PTO/SB/92 and MPEP 512.

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, including a copy of this Notice and selecting the document description "Applicant response to Pre-Exam Formalities Notice". 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.

Questions about the contents of this notice and the
requirements it sets forth should be directed to the Office

of Data Management, Application Assistance Unit, at
(571) 272-4000 or **(571) 272-4200** or **1-888-786-0101**.

/tgebre/

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	17123018
Filing Date	2020-12-15
First Named Inventor	Bjorn Markus Jakobsson
Art Unit	N/A
Examiner Name	N/A
Attorney Docket Number	MJAKP026

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6016476		2000-01-18	MAES STEPHANE HERMAN	
	2	6691232		2004-02-10	WOOD DAVID L	
	3	7512965		2009-03-31	AMDUR EUGENE	
	4	7697729		2010-04-13	HOWELL MARK J	
	5	7950051		2011-05-24	SPITZ SEAN T	
	6	8145916		2012-03-27	BOSHRA MICHAEL	
	7	8549300		2013-10-01	KUMAR KARTIK	
	8	8577813		2013-11-05	WEISS KENNETH P	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17123018
	Filing Date	2020-12-15
	First Named Inventor	Bjorn Markus Jakobsson
	Art Unit	N/A
	Examiner Name	N/A
	Attorney Docket Number	MJAKP026

	9	8856539		2014-10-07	WEISS KENNETH	
	10	8984596		2015-03-17	GRIFFIN STEPHANIE	
	11	9100826		2015-08-04	WEISS KENNETH P	

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20040107170		2004-06-03	LABROU YANNIS	
	2	20040236632		2004-11-25	MARITZEN MICHAEL L	
	3	20050198348		2005-09-08	YEATES ANTHONY J	
	4	20090100269		2009-04-16	NACCACHE DAVID	
	5	20100242102		2010-09-23	CROSS DAVID B	
	6	20110078771		2011-03-31	GRIFFIN STEPHANIE	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17123018
	Filing Date	2020-12-15
	First Named Inventor	Bjorn Markus Jakobsson
	Art Unit	N/A
	Examiner Name	N/A
	Attorney Docket Number	MJAKP026

	7	20110205016		2011-08-25	AL-AZEM SAMER	
	8	20110231651		2011-09-22	BOLLAY BENN SAPIN	
	9	20120110341		2012-05-03	BEIGI HOMAYOON	
	10	20120167193		2012-06-28	GARGARO GIANLUCA	

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2004051585	WO		2004-06-17	JAKOBSSON MARKUS		
	2	2005001751	WO		2005-01-06	REGENTS OF THE UNIVERSITY OF CALIFORNIA		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	"Managing Authorization and Access Control", Author: unknown, Published November 3, 2005, pp. 1-12, URL: http://technet.microsoft.com/en-us/library/bb457115.aspx	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17123018
	Filing Date	2020-12-15
	First Named Inventor	Bjorn Markus Jakobsson
	Art Unit	N/A
	Examiner Name	N/A
	Attorney Docket Number	MJAKP026

	2	BRANDS ET AL. Distance-Bounding Protocols. January 28, 1994: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.51.6437&rep=rep1&type=pdf	
	3	Hammer-Lahav, Ed. "The OAuth 1.0 Protocol", from https://tools.ietf.org/html/rfc5849, April 2010.	
	4	JAKOBSSON ET AL. Proving Without Knowing: On Oblivious, Agnostic and Blindfolded Provers. July 24, 1996: http://markus-jakobsson.com/papers/jakobsson-crypto96.pdf	
	5	MONROSE ET AL. Using Voice to Generate Cryptographic Keys. May 13, 2001: https://www.cs.unc.edu/~fabian/papers/odyssey.pdf	
	6	SESHADRI ET AL. Pioneer: Verifying Code Integrity and Enforcing Untampered Code Execution on Legacy Systems. October 23, 2005: https://netsec.ethz.ch/publications/papers/pioneer.pdf	

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17123018
	Filing Date	2020-12-15
	First Named Inventor	Bjorn Markus Jakobsson
	Art Unit	N/A
	Examiner Name	N/A
	Attorney Docket Number	MJAKP026

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/Yeu-Ting George Cheng/	Date (YYYY-MM-DD)	2020-12-16
Name/Print	Yeu-Ting George Cheng	Registration Number	69408

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 June 2004 (17.06.2004)

PCT

(10) International Publication Number
WO 2004/051585 A2

(51) International Patent Classification[7]: G07F 7/10

(21) International Application Number:
PCT/US2003/037928

(22) International Filing Date:
26 November 2003 (26.11.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/429,754 27 November 2002 (27.11.2002) US

(71) Applicant: **RSA SECURITY INC** [US/US]; 174 Middlesex Turnpike, Bedford, MA 01730 (US).

(72) Inventors: **JAKOBSSON, Markus**; 1203 Garden Street, Hoboken, NJ 07030 (US). **JUELS, Ari**; 131 Freeman Street, Brookline, MA 02446 (US). **KALISKI, Burton, S., Jr.**; 22 Pembroke Road, Wellesley, MA 02181 (US).

(74) Agent: **PRAHL, Eric, L.**; Hale and Dorr LLP, 60 State Street, Boston, MA 02109 (US).

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

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

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

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

(54) Title: IDENTITY AUTHENTICATION SYSTEM AND METHOD

(57) Abstract: A method and system for generating an authentication code that depends at least in part on a dynamic value that changes over time, an event state associated with the occurrence of an event, and a secret associated with an authentication device. By generating the authentication code responsive to an event state, an identity authentication code can be used to verify identity and to communicate event state information, and to do so in a secure manner.

WO 2004/051585 A2

IDENTITY AUTHENTICATION SYSTEM AND METHOD

Cross Reference to Related Applications

[0001] This application claims the benefit under 35 U.S.C. § 119(e) of U.S. Provisional Application No. 60/429,754, filed November 27, 2002.

Field of the Invention

[0002] The invention relates generally to the fields of cryptography and security. More specifically, the invention relates to the generation and verification of identity authentication codes.

Background of the Invention

[0003] Generally, security systems employ identity-based authentication schemes to verify the identity of an entity that is allowed access to a physical location or object, in the case of a physical security system, or electronic access to a computer system or data, in the case of a data security system. One goal of such security systems is to accurately determine identity so that an unauthorized party cannot gain access. Security systems can use one or more of several factors, alone or in combination, to authenticate entities. For example, identification systems can be based on something that the entity knows, something the entity is, or something that the entity has.

[0004] Examples of something an entity knows are a code word, password, personal identification number ("PIN") and the like. One exemplary computer-based authentication method involves the communication of a secret that is specific to a particular entity or user. The entity seeking authentication transmits the secret or a value derived from the secret to a verifier, which authenticates the identity of the entity. In a typical implementation, an entity

communicates both identifying information (e.g., a user name) and a secret (e.g., a password) to the verifier. The verifier typically possesses records that associate a secret with each entity. If the verifier receives the appropriate secret for the entity, the entity is successfully authenticated. If the verifier does receive the correct secret, the authentication fails.

[0005] Examples of something the entity is include characteristics that are unique to people, such as physical, biological, and psychological characteristics (referred to generally here as biological characteristics), such as fingerprints, handwriting, eye retina patterns, and face, body, and organ appearance, size and shape. Suitable biological characteristics typically are not under the control of the person, and are therefore difficult for anyone besides the intended person to present, because, in part, they are difficult to replicate. The verifier typically can observe the characteristic, and compare the characteristic to records that associate the characteristic with the entity. The observation of biological characteristics is referred to generally as biometric measurement.

[0006] An example of something an entity possesses is a physical or digital object, referred to generally as a token, that is unique, or relatively unique, to the user. A simple example is a conventional metal key for use in a door. Possession of the door key in effect authenticates the user to the lock and allows entry. Similarly, possession of a token such as a bank card having certain specific physical and electronic characteristics, for example containing a specific identification number that is revealed when the token is accessed in a particular manner, can be this type of factor. A token containing a computing device that performs encryption using an encryption key contained in the device would also be regarded as this type of factor. For example, a token could accept user input, which might include a PIN or a challenge value, and provide as output a result encrypted with a secret encryption key stored in the card. The verifier can then compare the output to an expected value in order to authenticate the entity.

[0007] A token might also, or alternatively, use additional input information, such as time, or a counter, for example, such that the result changes over time but is deterministic to an entity that possesses a secret (e.g., a value known only by the token and the verifier), but not predictable by an observer who does not possess the secret. These systems generally perform some computation using a stored secret as input to generate an authentication code that is used to authenticate the entity. Some systems are time-based, in that they use a time-based dynamic variable to calculate a non-predictable authentication code that ultimately authenticates the entity. Here, "non-predictable" means that the authentication code is not predictable by a party that does not know the associated secret, the algorithm for calculating the code, or both. One example, U.S. Patent No. 5,937,068 entitled "System and Method for User Authentication Employing Dynamic Encryption Variables," uses as input a combination or subset of three variables: the current time, the number of access requests made by the card, and a "secret dynamic encryption key" that is updated with each access request. The token, in this case, also verifies a PIN entered by the user before communicating an authentication code.

[0008] Although the dynamic nature of the authentication codes generated by such an approach avoids problems inherent with using fixed authentication codes, an unattended or stolen token remains vulnerable to attack. Would-be attackers who gain access to tokens can subject the tokens to sophisticated analysis intended to determine their methods of operation, and/or the secret(s) stored within. Attackers might inspect the token and conduct such analysis in order to determine the associated secret, the algorithm for calculating the authentication code, or both. The attacker might then be able to generate apparently valid authentication codes in order to illegally gain physical or electronic access to secured areas or systems. Many tamper-resistant hardware designs are available, however, new attacks are frequently developed to thwart tamper resistance. Further, current tamper resistant designs do not provide verifiers,

authentication systems, system administrators, or another relevant authority with any indication that the token has been tampered with.

[0009] One approach to detection of tampering is described in Johan Håstad, Jakob Jonsson, Ari Juels, Moti Yung, "funkspiel schemes: an alternative to conventional tamper resistance", ACM Conference on Computer and Communications Security 2000; 125-133. Håstad et al. describe several "funkspiel schemes" whereby a device can indicate to a verifier that tampering has occurred, without revealing to an adversary whether the tampering has been detected. The schemes are oriented toward the generation of a sequence of message authentication codes, where the message authentication may fail after tampering has been detected. In one example given, the message authentication code is embedded into a digital signature scheme, where the digital signature indicates whether a transaction has been approved by a device, while the message authentication code indicates whether the device has been tampered with. The message authentication code itself may not be suitable as an identity authentication code as it is oriented toward a sequence of message transactions rather than time-based identity authentication. In particular, Håstad et al does not provide any method for efficiently verifying a single authentication code among those over a very long period of time, without substantial computation by the verifier (e.g., a potentially long chain of function evaluations), substantial computation by both parties (e.g., asymmetric encryption) or substantial storage by both parties (e.g., many one-time bits).

Summary of the Invention

[0010] The invention addresses these shortcomings by including an indication of the occurrence of an event directly into the efficient computation of an identity authentication code, where the verifier may efficiently verify the authentication code and identify the signaling of an event state.

[0011] While the previous approaches do not have the flexibility to communicate event information in, or as part of, an authentication code, in the present approach, an authentication code is generated in a manner that communicates to the verifier information about the occurrence of one or more reportable events. A reportable event is an event other than events associated with the normal operation of an authentication method (and that can be reported to the verifier). Thus, for example, a reportable event would not include an event reporting a request for an authentication code. A reportable event could be, on the other hand, an event that is at least one of an anomalous, extraordinary, remarkable, unusual, and the like. A reportable event also could be any sort of event that can be detected and/or communicated by or to the device. Example reportable events include: device tampering; an event external to the device detected by the device; an environmental event, such as temperature exceeding or falling below a threshold; static discharge; high or low battery power; geographic presence at a particular location; confidence level in a biometric reading; and so on. A reportable event may also provide an indication of the likelihood that the security of the authentication system has been compromised or the likelihood that the authentication device has or will develop an operational problem (e.g., the condition of the authentication device). A reportable event can be the cumulative effect of multiple past events. A reportable event also can be the device operational status.

[0012] A reportable event may include information concerning the condition of the authentication device (e.g., tampering, low battery power, etc.), the security of the authentication system (e.g., strength of a user's biometric information, accuracy of a PIN entry, verification of an authentication device signature), the status of the user (e.g., mobile or stationary, network access location, location in a facility, etc.), the location of the device (e.g., region, country, city, etc.) or the environment where the device is located (e.g., temperature, radiation level, etc.). In one embodiment, the reportable event directly reports information concerning at least one of the condition of the authentication device, the security of the authentication system, the status of the

user, the location of the authentication device, and the environment where the authentication device is located.

[0013] In general, in certain aspects of the invention, a user or a device on behalf of the user, algorithmically computes an authentication code based on both a dynamic variable (e.g., that changes over time) and a secret associated with the user or the device. The generated authentication code is non-predictable to an observer, but is verifiable by a verifier. The authentication code can also depend, in part, on any other information, for example, on one or more of a PIN, a password, and data derived from a biometric observation, or information associated with the user, the authentication device, or the verifier.

[0014] The security of an authentication system is improved when a device takes specific action upon the occurrence of a reportable event. In one illustrative example, if an attacker attempts to disassemble or otherwise tamper with a device, it is useful for the device to signal the occurrence of such event (once detected by the device) to a verifier by communicating the device's event state. In this example, the tampering event has at least two possible event states; yes – tampering occurred, and no – tampering has not occurred. Other information also can be communicated, such as information about the type of tampering or information about the time that the tampering occurred. Other examples of reportable events include environmental events (e.g., high or low temperature), battery voltage level, and accuracy of PIN or password entry.

[0015] In one embodiment, the occurrence of an event is communicated explicitly in the authentication code. For example, one or more bits included in the authentication code can be dedicated to reporting the occurrence of an event, i.e., reporting the event state (and herein we refer to event state data as data representing, communicating, or derived from the event state) where the event state is information about the state of a device with respect to the occurrence or non-occurrence of event(s). In another embodiment, the device's event state can be communicated implicitly, such that only the device and the verifier can feasibly determine the

event state from the communication. It may be advantageous if an attacker with access to device is unable to determine if an event was detected and communicated because an unwarned attacker is more likely to take actions that can lead to observation and apprehension by authorities. In some embodiments, the device operates differently upon occurrence of an event, such that the occurrence of the event is communicated in identity authentication codes output by the device subsequent to the occurrence of the reportable event. This may help discourage copying. For example, when a device that is providing an alert of an anomalous event is copied, the "clone," or copied device will also report the anomalous event.

[0016] In one embodiment, authentication methods can be incorporated in a hardware device provided to the user, such as a token or a key fob. (Other possibilities are described below.) Additionally, a device can include a software program for carrying out the method, for example, as software executing on a general-purpose computer, handheld computer, telephone, personal digital assistant, and so on, or in some other manner. The device may, in some implementations, allow the user to input a second secret, such as a PIN, verifier identifier, and so on, in order to generate an authentication code.

[0017] In general, in one aspect, the invention relates to an authentication device that generates an identity authentication code by storing an event state in the device, modifying the event state in response to an event, and generating an authentication code that depends, at least in part, on a dynamic value (e.g. a time value), the event state, and a secret associated with the device. The authentication device thus produces a different identity authentication code based on the event state. By comparing a received authentication code to the possible authentication codes that could be generated by the authentication device, the verifier can not only verify the identity of the user, but can also determine the event state, and thereby determine whether one or more events occurred.

[0018] In some embodiments, the event state is associated with one or more reportable events. In some embodiments, the event state is modified in response to a reportable event. In some such embodiments, the event state is stored in the form of event state data, which reflects the state of one or more reportable events. The event state data thus can communicate the event state.

[0019] In some embodiments, the method is constructed such that it is not possible for an attacker who has access to the device to determine whether the report of an event was communicated in the authentication code. As briefly described above, the communication of the event information can be referred to as "covert." On the other hand, if some event information can be deduced by an attacker or observer, then the communication is referred to as "overt." Covert communication may be beneficial because it can be used to report the occurrence of an event without an attacker becoming aware of the report. Overt communication may be beneficial in that it allows a general observer to become informed about state information. It is possible to signal some part of an event state in a covert manner, and another part in an overt manner.

[0020] An implementation of a system for generating an identity authentication code using event state information can include a data store for storing an event state in an authentication device, an event recorder for modifying the event state in response to one or more reportable events, and an authentication code generator for generating an identity authentication code that depends at least in part on a dynamic value, the event state, and a secret associated with the device. Such an implementation can be included as either part of an authentication device (e.g., a token) or part of a verifier (e.g., a verification computer), or both. For both the device and the verifier, the system can be implemented as software running on a computer, such as a microprocessor or other general purpose computer. The system can also be implemented in hardware, as described above.

[0021] In general, in another aspect, the verifier receives authentication information that includes an identity authentication code generated by a device that at least in part depends on time, a secret associated with the device, and an event state. The verifier verifies the identity of the user and determines the event state in response to the received identity authentication code. The verifier can determine whether an event occurred from the event state. The verifier can take action in response to the determined event state, for example, logging the event state for later analysis, warning the system administrator or relevant authorities, or providing more limited access to the location or system than would be granted if a different event state was determined. The authentication information can also include one or more of a user identifier, a PIN, password, a biometric reading, and other additional authentication information.

[0022] In some embodiments, the verifier generates an expected identity authentication code that depends at least in part on a dynamic value associated with a time period and the event state. The event state can include an event state secret, described further below, and bits derived from the event state secret, where one or more bits are associated with a time interval.

[0023] In general, in another aspect, the invention relates to a system and method for generating an identity authentication code by, for example, an authentication device and/or a verifier. Describing first the device, the device stores a first secret value associated with the authentication device, and a second secret value associated with event state. The device also generates a dynamic value that changes over time. The device derives from the second value and the dynamic value event state data associated with a time period. The device derives a value for a time period from the first value and the event state data. The device then calculates an identity authentication code using the time-specific value as input. The verifier likewise can implement these method steps so as to determine one or more possible authentication codes, depending on the event state data.

[0024] In one embodiment, the event state data includes bits each associated with a time period, where the time-specific value is derived from the first value and the respective bit associated with the time period. In such an embodiment, there are two possible states associated with a time period, depending on the value of the bit. If an event occurs, the bits are modified in response to the detected event, such that the generated authentication code is the other of the two possible choices. Optionally, the second secret value (associated with the event state) can also be modified in response to the detected event, such that later generations of event state bits will have a different value than normal. The first secret value can be the same as the second secret value, or they can be different values, or they can partially overlap.

[0025] In one embodiment, the event state data comprises a number of bits associated with a respective time period, wherein the time-specific value is derived from the first value and the number of bits associated with the respective time period.

[0026] In general, in another aspect, a system for generating an identity authentication code associated with an authentication device includes an authentication code generator. The authentication code generator generates an identity authentication code that depends at least in part on a dynamic value that changes over time, an event state indicative of the occurrence of an event, and a secret associated with the authentication device. One embodiment of such a system is implemented as a software program for execution on a processor, such as a microprocessor or general purpose computer. The system can be included in an authentication device or a verifier, or in another system.

[0027] The foregoing and other objects, aspects, features, and advantages of the invention will become more apparent from the following description and from the claims.

Brief Description of the Drawings

[0028] In the drawings, like reference characters generally refer to the same parts throughout the different views. Also, the drawings are not necessarily to scale, emphasis instead generally being placed upon illustrating the principles of the invention.

[0029] FIG. 1 is a block diagram depicting an authentication system including an authentication device and a verifier according to an embodiment of the invention.

[0030] FIG. 2 is a block diagram depicting the generation of an authentication code according to an embodiment of the invention.

[0031] FIG. 3 is a block diagram depicting the generation of an authentication code according to an embodiment of the invention.

[0032] FIG. 4 is a block diagram depicting a detailed implementation of the embodiment of FIG. 3.

[0033] FIG. 5 is an example demonstrating the use of event state data in generating an authentication code.

[0034] FIG. 6 is a flowchart depicting an embodiment of a method for generating an authentication code.

[0035] FIG. 7 is a block diagram depicting the generation of an authentication code according to an embodiment of the invention.

[0036] FIG. 8 is a block diagram depicting the generation of an authentication code according to an embodiment of the invention.

Detailed Description

[0037] Referring to FIG. 1, in one embodiment of an authentication system 100 according to the invention, a verifier 105, is used to help securely authenticate the identity of exemplary user 110. As used here, "authenticate" means to verify the identity of a user, and so "authenticate" and "verify" can be used interchangeably throughout. Also, although the specification will

discuss, for simplicity, authentication of "users," it should be understood that "users" means any entity requiring authentication such as, for example, a person, animal, device, machine, or computer. The inclusion of a single user 110 is exemplary, and typically a verifier 105 will be used to verify a large number of users 110. Similarly, the inclusion of a single verifier 105 is exemplary, and typically a user 110 can have an authentication attempt verified by one or more of a large number of verifiers 105. In some embodiments, a single verifier 105 is able to verify a user 110, while in other embodiments, two or more verifiers 105 are together required to perform this task.

[0038] The verifier 105 can be any sort of device that implements the functions described here. In one embodiment, the verifier 105 is implemented as software running on a server class computer including a processor, memory, and so on, to enable authentication of a large number of users, for example, in an enterprise. The verifier 105 can also be implemented as software running on a desktop computer, laptop computer, special-purpose device, or personal digital assistant (PDA). For example, the verifier 105 can be implemented as a software program running on a general-purpose computer, possibly interacting with one or more other computer programs on the same or a different computer. Some or all of the verifier 105 functionality can be implemented in hardware, for example in an Application Specific Integrated Circuit (ASIC) and the like. In still further embodiments, the verifier 105 can be implemented in a cellular telephone, or specialized hardware embedded in a cellular telephone and adapted to interact with the cellular telephone's circuitry. Other sizes, shapes, and implementations are possible without departing from the spirit of the invention.

[0039] Authentication can result in the performance of one or more actions including, without limitation, providing access or privileges, taking action, or enabling some combination of the two. Access includes, without limitation: access to a physical location, communications network, computer system, and so on; access to such services as financial services and records,

health services and records and so on; or access to levels of information or services. The user 110 and the verifier 105 can be physically near one another or far apart.

[0040] As illustrated, a user 110 can communicate with a user authentication device 120. The user authentication device 120 provides information used to authenticate the user 110. The user authentication device 120 can optionally provide a user interface 130. Communication between the user 110 and the user authentication device 120 can take place via this user interface 130. The user interface 130 can provide an input interface, an output interface, or both. An input interface enables the user 110 to communicate information to the user authentication device 120. The input interface can be any mechanism for receiving user input, and can include, without limitation: a keypad or keyboard; one or more push buttons, switches or knobs; a touch sensitive screen; a pointing or pressing device; a trackball; a device for capturing sound, voice or handwriting; a device for capturing biometric input (such as a fingerprint, retina or voice characteristic); and so forth. An output interface enables the user authentication device 120 to communicate information to the user 110 and can be any mechanism for communicating to a user, including, without limitation: a visual display to support alphanumeric characters or graphics such as a LCD display or LED display; an electrophoretic display; one or more light sources; a loudspeaker, a sound or voice generator; a vibration interface; and so forth. In some embodiments, the user 110 provides, via the user interface 130, identifying information (such as a user identifier, PIN, or password, or a biometric characteristic such as a fingerprint, retina pattern, or voice sample), or possessions (such as physical keys, digital encryption keys, digital certificates, or authentication tokens) to the user authentication device 120.

[0041] The user authentication device 120 can take various forms in various embodiments of the invention, provided that the user authentication device 120 performs the functions required of the user authentication device 120 for secure authentication. The user authentication device 120 can be implemented in packages having a wide variety of shapes and form factors. For example,

the user authentication device 120 can be a credit-card sized and shaped device, or can be much smaller or much larger. One credit-card sized embodiment of the user authentication device 120 includes a microprocessor with on-board memory, a power source, and a small LCD display. The embodiment optionally includes a keypad or buttons for PIN entry, entry of authentication information requests, or for other entry or interaction with the device 120. In another embodiment, a credit-card sized device 120 includes a processor with on-board memory that is used as a "smart card," that can be installed into another device that provides power and/or interface. In still other embodiments, a credit-card sized device 120 is a card such as a credit card including a magnetic strip or other data store on one of its sides. In other embodiments, the user authentication device 120 is a "key fob," that is, a smaller device with a display and battery that is sized and shaped to fit on a key ring. In yet another embodiment, the user authentication device 120 is a peripheral device that communicates with a computer, telephone, or other device, such as a USB dongle. In still other embodiments, the user authentication device 120 can be a desktop computer, laptop computer, or personal digital assistant (PDA). For example, the authentication device 120 can be implemented as a software program running on a general-purpose computer, possibly interacting with one or more other computer programs on the same or a different computer. In still further embodiments the user authentication device can be a cellular telephone, or specialized hardware embedded in a cellular telephone and adapted to interact with the cellular telephone's circuitry, such as a SIM card. In this example and in others, the authentication device 120 can include two components in communication with each other, for example a wireless communications device (e.g., mobile telephone) and a removable accessory, such as a SIM card. Other sizes, shapes, and implementations are possible without departing from the spirit of the invention.

[0042] Exemplary authentication devices with which the embodiments of the invention can be used are members of the RSA SECURID family of authentication tokens, available from RSA

Security Inc. of Bedford, MA. Some RSA SECURID hardware devices, for example, display a generated authentication code to a user, who then communicates the displayed authentication code to a computer for communication to a verifier. For example, in one embodiment, the information is a numerical value.

[0043] In some embodiments, the user authentication device 120 stores a secret that is used to authenticate the user 110. Typically, the stored secret is information that only is available to the authentication device and the verifier. For example, in one embodiment, the information is a numerical value. The stored secret is used to generate an authentication code for the user 110. The user authentication device 120 also can store or access dynamic data, which, for example, can be the current time, if implemented with a running clock. The user authentication device 120 can also provide other information, or perform other calculations or combination functions, as described further below. For example, in one embodiment, in addition to storing a secret the device 120 receives a personally selected secret from the user 110 (such as a PIN or password) and generates a dynamic, non-predictable authentication code in response to the secret received from the user 110, the stored secret, and the current time. Here, for example, a non-predictable authentication code is not predictable to anyone who does not have access to the secret received from the user 110, the stored secret, and the algorithm that generates the authentication code. The user authentication device 120 optionally can also receive other input, such as a verifier identification, and use that and/or other additional information in the generation of the authentication code.

[0044] The exemplary user 110 optionally (and depending on implementation) has one or both of direct access to the communications terminal 140, and indirect access to the communications terminal 140 via the user authentication device 120. The communications terminal 140 can take various forms in various embodiments, including without limitation: a card reader; a device receptacle, cradle, or holder; a personal computer; a telephone; a personal digital

assistant (PDA); a network interface card; a wireless transceiver; and so on. During the authentication process the user 110 can directly communicate information to only the device 120, only the terminal 140, neither the device 120 nor the terminal 140, or both the device 120 and the terminal 140. Likewise, the communications terminal 140 can receive direct input from the user 110, the user authentication device 120, or both. As shown, the user 110 optionally communicates directly with the communications terminal via the terminal user interface 145 that can be present depending on the implementation of the communications terminal 140. Like the device user interface 130, the terminal user interface 145 can include an input interface, an output interface, or both. The input and the output interfaces can take one or more of the forms described above for the device user interface 130, or other forms.

[0045] The communications terminal 130 can optionally provide a device/terminal interface 160 for communications between the terminal 140 and the user authentication device 120. In one embodiment, this interface can take the form of a wired or wireless communications channel between the terminal 140 and the device 120, using standard or proprietary protocols. For example, in an embodiment in which the device 120 is a smart card and the terminal 140 includes a card reader, the communications interface 160 could be a wired serial communications link between the smart card and the reader. In another embodiment in which the device 120 is a token that has wireless communications capability and the terminal 140 includes a wireless transceiver, the interface 160 could be a wireless link.

[0046] The communications terminal 140 can provide a user interface 130, via a terminal interface 145, without providing a device interface 160 for the device 120. For example, the terminal 140 can be a telephone that the user 110 uses to communicate authentication information to the verifier 105. In such an embodiment the user authentication information can be represented as tones associated with a series of alphanumeric digits. In this embodiment the user 110 dials a telephone number to establish a communications connection with the verifier

105 and performs a series of key presses on the telephone to communicate the alphanumeric user authentication information to the verifier 105.

[0047] The terminal 140 and the authentication device 120 can each be integrated, together or separately, into another device, likewise, the functionality of the terminal 140, the device 120; and their respective interfaces 130, 145, 160 can be implemented in separable components. For example, the authentication device 120 can be implemented as an add-in card to a handheld computer (not shown). The handheld computer provides the user interface 130, and also provides the terminal 140 in the form of a wireless network interface. Likewise, a mobile telephone can provide terminal 140 and user interface 130 functions, while the mobile telephone, or a plug-in component such as a SIM card, provides some or all the authentication device 120 function.

[0048] The communications terminal 140 communicates information to the verifier 105 via a communications channel 170. The communications channel 170 can be any method and/or interface that enables communication of information to the verifier 105 that is required to authenticate the identity of the user 110. The communications terminal 140 can communicate information generated by the user 110, the device 120, or both, to the verifier 105 over a communications channel 170. The communications terminal 140 and the verifier 105 can implement the communication channel 170 through a variety of connections including standard telephone lines, LAN or WAN links (e.g., 802.11, T1, T3, 56kb, X.25), broadband connections (ISDN, Frame Relay, ATM), and wireless connections. Connections between the communications terminal 140 and verifier 105 can be established using a variety of communication protocols (e.g., TCP/IP, IPX, SPX, NetBIOS, Ethernet, RS232, and direct asynchronous connections). The verifier 105 processes the information received from the communications terminal 140. The verifier 105 can perform actions in response to

authenticating the identity of the user 110. For example, the verifier 105 can grant on-line access to data or physical access to restricted areas or physical items.

[0049] The authentication code communicated over the communications channel 170 is designed to be dynamic and unpredictable (to an observer without knowledge of the algorithm and/or the secret used to generate the authentication code and/or access to previous user authentication attempts) for each user authentication attempt. In some embodiments, the algorithm is selected such that the authentication code is non-predictable even if the algorithm is known to the attacker. Also, the algorithm may be selected such that knowledge of a large set of previous authentication attempts for a multiplicity of users would not make an authentication code predictable to an attacker. The authentication code can also communicate event state information, as described further below.

[0050] For each user authentication attempt, the verifier 105 receives user authentication information and verifies the received information. As described further below, in some embodiments, the verifier also determines an event state indicating whether one or more events has occurred, and optionally, in some cases, the nature of an event. In some embodiments, in order to authenticate the user, the verifier 105 performs algorithmic calculations for each user authentication attempt that is substantially identical to the algorithmic calculation performed by the user authentication device 120. In some embodiments, the verifier can determine authentication codes for a number of possible events and event states such that a number of authentication codes that can successfully authenticate the user 110 are possible. The verifier 105 compares the authentication information received over communications channel 170 and the authentication information generated by the verifier 105 to determine whether any match. If there is a match, then the verifier 105 can authenticate the identity of the user 110 depending on the event state determined. In one embodiment, when the received and generated user information do not match, the user authentication attempt fails. In some embodiments, the

verifier can communicate positive or negative acknowledgement to the communications terminal 140 via the communications channel 170, and the terminal 140 may or may not communicate the acknowledgement to the device 120 or directly to the user 110. In further embodiments, where a plurality of authentication codes that can successfully verify the user 110 are possible, the verifier 105 first determines an expected authentication code for an expected event state, and if the verifier receives a different authentication code, determines and compares authentication codes for other possible event states before indicating whether the authentication device has been successfully verified. Note that there can be other possible authentication codes as well, for example due to a generation value increment (described further below) and imprecisely synchronized time clocks between the verifier 105 and the authentication device 120.

[0051] In one embodiment, a determination by a verifier of event occurrence triggers a restriction on the activities of a user 110, rather than a complete denial of access. The restriction can be based on the type of events that have occurred since the preceding authentication attempt. For example, a workstation user's access to highly confidential information can be eliminated while access to non-confidential information continues to be permitted when the user's PIN was entered into the authentication token incorrectly more than a specified number of times.

[0052] The user authentication device 120 can maintain event state data which indicates whether an event has occurred. The reportable event(s) about which the event state is maintained may be unusual events that do not occur during normal operation of the device. Examples of such anomalous events include tampering with the device, an environmental event (e.g. aberrant temperature), incorrect power supply, radiation detection, and so on. Other examples of reportable events can include, without limitation, device location (e.g., is the device in a specific building, room, city, country, region, or some combination); the length of time a device (e.g., if a card, token, etc.) is inserted in a reader (possibly indicating that a user left an unattended device in the reader); authentication quality (e.g., a number of PIN errors prior to successful

authentication, strength of a biometric match, etc.); device signature or pattern (e.g., the device generates a pattern or sequence of bits that can be checked by the verifier, and the event state indicates the current bit in this pattern); related authentication (e.g., the verifier can determine whether access to network resources is being requested from a physical location that the requestor entered in an authorized manner); and location of the stored secret, (e.g., event state indicates whether a stored secret is in an approved hardware device (e.g., a card, token, etc.) or has been transferred (e.g., downloaded to a software container such as a laptop)). The size of the event state data can depend on the number of possible event states. For example, for two event states, only one bit is needed. For seven states, three bits, and so on. Thus, taking geographic location as an example, three bits can be used to indicate one of seven possible locations, or a much larger number of bits can be used to indicate longitude/latitude.

[0053] An event occurrence results in a change in the event state kept by the user authentication device 120, with the further result that the authentication code generated by the user authentication device 120, with high probability, will be different than otherwise expected by the verifier 105. The verifier 105 can determine whether a received identity authentication code is associated with one or more events, and if it is, take appropriate action, such as a warning to an administrator, restricted access, and so on.

[0054] The event state need not have a specific meaning to the verifier. For efficiency, the verifier can determine which event state(s) are most likely and initially check authentications with the authentication codes associated with the most likely event state(s). The verifier can verify authentication codes with the most likely event state information to determine whether the event state that is being signaled is either valid (e.g., expected) or invalid (e.g., unexpected). Additionally, the interpretation of the event state can be accomplished outside of the verification process. In one embodiment, the event state information is analyzed and interpreted by an entity who is not a verifier in order to determine what event the event state is signaling, e.g., tampering,

low battery, etc. The verifier can communicate the event state information to a service that can interpret the event state.

[0055] When the verifier checks authentication codes for their correspondence with likely individual event states, the efficiency of the verifier's operation may depend on the number of likely event states. For example, if there are only two likely event states, then the verifier may only perform, at most, two checking operations, whereas if there are ten likely event states, the verifier may perform as many as ten checking operations. The verifier may be able to accommodate a significant number of event states in this manner. However, in some embodiments, the verifier can accommodate an increased number of event states because the authentication code may provide a hint to the verifier about the event state. In other embodiments, the event state may be provided in a way that can otherwise be recovered from the authentication code without checking all likely individual event states. In such embodiments, the efficiency of the verifier's operation may not depend on the number of such event states.

[0056] Since each likely event state may correspond to a different authentication code, the probability that a random authentication code is accepted by the verifier may increase as the number of likely event states increases, particularly if the length of the authentication code is fixed. Accordingly, it may be prudent to increase the length of an authentication code as the number of likely event states increases in order to keep the probability that a random authentication code is accepted sufficiently small. For example, if there are ten likely event states, then the length of the authentication code may be increased by one numeric digit.

[0057] As a simple example that does not have as many security benefits as the embodiments described later, in one embodiment, the user authentication device 120 maintains an event state data store. In this example, prior to the occurrence of an event, the event state data store equals zero. The contents of the event data store are combined with (e.g., added to) a first authentication code produced by the device 120 to form a second authentication code that is

communicated to the verifier. Initially, the event state does not result in any change to the authentication code. Upon the occurrence of a specific event, the event state data store is modified to be one hundred. Specifically, in one embodiment, the authentication device 120 includes a switch activated by the opening of the case of the authentication device 120, such that if the device 120 is opened, the switch causes an interrupt, which causes the processor in the authentication device 120 to change the contents of the event data store to one hundred. When the second authentication code is the result of adding the contents of the event data store to the first authentication code, authentication codes generated thereafter will differ from the expected authentication code by exactly one hundred. The verifier will immediately recognize that a received authentication code (i.e., the second authentication code) is not the initially expected authentication code. The verifier will also recognize that the received authentication code is different than expected by a value of one hundred. The verifier will then conclude that the event that triggers the change in event state data (in this case, opening of the authentication device) has occurred. In further embodiments, different events may change the authentication code differently (e.g., add one, ten, etc.). In these embodiments, different events may be recognized depending on the resulting authentication code. As described further below, certain techniques can make it easier for the verifier to determine if an event occurred, while being much harder for an attacker to determine that an event occurrence was detected. The switch can be any means that provides a state change if the authentication device 120 is opened or otherwise tampered with including, without limitation, a separable contact surface, or any form of limit switch such as a pushbutton switch, rocker switch and the like.

[0058] In one embodiment, in order to authenticate the user 110 and determine the event state of the authentication device 120, the verifier 105 performs an algorithmic calculation on a received authentication code that "reverses" some or all of an algorithmic calculation performed by the user authentication device 120. In a simplistic example, the user authentication device

120 generates an authentication code by arithmetically combining a secret stored by the user authentication device 120 and a user-supplied PIN. In order to verify the user in this example, the verifier retrieves from its records the PIN associated with the user and the secret stored on the user's authentication device 120. The verifier 105 reverses the combination operation, e.g., by subtracting and/or XOR the user's PIN from the received authentication code. The verifier 105 compares the result after PIN removal to the value of the secret stored on the user's authentication device 120, or to the value that should have been generated at that time by the device 120 using the stored secret. If they match, the user is authenticated. If they do not match, user authentication fails. In some embodiments the verifier 105 decrypts a value encrypted by the user authentication device 120 using symmetric key encryption or asymmetric encryption techniques, such as public key encryption. In some embodiments, the verifier 105 also calculates the authentication code with an input that indicates whether one or more events have occurred. In other versions, the verifier 105 calculates the authentication code with an input that indicates whether an event has occurred, and also indicates additional information concerning the event.

[0059] In other embodiments, a first authentication of user 110 is performed by the user authentication device 120 based on information supplied to the authentication device 120 by the user 110. For example, the information supplied by the user may be a PIN, a password or biometric information. The device 120 may perform this first authentication alone or in combination with another device. If the first authentication is successfully verified by the authentication device 120, the device 120 generates an identity authentication code which is verified by the verifier 105. In one embodiment, the strength of the first authentication is communicated as event state in the authentication code that is verified by the verifier 105. For example, the event state can reflect the degree of the match of a biometric element. In a further embodiment, the first authentication is a local authentication performed in the presence of the user 110.

[0060] Referring to FIG. 2, in one embodiment of the user authentication device 120 and verifier 105 of FIG. 1, various values are combined by a combination function 230 to generate an authentication code 290. In general, the combination function 230 generates an authentication code 290 based on the data 235 stored or accessed by the user authentication device 120. As shown, such device data 235 includes a device secret (K) associated with the user authentication device 120, a dynamic, time-varying value (T) generated by the user authentication device 120, and an event state (E) representing the occurrence of one or more events.

[0061] Other examples of device data 235 include the time and date of manufacture of the user authentication device 120, the amount of time since generation of the last authentication code, an encoding of the location (e.g., latitude and longitude) of manufacture of the user authentication device 120, an encoding of the location (specifically or generally) of the user authentication device 120 at the time of generation of the authentication code (using GPS or enhanced GPS, for example), device signature or pattern, device type (e.g., hardware or software), or any combination of one or more of these or other quantities. The combination function 230 can also optionally employ one or more of user data (shown in phantom view as user data (P)) or verifier data (shown in phantom view as verifier identifier (V)) and a generation value (shown in phantom view as generation value (N) and described further below) to generate an authentication code (A) 290 for the user. Other examples of user data include data derived from biometric information such as retinal scans and fingerprints; identifying information such as social security number, birth date (possibly including time of birth); and unique names and numbers, or other information. Verifier data can include information identifying the verifier 105, such as a name, number, IP address, or processor serial number. A generation value N can indicate the number of authentication codes requested in a specified time period.

[0062] The combination function 230 can be implemented as instructions executed by a computer, for example, by firmware running on an embedded microprocessor. In other

embodiments, the combination function 230 can be implemented in special-purpose hardware, such as an application specific integrated circuit, a field-programmable gate array, or other logic device. In still other embodiments, the combination function 230 can be implemented as a software application program running on a general-purpose desktop, laptop, or handheld, or other computing device.

[0063] The figure depicts generally a number of exemplary embodiments for generating an authentication code 290. It should be understood that the manner of combination and the input provided to the combination function 230 could vary from these examples. In one embodiment, an authentication code 291 is constructed from a stored secret (K), a dynamic value (T), and an event

[0064] The combination function 230, and the elements of the combination function can be implemented in the device 120, the communications terminal 140, or a combination of the two.

[0065] The stored secret (K) is a unit of information such as a numerical value that is uniquely associated with the device 120. In a typical hardware implementation of the device 120, the secret (K) is manufactured into and stored inside the device 120 such that it is very difficult to extract the secret (K) from the device. In a typical software implementation of the device 120, the secret (K) is stored in a data store, preferably secure, and accessible to the device 120. In addition to being accessible to the device 120, the secret (K) is also stored in a secure data store accessible to the verifier 105. In some embodiments, only the device 120 has access to the secret (K), and the verifier has access to a function of the secret (K), or vice-versa. In some embodiments the device's 120 secret (K) corresponds to, but is not the same as a value stored with the verifier 105, for example, where each has one of a pair of keys in a public key cryptosystem. In other embodiments the secret (K) can be derived from a master secret (K_{MASTER}), as described below. In some embodiments, the secret (K) is a value that is chosen from a large number of possible values such that it would be difficult for an attacker who had

access to the output of the combination function 230 to guess the secret by trying each possible secret value to see if it resulted in the observed authentication code. In one particular embodiment, the secret (K) is selected from the group of numbers that are 128 bits in length, (i.e., the set of nonnegative numbers less than or equal to 2^{128}-1).

[0066] The dynamic value (T) is a unit of information such as a hexadecimal or decimal numerical value that changes over time. In one embodiment, the dynamic value (T) is uniquely associated with a particular pre-determined time interval demarcated by a particular starting time and ending time. The time interval is not required to be of any particular length nor is every time interval required to be the same length. The only requirement is that the time interval schedule be roughly synchronized between the device 120 and the verifier 105. Exemplary methods that can be used to synchronize the device 120 and the verifier 105 are described in United States Patent No. 4,885,778, titled "Method and Apparatus for Synchronizing Generation of Separate, Free Running, Time Dependent Equipment." A time interval could have the length of a second, a minute, an hour, a month, a year, or any other convenient length of time. There is a balance to be struck between increased security from a shorter time interval and the processing capabilities of the device 120 and verifier 105, as well as the time that it will take for the authentication device 120 to provide the code to a verifier. For example, if the device 120 displays the authentication code for the user to type into the communications terminal, a time interval of a minute may be used. In one embodiment, the dynamic value (T), identifying a particular time interval, remains constant for all authentication codes generated within that particular time interval.

[0067] For example, in one embodiment, a constant time interval of a minute is used, and the dynamic value is the number of minutes since midnight, January 1, 1980. In another embodiment, a time interval of an hour is used and the dynamic value is the number of seconds since Noon, Dec. 15, 1999. The number of seconds is determined for the first second of each

time interval. In such an embodiment, the time from which counting begins can be a secret that is shared between the device 120 and verifier 105. The interval period length(s) can also be secrets that are shared between the device 120 and the verifier 105.

[0068] In another embodiment, the length of each time interval is an hour. Since, there are 24 hours in a day, each hour can be identified by a unique value such as the values 1 through 24; each of the 365 days of the year can be uniquely identified by the values 1 through 365; and each year can be identified by the number of the year, for example 2001. These three values, each identifying an hour, a day or a year, are combined in such a manner to produce a value that uniquely identifies one and only one particular one-hour time interval. This one hour time interval can be indicated by a particular (hour-day-year) combination. For example, the value 100232001 would uniquely identify the period of time between 9:00 am and 10:00 am on the 23rd day (023) of the year 2001 (2001), that is January 23, 2001. Similarly, the value 170322001 would uniquely identify the time period between 4:00 pm and 5:00 pm on the 32nd day (032) of the year 2001 (2001), that is February 1, 2001. Other variations will be immediately understood by those of ordinary skill in the art.

[0069] In one embodiment, the dynamic value (T) is provided as the output of a time clock function, which output is in turn provided to a dynamic value function. The dynamic value function determines the appropriate dynamic value (T) in response to the data provided by the clock function. In one such embodiment, implemented in a device having a clock and a processor, the dynamic value (T) is generated by a clock that is a counter that is set to an initial value and is incremented every second. This clock counts the number of seconds since the initially configured time. Every sixty seconds the clock signals the dynamic value function, which reads the clock, increments the dynamic value (T), and stores the incremented dynamic value as the dynamic value (T) for that time interval. In some embodiments the time value is provided in ISO-8601 format.

[0070] In some embodiments, the dynamic value (T) is provided by an external clock, for example, the clock of the communications terminal 140. In some embodiments, the dynamic value (T) changes based on some regularly-occurring action, for example, upon a request for an authentication code, or upon a received external signal. The regularly occurring action could be an event observable to the device 120 and preferably observable or roughly approximatable by the verifier 105 for example, a received radio signal, or an authentication attempt. Upon such a regularly occurring event, the dynamic value (T) changes. Such an event typically will not be an event that results in a change in event state (E). Thus, such an event typically will not be a reportable event.

[0071] In one embodiment, the secret (K), the dynamic value (T) and the event state (E) are provided to the combination function 230 for combination as authentication code A (K, T, E) 291. The combination of the secret (K), the dynamic value (T) and the event state (E) can take place in any order and can use one or more various combination methods. For example, in one simplistic embodiment, a one-way function such as a hash function, is applied to the values (K, T, E), and the result truncated to the right length, in order to arrive at a resulting authentication code. In another embodiment, at least two of the values (K, T, E), or portions thereof, are provided as input to the one-way function. A one-way function is a mathematical function that maps a universe of input values to a universe of output values in such a way that knowledge of the output of the function does not allow one to reconstruct the input provided. Examples of one-way functions are a hash functions, such as MD5 and SHA-1, and key derivation functions. In one particular embodiment, a block cipher, such as the RC6 or Rijndael (AES) algorithms, uses the secret (K) as the key and the dynamic value (T) as the data in order to generate the combination of (K) and (T). In one of these embodiments, the combination function 230 is designed such that each different event state (E) that is combined with a constant stored secret (K) and a dynamic value (T) results in a different authentication code value. As noted above,

any order of combination is possible, and two of (K), (T), and (E) can be combined at the user authentication device 120 and the other combined with that result at the communication terminal 140.

[0072] User data (P) can also be provided as input to the combination function 230. The user data (P) is a unit of information such as an alphanumeric character string, or a strictly numerical value, for example a personal identification number (PIN) or password. In one embodiment, the user data (P) is information uniquely associated with the user 110. The user data (P) can also be obtained by biometric measurement or observation. In one embodiment, the identity or value of the user data is a secret known only to the user 110 and the verifier 105 (i.e., not to the device). The user data (P) can be stored in a manner accessible to the verifier 105 that protects it from being compromised. The user data (P) can be the actual PIN, password, biometric data, etc. that is provided by the user, or the user data value (P) can be the result of processing of the user data by one or more other functions. For example, the user data (P) can be mapped to another value with a one-way function, such as a hash function, or a key derivation function before being provided as an input to the combination function 230. Derivation functions can be used that combine the password with other information. For example, to increase security a random string of information referred to as a salt can be combined with the password prior to the application of the derivation function. The salt need not be a secret value. An iterative function can also be included in a derivation function. A number, referred to as an iteration count, can be used to indicate how many times to perform an underlying function by which the password is derived. The incorporation of the iteration count into the derivation function increases the effort required to derive a password. A modest number of iterations, for example 1000, is not likely to be a burden for legitimate parties when computing a key (e.g., user data), but it will be a significant burden for attackers. If the user data value is random and selected from a large number of possible values, a smaller iteration count can be used.

[0073] In one embodiment, the combination function 230 combines the user data value (P) with the secret (K), the dynamic value (T), and the event state (E) to generate an authentication code A (K, T, E, P) 292. The combination function 230 can combine these values (K, T, E, P) in any order (and with other values not mentioned) to generate the authentication code 292. In one particular embodiment, the user authentication device 120 first combines (K, T, E) to generate an authentication code A (K, T, E) 291 as described above. The combination function 230 then combines the generated authentication code 291 with the PIN (P) to generate an authentication code 292 that is a function of (K, T, E, P). The PIN (P) can be combined with A (K, T, E) by prepending or appending the PIN (P) to A (K, T, E), by arithmetically adding the PIN (P) to A (K, T, E), or using a block cipher or other one-way function, or other algorithm, or a combination of these and other techniques that combine two or more input values together. The same steps can be used for both combinations, or they can be different – for example, (K) can be provided as key input to a block cipher and (T, E) as data inputs to the block cipher, and the PIN combined with the block cipher result by an addition or exclusive-or operation. In another embodiment, the user data value (P) and the event state (E) are combined first for use as input to an encryption function, and then the dynamic value (T) and the secret (K) are combined with them by using them as a key to encrypt the result. In another embodiment, the dynamic value (T) and the secret (K) are combined, and the user data value (P) and the event state (E) are combined with the result. The combination can take place at the same time, for example, as the values are provided as input to a single function, or in stages, as some values are combined with others. Certain combinations can take place on the user authentication device 120 while others can take place on the communication terminal 140. Of course, it should be understood that the combination can include as variations other values or processing.

[0074] As described, various embodiments of the device 120 can receive input of the user data (P) in various ways. These can include without limitation, user input (e.g., of a PIN) via a

keypad, a keyboard, a touch sensitive screen, selection with a pointer or mouse, handwriting recognition, voice recognition and so on. The user data can be read using a biometric reader that is integrated with the authentication device 120. The user data (P) can also be communicated from another device via electrical or electromagnetic means. It should be understood that there can be more than one item of user data (P), for example, provided by PIN entry and a fingerprint reader. Likewise, as another example, a PIN can be verified by the device, and data provided to the combination function in response to successful verification of the PIN by the device.

[0075] In various other embodiments, other data can be combined with the data just described (i.e., with or without the user data (P)) to generate the authentication code 293. This other data can include a generation value (N), which is incremented for each authentication code requested within a time interval. See co-pending U.S. Patent Application Serial No. 10/010,769, entitled "Enhanced Time-Based Authentication," by Brainard et al., the contents of which are incorporated herein by reference.

[0076] The other data also can include a verifier identifier (V), which is a value associated with the identity of a particular verifier (105) or group of verifiers. The use of the verifier identifier (V) allows the same user authentication device 120 (with the same secret (K)) to be used with verifiers operated by different entities without giving a particular entity information that could be used to impersonate the user to another entity. See co-pending United States Patent Application Serial No. 09/304,775, entitled "System and Method for Authentication Seed Distribution," by Brainard et al. the contents of which are incorporated herein by reference.

[0077] For example, in one embodiment, the combination function 230 combines a secret (K), a dynamic value (T), event state (E), user data (P), verifier identifier (V), and a generation value (N) to generate an authentication code 293. The combination function can combine these values (K, T, E, P, V, N) in various ways and in any order. Before being combined by the combination function 230, these values can be processed by one or more other functions.

Various embodiments of the authentication device 120 can receive input of this data in various ways.

[0078] In one embodiment, the portion of the secret (K) used to generate an authentication code 290 changes over time. Portions of the secret (K) are derived from other portions based on the dynamic variable (T). For example, there can be a portion of the secret value (K) that is allocated for a particular time interval. In this embodiment, a portion of the secret (K) can be different for each second, each minute, each hour, each day, each month, or each year. This can be accomplished by representing secret (K) as a set of secrets: one corresponding to the current year (K_Y), one corresponding to the current month (K_M), one corresponding to the current day (K_D), one corresponding to the current hour (K_H), and one corresponding to the current minute (K_{MIN}), that is, $K=(K_Y, K_M, K_D, K_H, K_{MIN})$ (or a subset or a function based on one or more of them), for each minute time value according to dynamic value (T). Thus, in these embodiments, portions of the secret (K) can be derived from each other, and a portion of the secret (K) can be used to generate the authentication code 290.

[0079] For example, the yearly secret (K_Y) can be generated by using a block cipher with a secret as the key and the current year, appropriately padded, as the data value. For example, in an embodiment using a 128 bit block cipher, the current year value (0000-9999) can be padded with 0's, 1's, or some random pattern that is known to the verifier 105, in order to provide a 128 bit data block. Thus, $K_Y=E_K$ (YYYYPPPPPPPPPP) where P represents padding and E_K represents a block cipher of the data YYYY using the secret as the key. In a similar manner, a monthly secret can be derived by applying the same or a different block cipher a second time: $K_M=E_{KY}$ (YYYYMMPPPPPPPPPP) where YYYYMM represents the current month and year values and the yearly secret is used as the key to the block cipher. Daily and hourly secrets can similarly be generated: $K_D=E_{KM}$ (YYYYMMDDPPPPPP) and $K_H=E_{KD}$ (YYYYMMDDHHPPPP).

[0080] In various embodiments, each of the secrets can be used during the relevant time interval to generate the authentication code. For example, the hourly secret can be used as the secret above, combined with the time and event state data to generate an authentication code. Although the above example has been given with respect to block ciphers, it will be understood that any of the methods described here for generating the secrets can be used (e.g. hash functions). Other techniques for generating new secret values are described in United States Patent No. 5,361,062 to Weiss, entitled, "Personal Security System."

[0081] In another approach, the event state can be communicated in a manner such that it is not provided directly as input into the combination function. In one such embodiment, for example, the event state can be communicated by modifying the time provided by the device's clock in response to the event state. In an exemplary implementation of this embodiment, the device advances its clock by one or more minutes to indicate the occurrence of an event. The clock is decremented by one or more minutes to indicate another event. Provided that the device's clock and the verifier's clock have the required degree of accuracy, the verifier can determine the event state simply by determining whether the device's time is earlier, later, or the same as the time expected by the verifier. Moreover, it should be understood that other values and calculations can be used in combination with those described.

[0082] A challenge may also be an input to the combination function 230. In one implementation, the response is derived from a challenge, the secret key, and the event state, i.e., it is not derived from time. For example, a verifier-supplied challenge value could be used as the dynamic value (T) as described above.

[0083] Also, as part of the combination function, one or more values (e.g., the event state (E)) can be used to select data to be provided as input to mathematical operations. In one embodiment, there are two or more secrets (K) which can be used as input to the combination function. As part of the combination function, the value of the event state (E) is used to

determine which of the secrets (K) will be used in the combination function to generate an authentication code. For example, in an implementation in which the event state (E) is one bit, and there are two secrets (K_0) and (K_1), an event state of 0 selects one secret (e.g., K_0) for use as K in the function 291 described above, and an event state of 1 selects the other secret (e.g., K_1). Thus, in an illustrative example, unless the device has been tampered with, the event state is 0, and the secret K_0 used in the function 291. Upon detection of tampering, the event state is set to 1, and the secret K_1 used in the function 291.

[0084] Referring now to FIG. 3, the data flow is shown for the operation of an embodiment that includes event state data 320 directly in the determination of an identity authentication code 330. An authentication device stores or calculates a first secret value, which is a device secret 305 associated with the device. This first secret value 305 can be the secret K described above, a portion of the secret K, or a variation or derivation thereof. The authentication device also stores or calculates a second secret value, an event secret 310 which is associated with the event state of the device. The event state represented by the event secret 310 is associated with an event which the device can communicate to a verifier. As mentioned, this may be a remarkable or anomalous event, not encountered in the usual operation of the device. The event secret 310 can be independent from the first secret value 305, derived from the first secret value 305, or the first secret value 305 and the value of the event secret 310 can be the same or derived from the same secret. The authentication device also has access to and/or calculates a dynamic value 315 which, as described, can be based on the current time as provided by a clock, or on another value, such as the number of authentication attempts, such that the dynamic value 315 changes over time.

[0085] Using the dynamic value 315 and the event secret 310, the authentication device 120 derives event state data 320 associated with a time period. In a version of this embodiment, the event state data 320 is a value represented by one or more bits of data. The event state data 320

can be determined in an iterative loop that is triggered by a change in the dynamic value 315, and/or the event secret 310. Additionally, the event secret 310 can be mathematically combined with all or a portion of the dynamic value 315. The event state data 320 is combined with the device secret 305 and the dynamic value 315 to form a time-specific value 325. The time-specific value 325 is then used to calculate the identity authentication code 330. The time-specific value 325 can be mathematically combined with a PIN, password, value derived from biometric reading, generation value, verifier identifier, and/or other information to form the identity authentication code 330. If event state data 320 is combined only with the dynamic value 315, then the attacker can determine whether the event state changed by requesting another authentication code before the dynamic value changes. Use of the generation value described above as input to the combination function, for example, will prevent this. Further, changing the event state each time the dynamic value is changed will make the state detection even more difficult for an attacker to determine.

[0086] In general, the occurrence of the event(s) associated with the event state results in the modification or some change associated with the event state data 320. In one embodiment, when a processor detects an event, it modifies event state data 320 stored in memory. In another embodiment, the event state data 320 is stored in memory that is inherently sensitive to an environmental event (e.g., electrostatic discharge) such that occurrence of the event will modify the event state data 320 without explicit action by the device. Also, the data store hardware for the event state data 320 can be designed such that an event (e.g., disassembly of the device) will automatically modify the event state data 320. The occurrence of the event associated with the event state data 320 can also result in the modification of the event secret 310. In this way, when new event state data 320 are generated, the new data will communicate the occurrence of the event. For certain events, however, it may be beneficial to only report (but not save) the current

state by determining event state data 320 from the event secret 310 without modifying the event secret 310. This allows events to be reported for either a long-term or a short-term.

[0087] In one embodiment, the event state data 320 are stored in the form of bits each associated with a time period (e.g., an hour). The respective event state bit associated with a time period is used to derive the time specific value 325 for that time period. In this exemplary embodiment, there are two possible choices for the event state bit, but there may be multiple bits (and thus multiple states) in other implementations. When a verifier receives the identity authentication code 330, the verifier will determine whether the received code is an expected value. If not, the verifier will calculate the expected authentication code for the opposite state bit (i.e., replacing 1 with 0 or 0 with 1). If the verifier obtains the received identity authentication code with the opposite state bit, the verifier has determined that the event occurred, and can take appropriate action. In another embodiment, the event state data 320 is one bit, and is the same as the event secret 310. The one bit indicates whether or not the event has occurred.

[0088] Referring to FIG. 4, an embodiment of a method for deriving authentication codes that communicate event state data is shown in which the value of the event secret (ES) 410 is repeatedly updated, for example, at the time that the dynamic value (T) 415 changes. In one embodiment, repeated updates prevent an attacker with access to event state data from determining whether an event has been detected, because the attacker cannot determine whether the changes to the event state data are the result of event detection or a routine update. Thus, event detection remains covert. In one embodiment, the event secret (ES) 410 is updated, or modified, regularly during normal operation, for example, when the dynamic value (T) 415 is updated. In another embodiment, the event secret (ES) 410 is regularly or periodically modified based upon some other interval or upon some other regular operation.

[0089] Upon the occurrence of a reportable event, the device takes an action to modify the event secret (ES) 410 in some way. For example, in some embodiments, the event secret (ES)

410 is modified one or more additional times upon occurrence of a triggering event and the modifications are made using the same function that is used for the regular modifications. In other implementations, upon the triggering event, the event secret (ES) 410 is modified using a different function than normally used, or by combining the event secret (ES) 410 with different data.

[0090] In one embodiment, the authentication device has a device secret (not shown) which is used in combination with the dynamic value (T) 415 to generate a secret associated with a day (K_D) 405. The day secret (K_D) is generated by encrypting information concerning the current date using the month encryption key K_M. For example, $K_D = E_{KM}(T) = E_{KM}$ (YYYYMMDDPPPPPP), where T represents the current dynamic value in a year-month-day format. The authentication device also stores the event secret (ES) 410, which in this embodiment has an initial value 411. In one version of this embodiment, the initial value 411 can be independent from the device secret. In another version, it is derived from the device secret. Also, the device secret and the initial value 411 can be the same or derived from a common value.

[0091] Periodically, as determined by the dynamic value (T) 415, a new value of the event secret (ES) 410 is derived using the event secret key (K_{ES}) 413, e.g., upon the first derivation, the initial value 411 is replaced. Changes to the value of the event secret key (K_{ES}) 413 also result in changes to event state bits (EBITS) 420 which are derived from the event state secret (ES) 410 using the event secret key (K_{ES}) 413. The event state bit or bits (EBITS) 420 associated with a particular hour are then used to generate an identity authentication code.

[0092] In this embodiment, the event secret key (K_{ES}) 413 is derived according to the equation K_{ES} = (ES xor FPAD1), where FPAD1 is a predetermined constant value. At each update interval, the new value of the event secret (ES) 410 is derived by using the event secret key (K_{ES}) 413 to encrypt the results of a logical operation applied to the existing value of the

event secret (ES) 410, for example, according to the equation ES = E_{KES}(ES xor FPAD2), where FPAD2 is also a predetermined constant value. Event state bits (EBITS) 420 are also derived by encrypting the results of a logical operation applied to the event secret (ES) 410, for example, according to the equation EBITS = E_{KES}(ES xor FPAD3), where FPAD3 is another predetermined constant value. Thus, to form the event state bits (EBITS) 420, an exclusive-or operation is applied to the event secret (ES) 410 and the FPAD3 constant value. In one embodiment, a group of 72 event state bits (EBITS) 420 are derived for each three-day period (i.e., a 72 hour period), and each of the event state bits 420 are each associated with an hour within the period.

[0093] The derivation of an authentication code based on the event state bits (EBITS) 420 may be completed by deriving additional secrets. First, a secret for the hour K_H 425 is derived from the daily secret K_D, the dynamic value (T) 415, and the event state bit associated with that hour (EBITS(T)) by providing these values as input to a function (g), which can be a one-way function, message digest, block cipher, and so on. This can be written as $K_H = g(K_D, T, EBITS(T))$. A secret for a minute (K_M) 429 within the hour can be calculated using a function (f), which can be the same or different than the function (g), and where (f) takes as input (K_H) 425 and the dynamic value for the minute, which can be written as $K_M = f(K_H, T)$. The minute secret (K_M) 429 can be used directly as an authentication code. Alternatively, the authentication code can be further derived from the minute secret (K_M) 429 for example by combining a PIN and/or other values as described.

[0094] Referring to FIG. 5 the contents of two value storage portions of device memory are shown in column 1 and column 2. Here, value 1 represents a secret value associated with the authentication device, and value 2 represents event state data associated with an event state. As actions occur, as shown in column 3, the actions can affect the example output (column 4) and/or the stored values (column 1, column 2). The leftmost column represents time increments

beginning with initial time T_1 and ending at time T_7. Because events may not occur on a periodic basis, it should be noted that the length of time between two adjacent times (e.g., T_1 and T_2) may not equal the length of time represented by another pair of adjacent times (e.g., T_2 and T_3). In this example, the output is displayed on a screen, however, as previously mentioned, other means of output are possible. In one embodiment, the secret value (column 1) that is updated is not the master secret value, e.g., a master seed derived from the master secret value.

[0095] At a first time period T_1, the authentication device is initialized. This can be performed either during the manufacturing process, or in a later setup process. Initialization can be accomplished either remotely or locally, for example, by wirelessly transmitting the device secret to the mobile device or downloading the secret to a device that is connected to a network. The initialization process is performed such there is at least partial synchronization between the device and at least one verifier. Here, synchronize is used to mean that two or more devices (i.e., the authentication device and the verifier) obtain consistent representations of some information. This can include the verifier sharing the complete representation of data A1 stored as the device secret (column 1) and the complete representation of data B1 stored as the event state data (column 2). It can also include, for example, sharing a portion of the data, or a representation in the sense of a public key related to a stored private key in a public key encryption system.

[0096] At a second time period T_2, time has elapsed and according to a change in the dynamic value, the secret value (column 1) and the event state data (column 2) are updated. As shown in the table, the device secret has the value A_2 and the event state data (column 2) has the value B_2. In one embodiment, the update of the values are performed by replacing their old values by values that are derived from these, preferably using a one-way function. In another embodiment, the value of each bit that represents the secret value or the event state data could be changed to a state that is opposite the state present at the time of the update (e.g., an inverse

operation). Other variations are possible, for example other sorts of modifications and combinations with other values.

[0097] At a third time T_3, the device secret in column 1 and event state data in column 2 respectively are the same as they were at time T_2, because the elapsed time since time T_2 is not sufficient to complete another update period for the dynamic value. In this example, at time T_3, a user enters a challenge and a correct PIN in the device, and obtains an output. In other embodiments, a challenge might not be used. In this example, the output (column 4) is a function of the device secret (column 1) and the event state data (column 2) as well as the challenge and PIN. It should be understood that entry of a challenge or a PIN is not a requirement of the invention even though it is included in this example. As described above, the output is communicated to a verifier, potentially along with the same or a different PIN or password, and a user identifier. The verifier determines whether the output is consistent with the state it believes the device to be in, which will be derived from (A_2, B_2) and the other described values. If it is not, the verifier attempts to determine if there is a state with which it is consistent. Based on a conclusion of one of a set of acceptable states, the user can be granted some permission associated with his account, identity, or membership, or an alert triggered, and so on.

[0098] At a fourth time T_4, time again has elapsed and due to a change in the dynamic value, the device secret (column 1) and the event state data (column 2) are updated such that the device secret has the value A_3 and the event state data has the value B_3.

[0099] At a fifth time T_5, an event occurs, which triggers a change in the event state data (column 2). As described above, this change could be the result of a direct effect on the memory due to the event. The change could also be implemented by processor instructions as a result, for example, of an interrupt or a change in a polled signal line. As shown in the table, the device secret still has the value A_3 but the event state data now has the value B_4, which represents an updated or modified state. In this example, the update of the event state value is performed by

replacing the old value B_3 by values that are derived from it, preferably using a one-way function. Replacement of the event state data (column 2) with a value that is known (e.g., an additional update) makes it possible for the verifier to determine whether there is an event occurrence recorded at the authentication device, as this change is reflected in future authentication codes. For example, the bits EBITS of the embodiment of FIG. 4 could be replaced.

[0100] At a sixth time T_6, time has again elapsed and according to a change in the dynamic value, the device secret value (column 1) and the event state data (column 2) are again updated. As shown in the table, the device secret now has the value A_4 and the event state data has the value B_5. The event state data is different from what it would have been had no event been registered at time T_5. This is because the values are updated by applying a function to their previous state; therefore, any modification will cause the event state data in future time periods to remain altered.

[0101] At time T_7, the user again enters a challenge and a correct PIN, and obtains an output value. The identity authentication code generated by the authentication device will be derived from the device secret A_4 (column 1) and the event state data B_5 (column 2). The output value is such that the user (or an observer) cannot determine without knowledge of the device secret or the original event state data that the event was registered in row five, even if an observer saved all communication between the user and a device, between the device and a verifier, and between a user and a device. Even so, the output value is still such that it can be detected by the verifier (upon verification of the value and associated information) that the registered event took place during or before the time of row 7. Thus, for example, an attacker who tampers with a token will remain unaware that event information is being transmitted to the verifier each time the altered token is used.

[0102] Referring again to the embodiment of FIG. 4, as an exemplary implementation, at time T_5, the used bits EBITS 420 (FIG. 4) are replaced. Thus, B_5 would be different at time T_7 from what it had been had the event not registered at time T_5. The change at time T_5 is included in later versions of the event state, and is reflected in the authentication code of time T_7.

[0103] In other implementations, it is possible that more information, such as the nature of the event and the time of the event, can be determined by the verifier. In this example, the verifier detects that the identity authentication code is a value associated with the user, but does not determine the event state. However, the value of the event state data can be modified in a manner which results in the generation of an authentication code, based on the event state data, that provides information concerning the nature and time of the event. For example, it is possible for one type of event to affect a first portion of the output, while not a second portion; whereas a second type of event can affect the second portion, but not the first. In some embodiments, the first and second portion can partially or fully overlap. If the first and second portion fully overlap, the two different events cause two different resulting output values, from which the verifier can determine not only that an event must have taken place, but also what type of event it was (i.e., the nature of the event). Similarly, the registration of an event during different time periods can affect different portions of the output, or cause the value of the output to fall within a different range of values. More detailed information concerning the event can also be communicated by, for example, associating a multi-bit value comprised of a plurality of event state bits 420 with each selected update period, e.g. an hour. The multi-bit binary value can allow for the communication of more information concerning the event than a single-bit value. For example, where the event is associated with the location of the device (e.g., is the device outside the U.S.?) there may only be two possible event states – yes or no. In this example, the nature of the event can be communicated with only a single bit. However, when the event state registers that the device is located outside the U.S., the verifier may be interested

in more specific information concerning the location event. In this example, the event state can communicate one of a number of possible cities, countries, or regions, etc.

[0104] In either case, and as previously mentioned, it is only possible for the verifier (with whom the device has been at least partially synchronized at some point in time, whether by direct communication, or by proxy) to determine from the output, or distribution of the output, whether an event was registered; what event(s) were registered; and when the event(s) were registered by the device. It should be understood that the values in the different columns only are meant to illustrate the teachings of the invention, and that they can be longer, shorter, of a different format or representation, or a combination thereof.

[0105] If the verifier determines that the determined state is one associated with the authentication device that the verifier is communicating with, while it may not be an acceptable state for granting access, it is possible for the verifier to take a specific action, for example (without limitation) to alert authorities; block access to the account; cause an event to happen, where this event can later be registered by said device; or any combination of these. As mentioned above, there can be multiple states for an event. However, in the description of Fig. 5, only two general categories (acceptable vs. not acceptable) are used for simplicity of exposition. It should be understood that a person skilled in the art can easily extend the two categories of states to three or more, given the teachings here.

[0106] Referring to FIG. 6, in one embodiment, a method for generating an identity authentication code by an authentication device includes storing event state data in an authentication device (STEP 601). The event state data can be stored in multiple parts, for example with an event secret and separate event state bits, as in the embodiment of FIG. 4. The event state value representative of the occurrence of an event can be stored in a data store such as a conventional memory, which can be internal to or external to a processor. The event state data can be stored in a memory that is sensitive to the event, such that the event causes a memory

modification without processor or other intervention. The event state data can be an electronic signal or port that is read by a processor. The event state data can be continuously updated. For example, the event state can include a memory that is continuously updated upon an appropriate change in a dynamic variable, with a function of itself, for example as described with reference to FIG. 5. The event state data can be stored as a value associated with the event state and bits derived from the value. In one such embodiment, the bits are each associated with a time interval.

[0107] The method also includes the step of modifying the event state data in response to an event (STEP 602). This modification can be accomplished by a processor receiving an appropriate signal, from a switch or otherwise. The event state data store can be designed such that the occurrence of the event inherently modifies the event state data. For example, electrical terminals of a memory can be connected to the device case such that removal of the case will change the memory contents.

[0108] As described above, the event can take many forms, and can be an unusual, or remarkable event, or an event that is not associated with normal operation of the authentication device. In general, authentication will not be as efficient if there is not a single expected state, because the verifier will have to compute the authentication codes associated with the other event states. Non-limiting examples of unusual events include tampering with the device (e.g., trigger of a case switch), and events external to the device, such as an environmental event (e.g., temperature or radiation exposure), incorrect power input (e.g., too high or too low), and so on. The event can also include the absence of such an event (e.g., power normal).

[0109] The modification can include immediately storing a first value in the event state data store, and thereafter storing a second value in the same data store or in another data store. If the values are stored in two different data stores, they still can overlap in part. The immediately stored value can be deterministically computed, or it could be a constant, such as 0 or 1. The

immediate data storage can be asynchronous meaning here that it is not updated synchronous with a processor or other hardware clock. The second value can be at least partially non-deterministic, for example if it is calculated from the original value, for example using a one-way function.

[0110] The method also includes generating an identity authentication code that depends at least in part on a dynamic value, the event state data, and a secret associated with the device (STEP 603). The generated authentication code can also depend on user data, such as one or more of a PIN, a password, and data derived from a biometric observation. The user can provide this data to the authentication device. Some user data can be stored on the authentication device, possibly in encrypted form. The user can provide some input to the authentication device (i.e. biometric data) and the authentication device can decrypt other data.

[0111] The authentication device can verify the correctness of user data, and only provide an identity authentication code if the user data is correct. The presentation of incorrect user data a number of times can, in some embodiments, result in the modification of event state, so that the continued presentation of incorrect user data is reported to the verifier.

[0112] Authentication information including the identity authentication code is communicated to a verifier (STEP 604). As mentioned, the communication to the verifier can take place with or without human intervention. The verifier receives the authentication information, which can optionally include other authentication and identification data, such as a PIN, password, biometric reading, and the like. The verifier has access to a dynamic value and a secret associated with the device that can be the same, derived from, or related to the information stored or accessed by the authentication device. The verifier can verify the identity of the user and determine the event state in response to the received authentication code.

[0113] As described above, through appropriate design, the communication of the event state can take place such that only the authentication device and the verifier are aware of the communicated state.

[0114] Referring to FIG. 7, in one embodiment, the event state data comprises two secret values. The first secret value is a security enhancing secret (C). The second secret value is a status counter secret (X). In a version of this embodiment, each of the security enhancing secret (C) and the status counter secret (X) comprise bit strings of sufficient length to achieve strong cryptographic security, e.g., at least 80 bits. Regardless of their length, each secret (C) and (X) can be updated via a one-way cryptographic transformation such as a hash function, block cipher and the like. The security enhancing secret (C) is periodically updated. For example, when the security enhancing secret (C) is employed in an authentication device 120 (e.g., a token) the secret (C) can be updated at each time interval in which a new identity authentication code is produced for the token. As is described below, the time-varying nature of security enhancing secret (C) improves the security of the embodiment because possession of past values of the security enhancing secret (C) are generally not useful to attackers. The status counter secret (X) is updated on the detection of an event. The extent of the update that is made to status counter secret (X) can depend upon the quantity of events that are detected, the nature of detected events, or both. When updates to the status counter secret (X) are made to indicate the nature of the detected events, a classification system can be employed so that a specific update value corresponds to a specific detectable event. For example, different values of X can refer to different events or event states.

[0115] An event code (F) is a value that is the result, at least in part, of the combination of the security enhancing secret (C) and the status counter secret (X). For example, the event code (F) value can be some portion of an output of a function that is applied to secrets (C) and (X). In one version, the event code (F) is some portion of the value that results when an exclusive-or

operation is applied to (X) and (C). If the status counter secret (X) is a strong secret, this approach is advantageous because it provides forward-secure encryption. In another version, the event code (F) is some portion of the value of status counter secret (X) encrypted under a standard symmetric cipher (e.g., AES) where security enhancing secret (C) is employed as the secret key. As used here, the term portion refers to values comprised of the whole or some part thereof.

[0116] The event code (F) can be used to generate authentication codes that communicate the quantity of detected events, the nature of detected events or both. For example, as shown, the event code (F) can be combined with an authentication value (S), which is, a value resulting from the combination of secret (K) and dynamic value (T). The result of combining (F) and (S) is the authentication code (A). In one embodiment, the authentication code (A) is some portion of the value that results when an exclusive-or operation is applied to event code (F) and authentication value (S). Alternatively, the authentication code (A) is derived when a message authentication code (MAC) is applied to event code (F) where authentication value (S) is employed as the secret key.

[0117] For the purpose of the following description, the authentication code generated by the authentication device 120 is represented by (A_D) in order to distinguish it from the authentication code generated by the verifier, also using the technique just described, which will be referred to as (A_V).

[0118] The authentication code (A_D) is transmitted to a verifier for verification. In one embodiment, the verifier attempts to reconstruct authentication code (A_D) by updating the security enhancing secret (C) for the current time in a manner similar or synchronized with the authentication device, and computing the current authentication value (S). The verifier also employs the stored value of the status counter secret (X) and security enhancing secret (C) to derive event code (F) as previously described. The verifier employs the values of the event code

(F) and the security enhancing secret (C) to derive a first authentication code (A_{1V}). The verifier compares the value of the first authentication code (A_{1V}) with the value of the received authentication code (A_D) generated by the authentication device 120. The authentication code (A_D) is accepted by the verifier if (A_D) is equal to (A_{1V}).

[0119] If the received authentication code (A_D) does not equal first authentication code (A_{1V}), the value of status counter secret (X) that is stored by the verifier is updated. The updated value of status counter secret (X) is used to derive an updated value of event code (F). The verifier then employs the updated value of event code (F) and the security enhancing secret (C) to derive a second authentication code (A_{2V}). Again, the authentication code derived by the verifier (i.e., (A_{2V}) in this iteration) is compared with authentication code (A_D). If (A_D) is equal to (A_{2V}) the verifier can determine the quantity and/or nature of any events indicated by the value of status counter secret (X). The verifier can employ this knowledge to authenticate the authentication code (A_D), determine that authentication code (A_D) is invalid, notify a trusted authority that one or more events have occurred (e.g., device tampering), or a combination thereof. Additionally, where appropriate the verifier can also notify the user 110 of the event, notify the issuing authority of the event, or both. If authentication code (A_D) does not equal second authentication code (A_{2V}), the verifier can repeat the process of updating status counter secret (X) and deriving values of event code (F) and authentication code (A_V) until the value of status counter secret (X) that produces authentication code (A_D) is determined. Alternatively, the verifier can determine that authentication code (A_D) is invalid without repeating the authentication process for a particular authentication code (A_D) supplied by authentication device 120. If the received authentication code (A_D) does not match the expected authentication code (A_{1V}), the verifier can also calculate additional authentication codes associated with adjacent time periods to account for possible clock drift between the authentication device and the verifier.

[0120] In one embodiment, a verifier can also efficiently determine the event or events corresponding to the value of status counter secret (X) that an authentication code (A_D) is, in part, derived from when the event code (F) and the status counter secret (X) are derived in a particular manner. In a version of this embodiment, the event code is event state data. Specifically, where both event code (F) is derived from an exclusive-or applied to security enhancing secret (C) and status counter secret (X), and authentication code (A_D) is derived from an exclusive-or applied to event code (F) and authentication value (S), the verifier can efficiently compute the status counter secret (X_D) corresponding to authentication code (A_D). First, the verifier computes event code (F_D) corresponding to the authentication code (A_D) as a function of an exclusive-or operation applied to authentication value (S) and authentication code (A_D). Next, the verifier computes corresponding status counter secret (X_D) as a function of an exclusive-or operation applied to event code (F_D) and security enhancing secret (C). As described in the previous example, the process can be repeated until either the verifier can determine the quantity and/or nature of any events indicated by status counter secret (X_D) or the authentication code (A_D) is invalidated.

[0121] Referring now to FIG. 8, in one embodiment, a system for authentication and event state communication is one implementation of a design to make it difficult for an attacker who has access to the device to determine if an event was detected by an authentication device 120 and/or communicated in an authentication code 810.

[0122] In an authentication device 120, event state data 812 is stored in a memory, such as a register 814. (A verifier can store event state data 812 for one or more authentication devices 120 in a similar manner.) Event state data 812 is periodically updated, for example in response to a change in dynamic value (T) 815. These scheduled updates are made by both the authentication device 120 and the verifier. A register 814 for such a system can be initialized by

employing a random value known by both the authentication device 120 and the verifier but no one else.

[0123] In one implementation, the event state data 812 itself is updated simply by applying the event state data as the input (or one of the inputs) to a one way function. This is shown in the figure as $ES_t = f_1 (ES_{t-1})$, where in this example, ES_t is the current event state data 812, ES_{t-1} is the event state data 812 from the previous period, and f_1 is a one way function such as a hash function (e.g., MD5 and SHA-1), key derivation functions, and the like. Other operations (e.g., bit-swapping, math operations) can also be performed as part of the updating function f, and other data, such as a device secret, can also be included in the updating operation. This periodic updating is deterministic such that the event state data is predictable at a given time to those devices and entities that know both the value of ES_{t-1} and the algorithm that is being employed in the updating operation. This predictability allows the event state data 812 that is provided by the authentication device 120 to match the event state data 812 that is predicted by the verifier provided that the verifier is appropriately synchronized with the authentication device.

[0124] Because a past value of the event state data 812 is employed in deriving the next value of the event state data 812, past events have a continuing impact on later derived values of the event state data 812. For example, at a given time T_1, the event state data 812 will have a particular value, and at a second time T_2, the event state data 812 will have (with very high probability) a different value, which is predictable to a verifier. However, the event state data 812 is not predictable to an observer who does not know the original value. The observer's uncertainty about the starting time may also be an obstacle. An attacker who gains access to the event state data 812 will know when the data is updated, but will not know how the event state data 812 relates to previous event state data 812, i.e., whether the previous event state data 812 was simply updated, or previously modified and/or updated with different operations, or at a different time, than the normal operation. Thus, it is not possible for the attacker to recreate a

past value of the event state data 812 to eliminate evidence of the occurrence of an event that the attacker does not want revealed (e.g., device tampering).

[0125] Upon the occurrence of an event, the event state data 812 of the authentication device 120 is modified in a manner that is different than it otherwise would be during normal operation. These unscheduled updates (U) modify all or a portion of the event state data 812 in a manner that corresponds to the occurrence of the detected event, the nature of the event, the state of the event or a combination of the nature and the state. In one embodiment, upon occurrence of the event, the event state data 812 has a value that is for the next time period, rather than the current time period. This approach has the advantage of making the operation of the device (i.e., event state data updating) appear normal, as the attacker will likely not know if the update was a result of event detection or normal operation. In another embodiment, when an event occurs, a different method of performing unscheduled updates (U) is used to update the event state data 812 than the method employed to generate the periodic updates. In one such implementation, secret data (not shown), which may or may not be the device secret 802, is used in performing unscheduled updates (U). For example, the secret data or a value derived from the secret data can replace, or can be combined with the event state data 812.

[0126] The register 814 includes a plurality of bits 817 (e.g., a and b) and can include a first portion 818 and a second portion 820. When the event state data 812 is split into two or more portions, where one or more portions can indicate the current event state (ES_c) 818, and one or more portions can correspond to previously detected events (ES_{LT}) 820. In one embodiment, the periodic updates modify (e.g., set, reset, or perform operations using other data) the bits corresponding to the current event state (ES_c) 818 while leaving the long-term event state (ES_{LT}) 820 unchanged. In this example, both the long term event state (ES_{LT}) 820 and the current event state (ES_c) 818 are used in the updating operation.

[0127] In FIG. 8, the long-term event state data 820 and the current event state data 818 are shown as continuous portions comprised of adjacent bits 817. However, either or both of the long term event state data 820 and the current event state data 818 can be partitioned into non-adjacent portions of register 814. These portions can be comprised of a single bit, adjacent bits, non-adjacent bits, or bits 817 that are selected from the register 814 in some other deterministic fashion. Further, each of the long-term event state data 820 and the current event state data 818 can employ none of the same bits, some of the same bits, or all of the same bits. Where an apportioned register 814 is employed, an event that occurs during the present time period can, in one version, only act to update the value of the portion of the register 814 that contains information concerning the current event state data, e.g. (ES_c) 818. Thus, the detection of an event can have a long-term or short-term effect, depending on what portion of the event state data is modified.

[0128] In one embodiment, a selector 822 selects a secret from a plurality of secrets, shown in the figure as S_1, S_2, etc., which can be employed in generating an identity authentication code 810. The plurality of secrets are values that are generated in a manner that prevents their disclosure to an attacker, for example, the secrets can be the result of a random number generator, a cryptographic algorithm and the like.

[0129] A portion of the event state data stored in register 814 is used at a particular time to select from two or more secrets $S_1, \ldots, S_n$. For example, if there are two secrets S_1 and S_2, one bit (a) can be used to select between the two secrets, e.g., S_1 if a = 0; and S_2 if a = 1. If there are four secrets S_1, S_2, S_3, S_4 two bits (ab) can be used to select between the secrets, e.g., S_1 if a = 0, b= 0; S_2 if a = 1, b = 0; S_3 if a = 0, b= 1; and S_4 if a = 1, b= 1. The selected secret is supplied by the selector 822 to a combination function 826 to generate the authentication code 810. Thus, the authentication code 810 provides the verifier with information concerning an event's

occurrence and/or the nature of the event. Of course, other variations are possible. For example, a portion of the selected secret itself could be used as the authentication code.

[0130] In a further embodiment, a multi-level hierarchy of secrets is employed. One general example of a multi-level hierarchy is a set of values that include a month seed, a day seed, an hour seed, and a minute seed. In this example, the month seed is the highest level seed because it is required in order to determine the values of the day seed, the hour seed, and the minute seed. In the embodiment shown in FIG. 8, each secret $S_1, \ldots, S_n$ is generated from parent secret S_0, which could be the month seed, for example. Each secret is thus a different potential day seed. In one implementation of this embodiment, a secret is generated when, for each secret S_n, a function (f_2) is applied to parent secret S_0 and the corresponding secret number (n). The function (f_2) can be a one way function such as a hash function (e.g., MD5 and SHA-1), key derivation functions and the like. The secrets $S_1, \ldots, S_n$ generated in this fashion will also be periodically updated when the parent secret S_0 is updated. Thus, when a new day secret is generated, new event secrets can be generated as well. In a further version of this embodiment, the secret from the previous time period (e.g., S_n at T_1) can also be supplied as an input to function (f_2) to generate the secret for the present time period (e.g., S_n at T_2).

[0131] In general, the combination function 826 generates the authentication code 810 using data that is stored onboard the authentication device 120 and/or remotely accessed during the authentication process. As shown, the data can include values such as a secret $S_1, \ldots, S_n$ representing the occurrence of one or more events, a device secret 805, dynamic value (T) 815, a generation value (N), and the like. As in the other examples, values derived from these values could be used (e.g., a dynamic value, or a month seed derived from a device secret instead of a device secret). Likewise, additional values can be included in the combination function (e.g., a challenge value or other data).

[0132] In a version of this embodiment, a seven bit register 814 results in 128 available secrets, e.g., S_1, ... , S_{128}. However, the register 814 can be much larger, for example, 160 bits. The large register 814 size provides an opportunity to vastly increase the number of available secrets that can be selected. It should not be necessary, however, to expand the number of available secrets beyond the number required to provide the desired security level. This can be avoided by selecting only a portion of the total register 814 for use in providing event state data 820. Likewise, as another example, the register can be used for an hour, with two different bits used for each minute.

[0133] In other embodiments, the updates to event state data 812, updates to secrets S_1, ... , S_n, or some combination, result at least in part from challenges that the authentication device 120 receives from the verifier.

[0134] When a verifier receives the identity authentication code 810, the verifier determines, based on the known event state data 812, whether the received code 810 is an expected value. If it is not, the verifier calculates the expected authentication code 810 for one or more additional values of the event state data 812. Where a single bit of the event state data 812 is employed to generate the secret, there are only two possible event states. As a result, there are only two possible authentication codes 810 that could be provided by a valid authentication device 120, for example, a first authentication code derived using S_1, and a second authentication code derived using S_2.

[0135] When two bits are employed for selection, the verifier can determine whether the authentication code 810 was generated by any of the four possible events states of a valid authentication device 120 (e.g., 00, 01, 10, 11). When two bits are used, the verifier would compare the received code with the received codes that would be generated by secrets S_1, S_2, S_3 and S_4, and determine whether the authentication code indicates that an event took place or if an invalid authentication code was received. As described above, a larger the number of bits 817

included in the plurality of bits 817 increases both the number of potentially valid secrets, and the number of potentially valid authentication codes 810. However, these calculations performed by the verifier can be more rapidly completed where the verifier begins by calculating authentication codes 810 based on the most likely secret (i.e., the most likely value of the event state data 812). For example, the verifier will know the value of the event state data 812 at each of the preceding authentications. The verifier's knowledge reduces the number of iterations required before the verifier determines the event state of a valid authentication device 120, or the invalidity of the authentication code 810. Where event state data 812 is formed from a large number of bits 817, the reduced number of iterations can substantially increase the verifier's efficiency in processing authentication codes 810. Of course, a verifier that knows only how to generate the secrets $S_1, \ldots, S_n$ but not the event state data 812 can still verify an authentication code by trying each secret to see if one works, but lacks the preceding efficiency advantage and cannot determine the event state.

[0136] Alternatively, the authentication code 810 can include information that allows the verifier to immediately determine one or both of the time and the event state that the authentication code 810 is derived from without the need to perform iterative computations. In one embodiment, such an approach is implemented by including explicit information in the authentication code 810 that hints or suggests the time and/or event state.

[0137] The verifier may consider that an unscheduled update may have occurred when the event state corresponding to an authentication code is unexpected. The verifier may then recalculate the event state assuming that an unscheduled updated had occurred at some time between previous scheduled updates. If the recalculated event states continue to match event states corresponding to authentication codes in future authentication operations, the verifier may conclude that the unscheduled update has occurred at a particular time. Alternately, the verifier may conclude that an unscheduled updated has occurred without determining the time.

[0138] When an unscheduled update is detected by the verifier, the verifier can update the verifier's data concerning the authentication device 120 so that the results of future periodic updates performed by the verifier will correspond to the results of future periodic updates performed by the authentication device.

[0139] One or more of the preceding embodiments can be employed in a system that includes one or more master verifiers and one or more subordinate verifiers. Generally, the master verifier is more remote than the subordinate verifier from the communication terminal 140 employed during an authentication. In one embodiment, a master verifier stores the information required to calculate each secret and corresponding authentication code for one or more authentication devices 120. To facilitate authentication with authorized verifiers, both the authentication devices 120 and the master verifiers employed in this approach derive temporary secrets for each period. However, a subordinate verifier can only authenticate codes that are presented to it when it has received the secrets from a master verifier. Further, the secrets received by the subordinate verifier are only valid during specific periods of time (i.e., they are temporary secrets) and they are only valid for a limited number of authentication devices. As a result, the subordinate verifier only can authenticate for a reduced period of time. The periods during which the subordinate verifier can authenticate are limited to those periods for which the subordinate verifier possesses valid secrets that are used to generate authentication codes. This approach can be advantageous because it reduces damage that an attacker can do if the subordinate verifier is compromised.

[0140] A subordinate verifier subscribes to updates of the secrets and receives temporary secrets from the master verifier either on request, at scheduled updates, or both. These temporary secrets can be limited for use only during a specific period, e.g., a month, a day, an hour, etc. Additionally, or as an alternative, a set quantity of temporary secrets can be supplied where each secret can be used once at any time prior to the end of an expiration period. Some

values that can be employed as temporary secrets include, for example, device secret (K), dynamic value (T), and event state data (E) of FIG. 2. Alternatively, the temporary secrets of the preceding embodiments can be generated from a temporary master secret that is also only valid for a single period. In this alternative approach, the master verifier provides each of the subscribing subordinate servers with the temporary master secret that is employed to generate one or more of the device secret (K), dynamic value (T), and event state (E) for that period.

[0141] In a further embodiment that is also compatible with one or more of the preceding embodiments, intermediate servers are employed to facilitate the communication of information between the verifier 105 and the authentication device 120. This approach is advantageous because it increases the utility of authentication devices 120. For example, an authentication code can be presented to a system that generally does not participate with the authentication system 100, e.g., a system that lacks a verifier 105. In this embodiment, the intermediate server will communicate with the verifier 105 to complete the authentication.

[0142] One or more of the preceding approaches can also employ techniques to prevent an attacker from detecting past values of the event state and the event state data. This technique can be employed to prevent successful attacks by attackers who have access to the physical memory of authentication device 120. Such attacks have a potential for success because values stored in a memory for an extended period can burn themselves into the memory. Later attempts to erase or overwrite these values can not eliminate this hidden information from a properly equipped attacker. Magnetic storage media also suffers from undesired long term memory of previously stored values. As in the case of values stored in RAM, these past values can also be recovered by an attacker who has access to the memory.

[0143] In one embodiment, the frequent periodic update of event state data prevents burn in of past values of the event state data. In another embodiment, the event state data is cyrptographically protected. For example, event state data can be stored in more than one

register or in separate portions of the same register. Using this approach, an exclusive or operation can be applied to values that together form the event state data, and those values can be updated over time. The result is that the actual values of the event state data are not stored directly and no single value can burn in, but the event state data can still be easily determined. This method can be employed in conjunction with the previously described periodic updates. Such techniques are described, for example, in Di Crescenzo et al. "How to Forget a Secret," Symposium on Theoretical Aspects in Computer Science, 1999, the contents of which are herein incorporated by reference.

[0144] Variations, modifications, and other implementations of what is described herein will occur to those of ordinary skill in the art without departing from the spirit and the scope of the invention as claimed. Accordingly, the invention is to be defined not by the preceding illustrative description but instead by the spirit and scope of the following claims.

[0145] What is claimed is:

Claims

1. A method for generating an identity authentication code associated with an authentication device, comprising the steps of:

storing an event state in an authentication device;

modifying the event state in response to an event; and

generating an identity authentication code that depends at least in part on (i) a dynamic value, (ii) the event state, and (iii) a secret associated with the device.

2. The method of claim 1 wherein the event comprises a reportable event.

3. The method of claim 1 wherein the event comprises an anomalous event.

4. The method of claim 1 wherein the event comprises tampering with the device.

5. The method of claim 1 wherein the event comprises an event external to the device detected by the device.

6. The method of claim 1 wherein the event comprises an environmental event.

7. The method of claim 1 wherein the event comprises decreased battery power output.

8. The method of claim 1, wherein the event comprises the absence of at least one of an environmental event, decreased battery power output, and tampering with the device.

9. The method of claim 1, further comprising the step of displaying the identity authentication code.

10. The method of claim 1 wherein the generating step further comprises generating an identity authentication code that depends at least in part on (i) the dynamic value, (ii) the event state, (iii) the secret associated with the device, and (iv) at least one of a PIN, a password, and data derived from a biometric observation.

11. The method of claim 10 wherein the at least one of the PIN, the password, and the data derived from the biometric observation is stored on the authentication device.

12. The method of claim 11 wherein the at least one of the PIN, the password, and the data derived from the biometric observation is stored on the authentication device in encrypted form.

13. The method of claim 1 wherein the generating step further comprises generating an identity authentication code that depends at least in part on (i) the dynamic value, (ii) the event state, (iii) the secret associated with the device, and (iv) at least one of a PIN and a password stored in an encrypted form such that data obtained from a biometric observation can be used to decrypt.

14. The method of claim 10, further comprising, before the generating step, the step of receiving user input data comprising the at least one of a PIN, a password, and data derived from a biometric observation.

15. The method of claim 14 further comprising, before the generating step, the step of verifying the correctness of the user input data;

and further comprising the step of providing the identity authentication code only if the user input data is verified to be correct.

16. The method of claim 1, further comprising the step of transmitting the identity authentication code to a verifier.

17. The method of claim 16, further comprising the steps of:

receiving, by the verifier, authentication information comprising the identity authentication code;

determining, by the verifier, the identity of the user and the event state.

18. The method of claim 16 wherein the verifier comprises a representation of the secret associated with the device.

19. The method of claim 17, wherein the authentication information further comprises a user identifier.

20. The method of claim 17 wherein the authentication information further comprises at least one of a PIN and a password.

21. The method of claim 16 wherein only the device and the verifier can feasibly determine the event state.

22. The method of claim 1 wherein the step of modifying event state comprises storing event state data in a first data store.

23. The method of claim 22, wherein the modifying step comprises:

immediately storing a first value in the first data store, and thereafter storing a second value in a second data store.

24. The method of claim 22 wherein the first data store and the second data store are the same data store.

25. The method of claim 22 wherein the first data store overlaps with the second data store.

26. The method of claim 22 wherein the first data store is distinct from the second data store.

27. The method of claim 22 wherein the first value is deterministically computed.

28. The method of claim 22 wherein the first value is zero.

29. The method of claim 22 wherein the step of immediately storing is asynchronous.

30. The method of claim 22 wherein at least one of the first value and the second value is at least partially random.

31. The method of claim 22 wherein the second value comprises a calculated value.

32. The method of claim 1, wherein the generating step further comprises generating an identity authentication code that depends at least in part on a dynamic value associated with a time period and the occurrence of an event as reflected in the event state.

33. The method of claim 1, wherein the event state comprises a value associated with event state and bits derived from the value, the bits each associated with a time interval.

34. The method of claim 1 wherein the device comprises two components in communication with each other.

35. The method of claim 34 wherein at least a portion of the event state and at least a portion of the secret are stored on one of the two components.

36. The method of claim 34 wherein one of the components comprises a wireless communications device and the other component comprises a removable accessory to the wireless device.

37. A method for verifying a device:

receiving authentication information comprising an identity authentication code generated by a device that at least in part depends on time, a secret associated with the device, and an event state; and

verifying the identity of the user and determining the event state in response to the received identity authentication code.

38. The method of claim 37, comprising the step of taking an action in response to the event state.

39. The method of claim 37, further comprising the step of:

determining whether an event occurred in response to the determined event state.

40. The method of claim 37 wherein the event comprises tampering with the device.

41. The method of claim 37 wherein the event comprises an event external to the device detected by the device.

42. The method of claim 37, wherein the event comprises the absence of at least of an environmental event, decreased battery power output, and tampering with the device.

43. The method of claim 37, wherein the authentication information further comprises a user identifier.

44. The method of claim 43, wherein the authentication information further comprises at least one of a PIN and a password.

45. The method of claim 37 wherein only the device and the verifier can feasibly determine the event state.

46. The method of claim 37 wherein only the device and the verifier can feasibly determine if an event registered.

47. The method of claim 37, wherein the verifying step further comprises generating an expected identity authentication code that depends at least in part on a dynamic value associated with a time period and the event state.

48. The method of claim 46, wherein the event state comprises an event state secret and bits derived from the dynamic value, the bits each associated with a time interval.

49. A method for generating an identity authentication code by a device, comprising the steps of:

storing in a device a first secret value associated with the device;

storing in the device a second secret value associated with an event state;

generating by the device a dynamic value that changes over time;

deriving event state data associated with a time period from the second secret value;

deriving a time-specific value for a time period from the first secret value and the event state data; and

calculating an identity authentication code using the time-specific value as input.

50. The method of claim 49 wherein the event state data comprises bits each associated with a time period, and wherein the time-specific value is derived from the first secret value and the respective bit associated with the time period.

51. The method of claim 50, further comprising:
detecting occurrence of an event; and
modifying the event state bits in response to the detected event.

52. The method of claim 49, further comprising:
modifying the second secret value in response to the detected event.

53. The method of claim 49, wherein the first secret value is initially the same as the second secret value.

54. The method of claim 49 wherein the event comprises tampering with the device.

55. The method of claim 49, further comprising the step of displaying the identity authentication code on the device.

56. The method of claim 49, further comprising the step of transmitting the identity authentication code to a verifier.

57. The method of claim 49 wherein the event state data comprises bits and a plurality of the bits are associated with a respective time period, and wherein the time-specific value is derived from the first secret value and the plurality of bits associated with the respective time period.

58. The method of claim 49 wherein the event state data is derived from the dynamic value and the second secret value.

59. A system for generating an identity authentication code associated with an authentication device, comprising an authentication code generator for generating an identity authentication code that depends at least in part on a dynamic value that changes over time, an event state indicative of the occurrence of an event, and a secret associated with the authentication device.

60. A method for generating an identity authentication code by an authentication device and verifying said identity authentication code by a verification device that is approximately time synchronized with the authentication device, comprising the steps of:
storing event state in an authentication device;
modifying the event state in response to an event;

generating an identity authentication code that depends at least in part on a time value, the event state, and a secret associated with the device;

transmitting the identity authentication code to the verification device; and

verifying the identity authentication code by the verification device and determining the event state.

61. A system for authentication and event state communication, comprising:

an event state data value;

a first event state modifier for periodically updating the event state data value in a predetermined manner during normal operation and a second event state modifier for updating the event state data value upon the occurrence of an event;

a plurality of secret values;

a selector for selecting one of the secret values in response to the event state data value occurring when an identity authentication code is generated; and

a code generator for generating an identity authentication code in response to the secret value.

62. The system as claimed in claim 61, wherein a first portion of the event state data value is updated by the first event state modifier and a second portion of the event state data value is updated by the second event state modifier.

100
USER
110
USER
INTERFACE
130
TERMINAL
INTERFACE
145
USER
AUTHENTICATION
DEVICE
120
COMMUNICATIONS
TERMINAL
140
VERIFIER
105
160
DEVICE/TERMINAL
INTERFACE
170
COMMUNICATIONS
CHANNEL

FIG. 1

DEVICE DATA 235
SECRET (K)
DYNAMIC VALUE (T)
EVENT STATE (E)
VERIFIER IDENTIFIER (V)
COMBINATION FUNCTION 230
GENERATION VALUE (N)
USER DATA (P)
AUTHENTICATION CODE 290
A (K, T, E) 291
A (K, T, E, P) 292
A (K, T, E, P, ... {N, V, ...} 293

FIG. 2

DEVICE SECRET
305
DYNAMIC VALUE
315
EVENT SECRET
310
EVENT STATE DATA
320
TIME-SPECIFIC VALUE
325
IDENTITY AUTHENTICATION CODE
330

FIG. 3

INITIAL ES 411
EVENT SECRET (ES) 410
ES =E_KES(ES xor FPAD2)
K_ES = (ES xor FPAD1)
K_ES 413
DYNAMIC VALUE (T) 415
K_DAY 405
EBITS = E_KES (ES xor FPAD3)
EBITS 420
KHOUR = g (K_DAY, T, EBIT (T))
K_HOUR 425
K_MINUTE 429

FIG. 4

	COLUMN 1 DEVICE SECRET	COLUMN 2 EVENT STATE DATA	COLUMN 3 ACTION	COLUMN 4 OUTPUT
T_1	Initial - A_1	Initial - B_1	-	-
T_2	A_2	B_2	TIME	-
T_3	A_2	B_2	PIN ENTRY	ID AUTH CODE (A_2, B_2)
T_4	A_3	B_3	TIME	-
T_5	A_3	B_4	EVENT REGISTERED	-
T_6	A_4	B_5	TIME	-
T_7	A_4	B_5	PIN ENTRY	ID AUTH CODE (A_4, B_5)

FIG.5

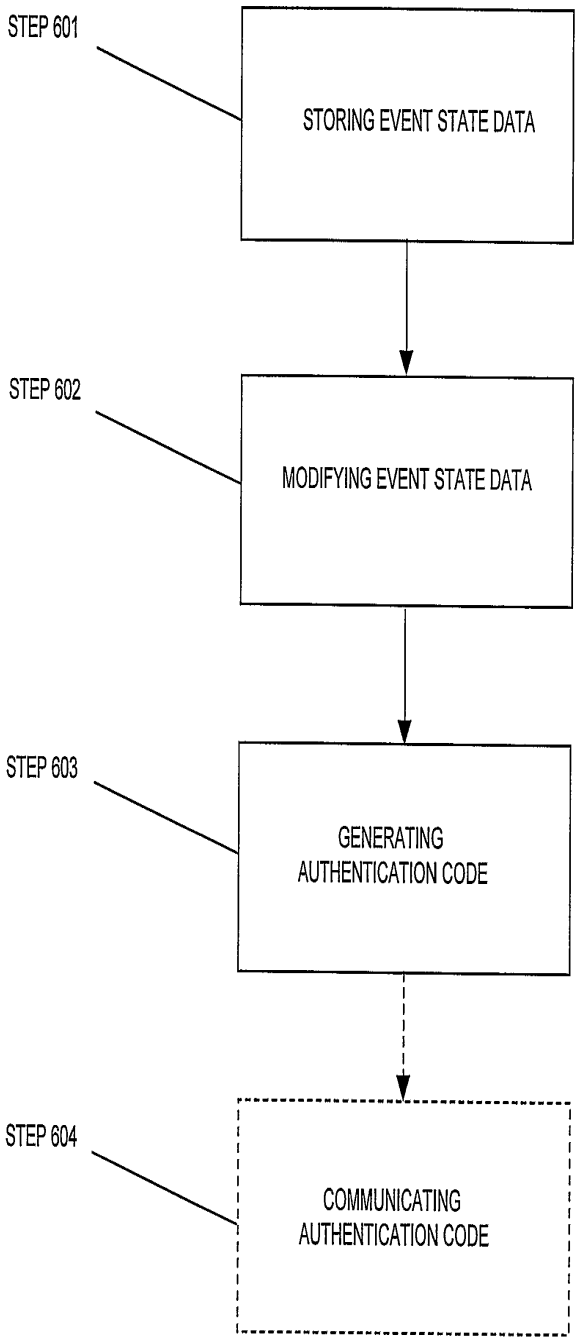

STEP 601
STORING EVENT STATE DATA
STEP 602
MODIFYING EVENT STATE DATA
STEP 603
GENERATING AUTHENTICATION CODE
STEP 604
COMMUNICATING AUTHENTICATION CODE

FIG. 6

SECRET
(K)
DYNAMIC
VALUE
(T)
EVENT STATE DATA
SECURITY
ENHANCING
SECRET
(C)
STATUS
COUNTER
SECRET
(X)
AUTHENTICATION
VALUE
(S)
EVENT
CODE
(F)
AUTHENTICATION
CODE
(A)

FIG. 7

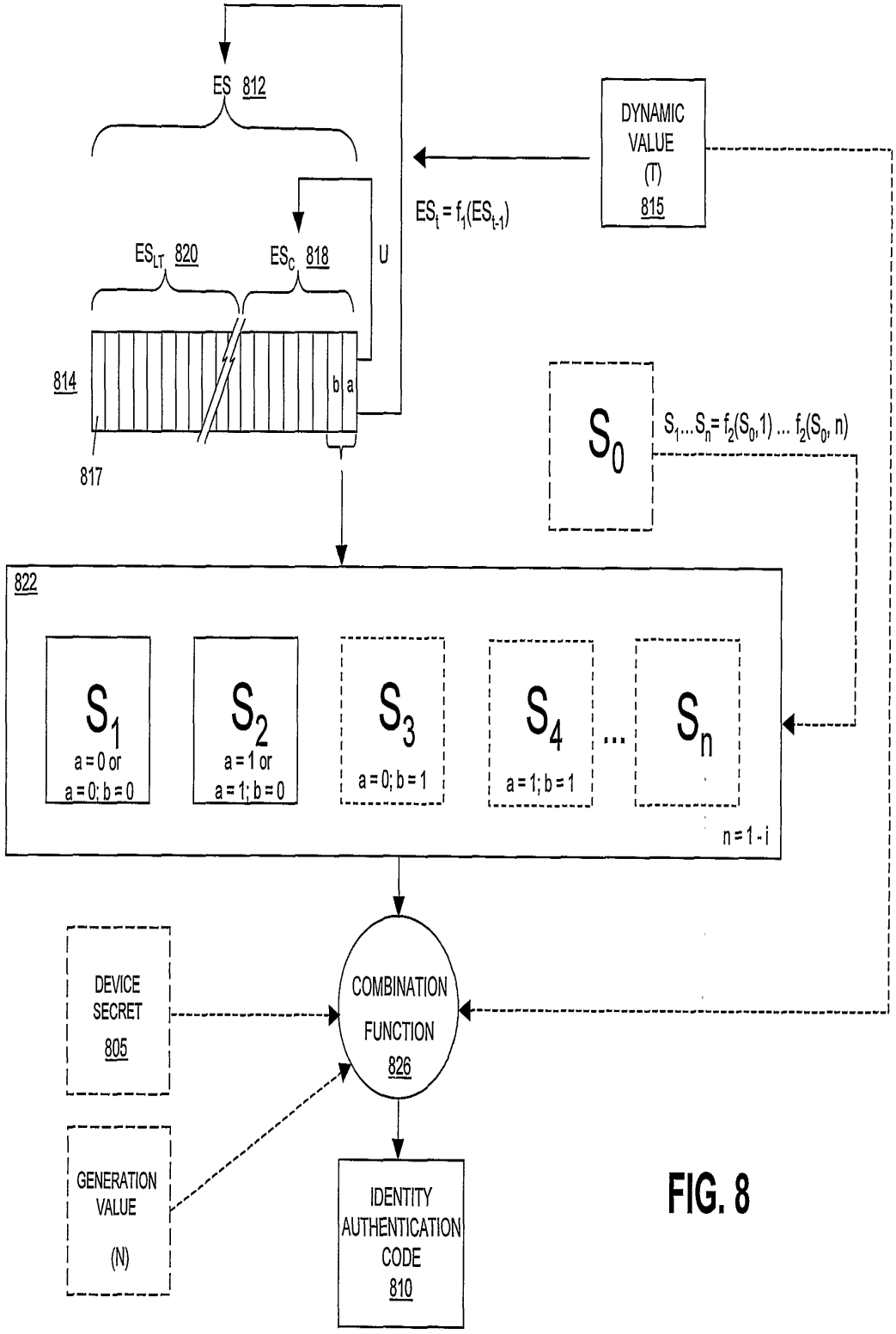

ES 812
DYNAMIC VALUE (T) 815
$ES_t = f_1(ES_{t-1})$
ES_{LT} 820
ES_C 818
U
814
b a
817
S_0
$S_1 \ldots S_n = f_2(S_0, 1) \ldots f_2(S_0, n)$
822
S_1 a = 0 or a = 0; b = 0
S_2 a = 1 or a = 1; b = 0
S_3 a = 0; b = 1
S_4 a = 1; b = 1
S_n
n = 1 - i
DEVICE SECRET 805
COMBINATION FUNCTION 826
GENERATION VALUE (N)
IDENTITY AUTHENTICATION CODE 810

FIG. 8

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 January 2005 (06.01.2005)

PCT

(10) International Publication Number
WO 2005/001751 A1

(51) International Patent Classification[7]: G06K 9/00, H04K 1/00, H04L 9/00

(21) International Application Number: PCT/US2004/017545

(22) International Filing Date: 2 June 2004 (02.06.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/475,242 2 June 2003 (02.06.2003) US

(71) Applicant *(for all designated States except US)*: **REGENTS OF THE UNIVERSITY OF CALIFORNIA** [US/US]; University of California, Los Angeles, 10920 Wilshire Blvd, Suite 1200, Los Angeles, CA 90024-1406 (US).

(72) Inventors; and

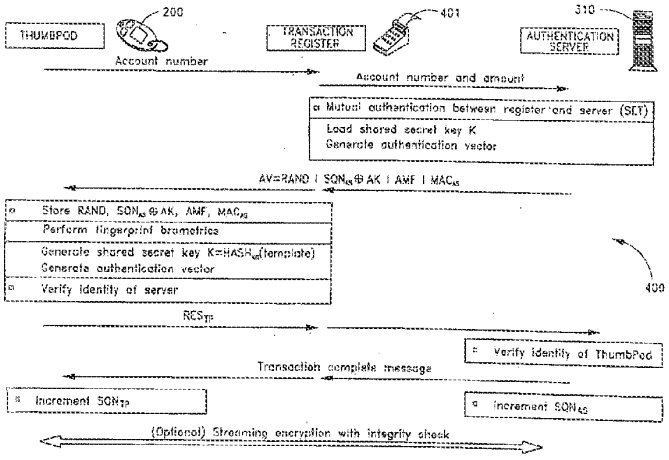
(75) Inventors/Applicants *(for US only)*: **VERBAUWHEDE, Ingrid, M.** [—/US]; 1123 23rd Street, #C, Santa Monica, CA 90403 (US). **SCHAUMONT, Patrick, R.** [—/US]; 10439 Holman Avenue, Los Angeles, CA 90024 (US). **HWANG, David, D.** [—/US]; 540 Kelton Avenue, #205, Los Angeles, CA 90024 (US). **LAI, Bo-Cheng** [—/US]; 10125 Palms Boulevard, #204, Los Angeles, CA 90034 (US). **YANG, Shenglin** [—/US]; 3170 Sawtelle Boulevard, Apt. #203, Los Angeles, CA 90066 (US). **SAKIYAMA, Kazuo** [—/US]; 3200 Sawtelle Boulevard, Apt. #202, Los Angeles, CA 90066 (US). **FAN, Yi** [—/US]; 310 S. Kenmore Avenue, Apt. #202, Los Angeles, CA 90020 (US). **HODJAT, Alireza** [—/US]; 2624 Kansan Avenue, #14, Santa Monica, CA 90404 (US).

(74) Agent: **DELANEY, Karoline, A.**; KNOBBE, MARTENS, OLSON AND BEAR, LLP, 2040 Main Street, Fourteenth Floor, Irvine, CA 92614 (US).

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

[Continued on next page]

(54) Title: SYSTEM FOR BIOMETRIC SIGNAL PROCESSING WITH HARDWARE AND SOFTWARE ACCELARATION



(57) Abstract: A secure embedded system that uses cryptographic and biometric signal processing acceleration is described. In one embodiment, the secure embedded system is configured as a wireless pay-point protocol for brick-and-mortar and e-commerce applications in which biometric information is localized and does not require transmission of biometric data for authentication. In one embodiment, a key-generation function uses a dynamic key generator and static biometric components. In one embodiment, an embedded system design methodology provides hardware and software acceleration transparency.

WO 2005/001751 A1

Apple 1107

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

Declaration under Rule 4.17:

---- *of inventorship (Rule 4.17(iv)) for US only*

Published:

— *with international search report*

---- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

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

SYSTEM FOR BIOMETRIC SIGNAL PROCESSING WITH HARDWARE AND SOFTWARE ACCELERATION

Reference to Related Application

[0001] The present application claims priority benefit if U.S. Provisional Application No. 60/475,242, filed June 2, 2003, titled "SYSTEM FOR BIOMETRIC SIGNAL PROCESSING WITH HARDWARE AND SOFTWARE ACCELERATION," the entire contents of which is hereby incorporated by reference.

Government Interest Statement

Portions of the subject matter of this application were invented under a contract with an agency of the United States Government, under NSF contract No. 0098361.

Background

Field of the invention

[0002] The present invention relates to systems using biometric signal processing for authentication in connection with a secure communication protocol.

Description of the Related Art

[0003] In February 2003, a computer hacker breached the security systems of Visa and MasterCard and accessed 5.6 million valid account numbers, which represents approximately 1% of all 574 million valid account numbers in the United States. Though the accounts were not used fraudulently, a burdensome recall and replacement of valid cards throughout many financial institutions was required. On the Internet, a number of black-market sites sell active credit card account numbers and expiration dates for a modest price. In brick-and-mortar credit card scenarios, photograph identification or signatures are inconsistently checked in normal purchases; hence, fraudulent transactions are commonplace. These situations are just a few which expose the current flaw in traditional transaction

protocols, which is mainly a flaw in authentication. Identity theft results in losses of well over a billion dollars a year for credit card issuers, and is even more widespread since the advent of e-commerce on the Internet. The primary reason for the continued success of identity theft is the lack of the ability to prove that an account is used by the genuine, authorized, consumer.

Summary

[0004] The present invention solves these and other problems by providing a secure embedded system that uses cryptographic and biometric signal processing to provide identity authentication. In one embodiment, the secure embedded system is configured as a wireless pay-point device, called a thumbpod, for brick-and-mortar and/or e-commerce applications. In one embodiment, the thumbpod localizes a sensitive biometric template and does not require transmission of biometric data for authentication. In one embodiment, a key-generation function uses a dynamic key generator and static biometric components. An embedded system design methodology known as hardware/software acceleration transparency is provided to improve performance of the thumbpod. In one embodiment, acceleration transparency is provided in a systematic method to accelerate Java functions in both software and hardware of, for example, an encryption function.

[0005] In one embodiment, the thumbpod is designed as a secure embedded device that provides a protocol for wireless pay-point transactions in a secure manner. The protocol uses secure cryptographic primitives as well as biometric authentication techniques. The security protocol used in the thumbpod is based on a protocol that uses the thumbpod as an interface between an authentication server and a user.

[0006] In one embodiment, the thumbpod includes a microcontroller, a fingerprint image sensor, signal processing hardware acceleration, cryptographic hardware acceleration, and a memory module enclosed within a form factor similar to an automobile keychain transmitter. The thumbpod provides flexible communication via ports, such as, for example, a port for wireless communication and/or a wired port for fast wire-line communication. The wireless port can be, for example, an infrared port, a radio-frequency port, an inductive coupling port, a capacitive coupling port, a Bluetooth port, a wireless Ethernet port, etc. The

wired port can be, for example, a USB port, a firewire port, a serial port, an Ethernet port, etc. The thumbpod can be used for a wide variety of authentication-related transactions, such as, for example, wireless credit card payments, keychain flash memory replacement, universal key functionality (house, car, office), storage of sensitive medical data, IR secure printing, etc.

[0007] In one embodiment, a security protocol binds the user to the device through biometrics, combines biometrics and traditional security protocols, protects biometric data by keeping at least a portion of the biometric data in a protected form that does not leave the device, and provides that biometric calculations are provided on the device. In one embodiment, biometric algorithms are provided to fit a relatively constrained environment of embedded devices. In one embodiment, algorithms are provided in fixed point arithmetic. In one embodiment, memory storage optimization and hardware acceleration are provided by converting a least a portion of one or more software algorithms into hardware.

Brief Description of the Drawings

[0008] The various features of the present are described with reference to the following figures.

[0009] Figure 1 shows layers of an embedded security protocol system.

[0010] Figure 2 shows one embodiment of a thumbpod device.

[0011] Figure 3A is a block diagram of an authentication protocol having a relatively strong one-way authentication protocol between the server and the device and a relatively week security protocol between and the device and the user.

[0012] Figure 3B is a block diagram of an authentication protocol having a relatively strong two-way authentication protocol between the server and the device and a relatively strong security protocol between and the device and the user.

[0013] Figure 4 is a further block diagram of one embodiment of the authentication protocol shown in Figure 3B.

[0014] Figure 5 shows authentication protocol vector generation in the authentication server.

[0015] Figure 6 shows authentication vector generation in the thumbpod device of Figure 2.

[0016] Figure 7 shows generation of authentication functions F1-F5.

[0017] Figure 8 is a block diagram of the Rijndael CBC-MAC algorithm.

[0018] Figure 9 is a block diagram of the Rijndael OFB-Counter algorithm.

[0019] Figure 10 is a block diagram of the NIST minutia extraction flow algorithm the fingerprint identification system.

[0020] Figure 11 shows window rotation in the fingerprint identification system.

[0021] Figure 12 shows an example of an original image in the fingerprint identification system.

[0022] Figure 13 shows minutiae points in the image of Figure 12 after binarization.

APPL-1002
APPLE INC. / Page 278 of 419

[0023] Figure 14 shows matching flow in the fingerprint identification system.

[0024] Figure 15 shows local features of fingerprint minutia.

[0025] Figure 16 is a chart showing the execution time for various operations in the minutia detection algorithm at the block diagram level.

[0026] Figure 17 is a chart showing the execution time for various operations in the minutia detection algorithm at the instruction level.

[0027] Figure 18 shows an example of the direction map.

[0028] Figure 19 shows the relationships between execution time, error rate, and ETH in the fingerprint identification system.

[0029] Figure 20 is a block diagram of a memory-mapped EFT accelerator.

[0030] Figure 21 is a chart showing execution time for different embodiments of the fingerprint identification system.

[0031] Figure 22 is a chart showing energy consumption for different embodiments of the fingerprint identification system.

[0032] Figure 23 shows profiling results for the baseline algorithm in the fingerprint identification system.

[0033] Figure 24 shows relationships between the pre-checking threshold and performance of the fingerprint identification system.

[0034] Figure 25A is a chart comparing the execution time for the baseline and the optimized fingerprint matching systems.

[0035] Figure 25B is a chart comparing the energy consumption for the baseline and the optimized fingerprint matching systems.

[0036] Figures 26A-26F show various embodiments of hardware or software acceleration transparency.

[0037] Figure 27 shows acceleration of the Rijndael algorithm using hardware and software acceleration.

[0038] Figure 28A is a block diagram showing a functional model of hardware/software accelerator design.

[0039] Figure 28B is a block diagram showing a benchmarking functional model of hardware/software accelerator design.

[0040] Figure 28C is a block diagram showing a transaction-level model of hardware/software accelerator design.

[0041] Figure 28D is a block diagram showing an embedded software implementation model functional model of hardware/software accelerator design for a personal computer implementation.

[0042] Figure 28E is a block diagram showing an embedded software implementation model of software accelerator design for a board-level implementation.

[0043] Figure 28F is a block diagram showing an embedded software implementation model of hardware/software accelerator design for a board-level implementation.

[0044] Figure 29(a) and (b) shows one embodiment of a software acceleration architecture.

Detailed Description

[0045] Figure 1 shows layers of an embedded security protocol system 100. At the highest level, the system 100 includes a protocol layer 101 that provides confidentiality and identify verification. An algorithm layer 102 is provided below the protocol layer 101. The algorithm layer 101 includes one or more algorithms, such as, for example, encryption algorithms (e.g., Kasumi, Rijndael, RC4, MD5, etc.), used by the protocol layer 101. In the present disclosure, the Rijndael algorithm is used by way of example of an encryption algorithm, and not by way of limitation. An architecture layer 103 is provided below the algorithm layer 102. In one embodiment, the architecture layer 103 includes a virtual machine, such as, for example, a JAVA virtual machine. A micro-architecture layer 104 is provided below the architecture layer 103. In one embodiment, the micro-architecture layer 104 includes one or more processor architectures. A circuit layer 105 is provided below the micro-architecture layer 104.

[0046] As security is only as strong as the weakest link, a breech in any of the abstraction layers 101-105 can compromise the entire security model. Hence design of the secure embedded system is based on a top-down design flow and security scrutiny at each abstraction level.

[0047] Figure 2 shows a thumbpod 200 as an embodiment of a device that is based on the security pyramid shown in Figure 1. The thumbpod 200, is configured as a keychain-type device that includes a biometric sensor 202, a communication port 204, and embedded hardware components. The sensor 202 obtains biometric identification data (e.g., fingerprint identification data, voice identification data, retina identification data, genetic

identification data, etc.) from a user. In an alternative embodiment, the thumbpod 200 includes a sensor 202 for obtaining identification data from a user, such as, for example, biometric identification data, password data, PIN data, Radio Frequency Identification Tag (RFID) data, etc. In one embodiment, the sensor 202 is a fingerprint sensor. In one embodiment, the sensor is an imaging device. In one embodiment, the sensor 202 includes a CMOS imaging device. A fingerprint device is used herein by way of example, and not by way of limitation.

[0048] The communication port 204 can include a wireless port and/or a wired port to provide flexible communication. In one embodiment, the port 204 includes a wireless port, such as, for example, an infrared port, a radio-frequency port, an inductive coupling port, a capacitive coupling port, a Bluetooth port, a wireless Ethernet port, etc. In one embodiment, the port 204 includes a wired port, such as, for example, a USB port, a firewire port, a serial port, an Ethernet port, a PCMCIA port, a flash memory port, etc.

[0049] The thumbpod 200 is configured to be used in connection with a security protocol (as described in connection with Figures 3 and 4 to provide safe use of biometric sensor data. The biometric data does not leave the thumbpod 200 but it is used with a split-key generation function to protect the data. The thumbpod 200 provides a verifiable bond between a user and the thumbpod 200 based on biometric sensor data. The thumbpod can be used for a wide variety of authentication-related transactions, such as, for example, wireless credit card payments, keychain flash memory replacement, universal key functionality (house, car, office), storage of sensitive medical data, IR secure printing, etc.

[0050] The thumbpod 200 uses biometrics to bind a user to an identification code, such as, for example, an account number, an access code, a password, an the like (hereinafter referred to generically as an account number). At each transaction, the user's biometric data (e.g., fingerprint) is used to digitally sign a transaction as proof of identification. This fingerprint is digitally verified by an authentication server. The protocol used by the thumbpod and the authentication server ensure that sensitive biometric data is not transmitted

freely, particularly across wireless or other insecure channels. The protocol described below provides an authentication scheme in which no actual biometric data is transmitted and no biometric data is stored at the server. Rather, biometric information is captured in the thumbpod 200 and used to generate a key K (which is stored at the authentication server) for symmetric-key encryption. This key is used to encrypt challenge and response functions, based on a random number, which are in turn transmitted across the wireless channel.

[0051] Figure 3A is a block diagram of an authentication protocol 300 that uses a relatively strong one-way authentication protocol between an authentication server 310 and an authentication device 311, and a relatively week security protocol between and the device 311 and a user 303, as is currently used in traditional credit card authorization systems. In the traditional credit card authentication scheme, a server authenticates merely with a physical credit card (or more specifically, with an account number stored on a magnetic strip of a credit card). In an e-commerce scenario, a physical card is not required—an account number and expiration date are sufficient. The traditional schemes provide a two-fold authentication: 1) the server authenticates the credit device, and 2) the server (nominally) authenticates the ownership of the card. A significant problem with the current credit card-type transaction protocols is the weak authentication tie between the user and the transaction device (the credit card). It is often the case that in brick-and-mortar commerce, proof of authentication is not required. In ATM transactions, a personal identification number (PIN) may tie a user to the card. However, PIN numbers do not provide high levels of security. PIN number are often easily broken or repetitive numbers, written on the back of cards, forgotten, etc.

[0052] Figure 3B is a high-level block diagram of an authentication protocol 301 used in connection with the thumbpod 200. The authentication protocol 301 uses a relatively strong two-way authentication protocol between the authentication server 310 and the authentication device (e.g., the thumbpod 200), and a relatively strong authentication protocol (e.g., biometric authentication) between and the thumbpod 200 and the user 303.

[0053] The protocol 301 is an example of a complex application in which thumbpod 200 uses both cryptographic and signal processing functionality. There are various other protocols for other applications for the thumbpod 200 that share one or both of the common denominators of cryptography and biometric signal processing. Other applications include encryption/decryption and/or verification for audio and video systems.

[0054] Figure 4 shows an example system 400 that uses the authentication protocol 301 and a flow diagram of the authentication protocol 301. The system 400 includes the thumbpod 200, a merchant's transaction register 401, and the authentication server 310. The authentication protocol 301 can be used in connection with a brick-and-mortar pay-point transaction, an e-commerce transaction, a computer login transaction, or any other transaction the requires authentication.

[0055] In the protocol 301, the thumbpod 200 sends an account number to the transaction register 401. The transaction register 401 then sends the account number and data regarding the transaction (e.g., a transaction dollar amount), to the server 310. The transaction register 401 and the server 310 provide mutual authentication through standard protocols, such as, for example, the SET protocol. The server 310 uses the account number to look up the identity of the thumbpod 200 and to obtain a secret key known to the thumbpod 200. The server 310 generates a first authentication vector and encrypts the first authentication vector using the secret key. The encrypted first authentication vector is then sent to the transaction register 401. The transaction register forwards the first authentication vector to the thumbpod 200. The thumbpod 200 decrypts the first authentication vector and verifies the identity of the authentication server 310. The thumbpod also authenticates the user and generates a second authentication vector. The second authentication vector is encrypted using the secret key. The thumbpod 200 returns the authentication vector to the transaction register 401, which forwards the second authentication vector to the authentication server 310. The authentication server 310 decrypts the second authentication vector and verifies the identity of the thumbpod 200. Once the identity of the thumbpod has been verified, the authentication server 310 sends a "transaction complete" message to the transaction register 401. The transaction forwards

the transaction complete message to the thumbpod 200, which then increments a transaction counter. In one embodiment, streaming encryption is provided between the thumbpod 200, the transaction register 401, and/or the server 310.

[0056] In order to make a transaction at the transaction register 401, the user 303 uses the thumbpod wireless port 204 to initiate communication with the register. Challenge and response functions are negotiated between the user 303 and the server 310, routed through the merchant's register 410 (which cannot interpret the data because it does not posses secret keys known to the thumbpod 200 and the server 310). In the course of the authentication protocol, the user 303 places his/her finger on the fingerprint sensor 202 to provide identity verification. This information is processed within the thumbpod 200 and, if a match is made, cryptographic hash functions and keys are generated using encryption algorithms and the protocol continues to its completion.

[0057] In the protocol 301, three items are used for valid authentication transactions: 1) the account number stored in the thumbpod 200, 2) the thumbpod 200 itself (which generates the secret key K), and 3) the correct biometric component (e.g., a finger, a retina, etc.) for live-scan sensing by the sensor 202. These three elements provide a strong tie between the user 310 and the thumbpod 200 account number. In an e-commerce situation, merely having a stolen account number (and expiration date) would be insufficient to make a transaction. Likewise, an account number and a stolen thumbpod 200 are also insufficient. All three components are required to make a valid transaction.

[0058] In the protocol 301 a threefold-authentication takes place: 1) the server 310 authenticates the thumbpod 200, 2) the thumbpod 200 authenticates the server 310 (and transaction register 410), and 3) the thumbpod 200 authenticates the user 310. Unlike traditional schemes, the user 303 authenticates the server and the transaction register 401, providing protection against fraudulent or malicious merchants. Hence, the protocol retains the advantages of the current credit card-type protocols, while supplementing the protocols with stronger security, transaction device-to-user binding, and authentication directionality.

APPL-1002
APPLE INC. / Page 285 of 419

Other advantages of the protocol 301 include fraud detection as well as authentication at each transaction.

[0059] As shown in Figure 4, the thumbpod 200 begins the transaction by transmitting the user's account identification to the merchant's transaction register 401. The transaction register 401 authenticates with the authentication server using conventional protocols. Note that the protocol 301 need not replace current protocols. Rather, the protocol 301 supplements the current protocols with an additional layer of encryption-based authentication. The transaction register 401 transmits the account number and the transaction amount to the authentication server 310.

[0060] The server 310 begins its side of the authentication process by loading the user's secret key *K*, which is shared only between the server 310 and the thumbpod 200. In one embodiment, the secret key is at least 128 bits. The server 310 also loads a user's counter value SQN_{AS} and an institution authentication parameter AMF. In one embodiment, the counter value SQN_{AS} is at least 48 bits, and the institution authentication parameter AMF is at least a 16 bits. The counter value SQN_{AS} is stored both on the server and on the thumbpod 200 and is used to prevent replay attacks. The server 310 loads and encrypts an operator code OP, producing OP_C (which can be optionally pre-stored). In one embodiment, the operator code OP is at least 128 bits. Finally, the server 310 generates a random value RAND and uses K with Rijndael primitives to generate a set of authentication parameters for the specific transaction. In one embodiment, RAND is at least 128 bits. The authentication parameters include:

- MAC_{AS}: a message authentication code of the server to prove its identity to the thumbpod 200 (in one embodiment, the MAC_{AS} is at least 64-bits).
- $XRES_{AS}$: an expected response of the thumbpod 200 to prove its identity to the server (in one embodiment, $XRES_{AS}$ is at least 64 bits).
- AK: an anonymity key to mask the counter value CTR_{AS} for transmission (in one embodiment, AK is at least 48 bits).

- CK (optional): a cipher key to allow for streaming encryption after authentication is performed (in one embodiment, CK is at least 128 bits).
- IK(optional): an integrity key allowing for data integrity and origin authentication of streaming encryption data (in one embodiment, IK is at least 128 bits).

[0061] After the above authentication parameters are generated, the server 310 transmits a subset of the authentication parameters—the authentication vector—to the transaction register, which forwards the vector to the Thumbpod 200. The authentication vector includes:

- RAND;
- SQN_{AS} : the counter value of the server masked by the anonymity key;
- AMF: the institution authentication parameter; and
- MAC_{AS}: the message authentication code of the server to prove its identity to the thumbpod 200.

[0062] As in 3GPP authentication, the authentication between the thumbpod 200 and the server 310 is a mutual authentication based on the shared secret key K. The random session value RAND is coupled with K to provide the two primary challenge/response vectors: MAC_{AS} and RES_{TP}. The MAC_{AS} vector proves the identity of the server 310 to the thumbpod 200. Only the server 310 with the precise value of K (and the current random session value RAND) will be able to produce the proper MAC_{AS}. When the thumbpod 200 verifies this value by comparison with its generated expected value of $XMAC_{TP}$ (based on K and RAND) it determines whether the proper key K was used, and hence whether the server 310 is genuine. The same argument holds for the RES_{TP} vector, which is used to verify the identity of the thumbpod 200 to the server by comparison with $XRES_{AS}$. When both challenge/response values are verified, then mutual authentication is assured. The random number RAND and the sequence number $SQN_{TP/AS}$ are used to prevent replay attacks on previously-used authentication vectors obtained through eavesdropping on the channel. Since the sequence number follows a deterministic pattern (bit increment at each transaction), it is

masked by a one-use anonymity key AK as it is transmitted over the channel to prevent smart replay attacks.

[0063] At this point, the protocol 301 enters into a biometric authentication portion which differs from 3GPP or other wireless authentication protocols. The thumbpod 200 stores the authentication vector and begins biometric authentication by requesting that the user 303 to provide biometric data (e.g., place his/her finger on the fingerprint sensor 202). The Thumbpod 200 performs imaging, feature extraction, matching, and decision. During imaging, the thumbpod 200 images fingerprint to produce a bitmap of raw data. In one embodiment, the bitmap is at least 128 x 128 8-bit grayscale. During feature extraction, the thumbpod 200 processes the raw data, enhances the image, and extracts the minutiae types (ridges, bifurcations) and locations of the candidate fingerprint. During the matching process, the thumbpod 200 loads a stored fingerprint template and performs a matching function to produce a match score. During the decision process, the thumbpod 200, using the match score, decides if the candidate fingerprint is a match to the template.

[0064] If the algorithm detects an incorrect match, an error vector is transmitted to the server 310 and the protocol 301 is terminated. If the algorithm detects a match, the authentication protocol 301 continues. Using Rijndael in CBC-MAC mode, the shared secret key K is created by hashing the fingerprint template using a pre-stored 128-b key generator value KG according to $K = HASH_{KG}(template)$. (Alternatively, the value of K can also be pre-stored in the embedded device.)

[0065] In one embodiment, after loading the received values of RAND and AMF, the thumbpod 200 loads OP and uses the secret key K and Rijndael primitives to generate:

- OP_C: an encrypted operator code (optionally pre-stored). In one embodiment OP_C is at least 128-bits.
- AK: an anonymity key to unmask the counter value CTR_{AS}. In one embodiment AK is at least 128 bits.

- CTR_{AS}: a counter value of the server. In one embodiment CTR_{AS} is at least 48 bits.
- $XMAC_{TP}$: an expected message authentication code of the server to prove its identity to the thumbpod 200. In one embodiment $XMAC_{TP}$ is at least 64 bits.
- RES_{TP}: a response of the Thumbpod 200 to prove its identity to the server. In one embodiment RES_{TP} is at least 64 bits.
- CK (optional): a cipher key to allow for streaming encryption after authentication is performed. In one embodiment CK is at least 128 bits.
- IK (optional): an integrity key to allow for optional data integrity and origin authentication of streaming encryption data. In one embodiment IK is at least 128 bits.

[0066] If the message authentication code generated by the server (MAC_{AS}) is equal to the message authentication code generated by the thumbpod 200 ($XMAC_{TP}$), then the identity of the server 310 is authenticated. If they are unequal, then the user immediately recognizes that either the transaction register or the server is fraudulent.

[0067] If the counters of the server 310 and the thumbpod 200 are synchronized, then the process continues. If the counters are not synchronized but the MAC test passes, the system enters into re-synchronization mode to restore synchronization.

[0068] If the two authentication tests are passed, the thumbpod 200 sends a response vector RES_{TP} to the transaction register 401, which forwards this vector to the authentication server 310.

[0069] To complete the protocol, the authentication server 310 verifies that $XRES_{AS} = RES_{TP}$. If the values are not equal, it immediately indicates a fraudulent user or fraudulent thumbpod 200, allowing the server 310 to act accordingly. If these values are equal, then the identities of the thumbpod 200 and the user 310 are verified by the server 310. Hence, the protocol 301 provides mutual authentication between the server and the thumbpod

200. After verification of the user's identity, the server 310 increments its local counter variable SQN_{AS} and sends a transaction-complete vector to the transaction register 401. The register 401 then completes the transaction by printing a receipt and forwarding the transaction complete vector to the thumbpod 200. The thumbpod 200 increments its local counter variable SQN_{TP} to conclude the authentication protocol 301.

[0070] Four functions require a relatively large amount of computation in the thumbpod 200: 1) authentication vector generation, 2) feature extraction, 3) template matching, and 4) the key generation hash function.

[0071] The protocol 301 and the thumbpod 200 can use any robust encryption method. In one embodiment, the cryptographic engine used in the thumbpod 200 is the Rijndael algorithm (e.g., using a 128-b key and 128-b data), otherwise known as the Advanced Encryption Standard (AES). In one embodiment, Rijndael was chosen for security considerations and the absence of any known vulnerabilities to attack. The Rijndael kernel is used in three configurations: ECB, CBC-MAC, and OFB/Counter for optional streaming encryption applications.

[0072] In one embodiment, the generation of authentication vectors in the server 310 is shown in Figure 5, and the generation of authentication vectors in the thumbpod is shown in Figure 6. Rijndael EBC mode is used to generate the authentication vectors in both the authentication server 310 and in the thumbpod 200, as described above and based on the 3GPP authentication protocol. After loading the particular initialization values, the following functions are used to extract the vector components:

- f1: generation of MAC_{AS} / $XMAC_{TP}$ message authentication code.
- f2: generation of RES_{TP} / $XRES_{AS}$ response.
- f3: (optional) generation of CK cipher key for streaming encryption.
- f4: (optional) generation of IK integrity key for integrity protection of streaming encryption data.
- f5: generation of AK anonymity key.

- f1* / f5*: generation of vectors for re-synchronization.

[0073] A closer examination of the functions f1-f5 is provided in Figure 7. The functions primarily encrypt the random value RAND using Rijndael ECB modules (with the secret key K) and wrap the Rijndael engine with various XOR modules and fixed rotations. In Figure 7 the variables c1-c5 and r1-r5 are constant-bit vectors and the OP_C value is the operator code encrypted by the secret key K. The generation of one set of authentication vectors involves six (seven including the encryption of OP_C) iterations of the Rijndael ECB engine.

[0074] Figure 8 is a block diagram of the Rijndael CBC-MAC algorithm. Rijndael is used in a variant of CBC-MAC mode to generate the keyed-hash function K = $HASH_{KG}$(template), as seen in Figure 9. The key generation value KG is used as the key for the Rijndael core. In one embodiment, the fingerprint template (5,120 bytes) is loaded as the input value to the encryption module 128 bits at a time. The 128 bit segment is encrypted and the output is both forwarded to be XOR'd with the next template segment as well as the next encryption output, a technique known as cipher block chaining (CBC). After the final template segment, the 128 bit value is encrypted once again with a special key (KG XOR'd with a string of hexadecimal A = 1010|1010|1010... values) and the output value is the message authentication code (MAC), otherwise known as a keyed-hash (to avoid ambiguity with the aforementioned MAC value). The CBC-MAC function is invoked for 40 + 1 iterations in order to hash the entire fingerprint template. The same function is used with the integrity key IK in order to provide integrity protection of messages send with streaming encryption.

[0075] Figure 9 is a block diagram of the Rijndael OFB-Counter algorithm. For applications which require high-speed transmission and encryption of data, the Rijndael core is configured as a keystream generator to form a stream cipher, as seen in Figure 9. The keystream is XOR'd with the plaintext data to be encrypted, producing a ciphertext stream which is sent over an insecure channel. At the server side, the same keystream is produced

and XOR'd with the ciphertext to produce the original plaintext. The keystream generator functions as follows. First an initialization vector is created, which is composed of the sequence number SQN concatenated with a direction bit (1 for uplink, 0 for downlink), followed by padding zeroes. The cipher key CK (generated during authentication) is XOR'd with a string of hexadecimal values of value 5 = 0101|0101|... and used as a key to encrypt the initialization vector. The ensuing value is a constant register used as a data kernel to drive the stream cipher. After the required keystream length is determined, the length is divided into a number of 128 bit blocks. Each keystream block is formed by XORing the constant register with the previous encryption output (output feedback—OFB) and with a counter module, which increments at each iteration. The keystream is then XOR'd with the plaintext block to produce a 128 bit block of ciphertext. The final XOR of plaintext utilizes only the required number of bits, which is maximally 128 bits. In one embodiment, a single Rijndael cryptographic co-processor described below is provided for the three Rijndael configurations (ECB, CBC-MAC, OFB-Counter) and which is capable of being configured in each of the modes.

[0076] The protocol 301 is resistant or immune to the following cryptographic attacks: false register or false authentication server attack, stolen account number authentication attack, stolen account number synchronization attack, multiple synchronization attempts attack, stolen thumbpod attack, timeout attack, and incorrect data format transmission attack.

[0077] One aspect of the protocol 301 is the key generation function, which traverses security issues found in prior art biometric systems. A deficiency with biometrics in general is the issue of true identity theft: once a biometric identity (fingerprint, iris scan, etc.) is stolen, it is forever compromised, as a person possesses only a finite number of biometric templates. Although the thumbpod 200 can be housed in a tamper-proof casing, in one embodiment, the biometric template in the thumbpod is stored in a matter that prevents biometric data from being extracted from a stolen thumbpod 200.

[0078] In one embodiment, the thumbpod 301 uses a key generation concept whose security relies on both a static component (e.g., fingerprint template) and a dynamic component (a key generator variable), $K = HASH_{KG}(template)$. The shared secret key K is obtained by using a KG as the key for the Rijndael CBC-MAC engine, which operates on the user fingerprint template (5,120 bytes). This is similar, at least in principle, to a split-key security system, where two users possess separate, different keys and both keys are necessary to activate the device in question. Prior art biometric authentication systems merely require a template match in order to allow access, and a stolen template gives a criminal full access to the user's identity.

[0079] If the thumbpod 200 is lost or stolen, for precautionary measures, the user 303 would notify his/her financial institutions to request a new KG. After obtaining a new thumbpod 200 and enrolling a new template, a new secret key K would be generated, rendering the old key useless. Hence, in the case that a criminal obtains the user's fingerprint template from a thumbpod 200, the system is not entirely compromised due to the split-key key generation function. Another security benefit of the split-key generation model is that the server 310 never receives a copy of the user's template; it only stores the current secret key K. Due to the one-way property of hash functions, a stolen secret key K would not allow a criminal to re-generate the user's fingerprint template, even with knowledge of the key generator KG. This localization of sensitive data, rather than a widespread distribution of biometric data to each financial institution, allows for both psychological as well as cryptographic security.

[0080] Since the thumbpod 200 performs biometric identification, relatively computation-intensive biometric signal processing is typically required for both the feature extraction and matching algorithms. Designing for secure embedded systems results in partitioning which is based not only on communication-computation tradeoffs, but also partitioning which is based on security considerations. For example, though transmitting plaintext raw fingerprint data over the wireless channel would perhaps save energy in the thumbpod 200, it is insecure in that a passive attacker could listen on the channel and steal

the fingerprint data. The following section describes the security-based partitioning of the biometric functions used for the protocol 301.

[0081] For purposes of explanation, and not by way of limitation, the thumbpod 200 is described in terms of six subsystems: 1) Data collection subsystem, 2) Signal processing subsystem, 3) Matching subsystem, 4) Storage subsystem, 5) Decision subsystem, and 6) Communication subsystem.

[0082] In one embodiment, the data collection subsystem includes the sensor 202. In one embodiment, the sensor 202 includes an Authentec AF-2 CMOS imaging sensor. An alternative placement of the sensor is within the merchant's transaction register 401. However, studies have shown the relative ease in which a fingerprint can be stolen from a traditional CMOS sensor. Hence, placing a sensor on the transaction register 401 presents a security risk in that a fingerprint can be easily stolen by a malicious merchant or another consumer. As for the resolution of the CMOS sensor, it is chosen based on consideration of security strength and system cost. In some embodiments, the size of thumbpod 200 limits computational power and energy consumption, thus the collected data from CMOS sensor is sized to be precise enough to obtain a reasonable matching result but small enough to meet a system requirement in such an embedded system.

[0083] The raw data collected by the sensor 202 is processed to extract biometric features for identification. In a fingerprint verification system, the features to be extracted are the minutiae type (ridge or bifurcation) and the location of the minutiae via a process is known as feature extraction or minutiae detection. In one embodiment, the thumbpod 200 uses the standard floating-point C NIST detection algorithm.

[0084] In one embodiment, the thumbpod 200 uses a fixed-point variation of the well-known standard floating-point NIST detection algorithm. There are several steps in the minutiae extraction algorithm, many of which require significant signal processing. The first step is to generate image quality maps, which include the detection of fingerprint ridge

directions, image refinement, and detection of low contrast areas, which are assigned lower quality factors. A binarization of the image is generated, and the detection algorithm scans this binary image of the fingerprint to identify localized pixel patterns that indicate the ending (ridge) or splitting of a ridge (bifurcation). In one embodiment, a fixed-point refinement and table lookup of mathematical functions are used to reduce the computational and energy burdens.

[0085] The matching subsystem includes a set of algorithms used to match a pre-stored fingerprint template (or multiple fingerprint templates) with a candidate fingerprint obtained from the sensor. After extracting the minutiae of the fingerprint, two steps are used to estimate the similarity of the input minutiae set and the template minutiae set. The first step is to discover the correspondence of these two minutiae sets. For each minutia, the distance and relative direction to its neighborhood is taken as its local structure. Since this local structure is rotation and translation invariant, it is used to choose the corresponding pair in the input and template minutiae sets. The second step is to align the other minutiae by converting them to a polar coordinate system based on the corresponding pair, then computing how similar the overall minutiae distributions are in the input pattern and template pattern. The total similarity is represented by matching score. For security reasons, the matching algorithm is embedded within the thumbpod 200. Thus, sensitive minutiae data is not required to be transmitted over the channel.

[0086] The storage of the fingerprint template is also partitioned onto the thumbpod 200. The template is stored on-device in order to localize the most sensitive information in the entire system—the user's fingerprint information. If the template is distributed to various financial institutions, a breech in only one system would cause a loss of the user's template data. The aforementioned split-key generation function, coupled with the template storage on the thumbpod 200, is used to address this security issue.

[0087] The decision subsystem receives the results of the matching algorithm and makes a decision based on a pre-defined correlation score

APPL-1002
APPLE INC. / Page 295 of 419

[0088] Since the biometric subsystems are embedded within the thumbpod 200 device, it allows for the communication subsystem to transmit data across an insecure wireless channel. The only unencrypted sensitive data sent over the channel is the initial account information required to begin the authentication protocol. All other transmitted information is either encrypted or irreversible (one-way hash values used for authentication verification).

[0089] The aggregate result of this system partitioning allows for two unique system characteristics. First, the protocol describes a biometric authentication system in which no biometric information is transmitted across any medium, wireless or wired. Second, as previously mentioned, the biometric data is stored only in the thumbpod 200 and not in any financial institution server. The localization of sensitive data minimizes the cost of breeches in the entire security context.

Fingerprint Identification

[0090] In one embodiment, the algorithm used to extract minutiae of the fingerprint image is originated from NIST Fingerprint Image Software. Figure 10 is a block diagram showing the flow of the fingerprint identification algorithm. The fingerprint data is provide to a map generation block and to a binarization block 1005. The map generation block 1004 generates direction maps and quality maps that are provided to the binarization block 1005. The binarization block 1005 generates a binarized image that is provided to a detection block 1006. The detection block 1006 identifies possible minutiae and provides the possible minutiae set to a removal block 1007. The removal block 1007 removes false minutiae from the set of possible minutiae and generates a final minutiae set.

[0091] The minutiae detection process is based on finding a directional ridge flow map. To get this map, the fingerprint image (e.g., 256 x 256 pixels) is first divided into a grid of blocks (e.g., 8 x 8 pixels). For each block, there is a surrounding window (e.g., 24 x 24 pixels) centered by this block. For each block, the surrounding window is rotated

incrementally and a DFT analysis is conducted at each orientation. In one embodiment, the number of orientation is set to 16, creating an increment in angle of 180°/16, i.e. 11.25°. Within an orientation, the pixels along each rotated row of the window are summed together, forming a vector of 24 pixel row sums. The 16 orientations produce 16 vectors of row sums, as shown in Figure 11.

[0092] The resonance coefficients produced by convolving each of the 16 row sum vectors with the 4 different discrete waveforms are stored and then analyzed. The dominant ridge flow direction for the block is determined by the orientation with the maximum waveform resonance calculated from Equation (1):

$$E(k,\theta)=\left|\sum_{n=0}^{23}\text{row\_sum}(n,\theta)W^{kn}\right|^2 \quad , \quad W=\exp\left(\frac{-j\pi}{16}\right) \qquad (1)$$
$$(k=1,\ 2,\ 3,\ 4)$$

[0093] Each pixel is assigned a binary value based on the ridge flow direction associated with the block to which the pixel belongs. Following the binarization 1005, the detection block 1006 scans the binary image of a fingerprint, identifying localized pixel patterns that indicate the ending or bifurcation of a ridge. Figures 12 and 13 show the original and binarized images respectively. By performing this scanning, minutiae candidates are identified. The removal block 1007 removes false minutiae.

[0094] After two minutiae sets (e.g., an input fingerprint image and a template fingerprint image, respectively) are extracted, the matching algorithm can be described. Figure 14 is a block diagram showing the matching process 1400 used to determine if there is a match between the two minutiae sets.

[0095] The first step 1401 in the algorithm 1400 is to find out the correspondence of these two minutiae sets. Each minutia, N, can be described by a feature vector: $N=(x,y,\varphi,t)$, where (x,y) is its coordinate, φ is the local ridge direction and t is the minutia type (ridge ending or bifurcation). However, x,y and φ cannot be directly used for matching

because they are dependent on the rotation and translation of the fingerprint. To solve this problem, it is useful to construct a rotation and translation invariant feature:

$$M = (d_1, d_2, \theta_1, \theta_2, \varphi_1, \varphi_2, n_1, n_2, t, t_1, t_2) \tag{2}$$

[0096] Fig. 15 graphically shows the details of this local feature, where $n_1 = 0$ and $n_2 = 1$. Assume $M_I(i)$ and $M_T(j)$ are the local feature vectors of the ith minutia of the input fingerprint and the jth minutia of the template fingerprint, respectively. A similarity level can be defined:

$$sl(i,j) = \begin{cases} 1 - \dfrac{|M_I(i) - M_T(j)|_W}{A}, if |M_I(i) - M_T(j)|_W < A(W) \; i = 1,2...p \quad j = 1,2...q \\ 0, otherwise \end{cases} \tag{3}$$

where p and q are the numbers of minutiae in the input fingerprint and the template fingerprint, respectively. $|M_I(i) - M_T(j)|_W$ is the weighted difference of $M_I(i)$ and $M_T(j)$. $A(W)$ is the threshold which is related to the weight vector W. Set $W = (1,1,8,8,8,8,3,3,1/3,1/3,1/3)$ and $A(W) = 55$. By searching of $sl(i,j)$, one pair (b_1, b_2) can be obtained so that $sl(b_1, b_2) = \max_{i,j}(sl(i,j))$.

[0097] The next step 1402 is to align the other minutiae by converting them to a polar coordinate system based on the corresponding pair (b_1, b_2). For minutia N, the new polar coordinate is $M^p = (r, \theta, \varphi)$, where

$$\begin{aligned} r &= \sqrt{(x - x_b)^2 + (y - y_b)^2} \\ \theta &= diff\left(\arctan\left(\frac{y - y_b}{x - x_b}\right), \varphi_b\right) \\ \varphi &= diff(\varphi, \varphi_b) \end{aligned} \tag{4}$$

[0098] The function $diff(\,)$ is the difference between two angles. Based on the aligned minutiae sets, we can compute the matching level of each minutia in the input fingerprint and each one in the template fingerprint:

$$ml(i,j)=\begin{cases}1-diff\_total/16, diff\_total<Bg\\ 0, otherwise\end{cases} \quad (5)$$

[0099] In Equation 5, $diff\_total=\left|M_I^P(i)-M_I^P(j)\right|_{WP}$. Bg is a bounding box where $Bg=(8,\pi/6,\pi/6)$ and $W^P=(1,8,8)$.

[0100] To avoid one minutia being used more than once for matching, $ml(i,j)$ is set to "0" if there is any k that make $ml(i,k)>ml(i,j)$ or $ml(k,j)>ml(i,j)$. Afterwards, the final matching score can be calculated by:

$$Ms=100\times\frac{\sum_{i,j}ml(i,j)}{\max(p,q)} \quad (6)$$

[0101] The algorithm 1400, provides fingerprint verification on thumbpod 200. In one embodiment, the sensor 202 used for fingerprint scanning has relatively small area (13 x 13 mm^2), so the performance is relatively strongly dependent on which part of the finger is captured by sensor. In one embodiment, the thumbpod 200 uses a two-template system to deal with the small sensor area. The fingerprint image sets (templates) used by the thumbpod 200 include 10 fingerprints per finger from 10 different fingers for a total of 100 fingerprint image templates. Each fingerprint is compared with every fingerprint template in pairs, and the two match scores from each pair are ported into a decide engine in order to get the final matching result. A total of 7,200 decisions involved for the matched case and a total of 81,000 decisions are involved for the mismatched case. The size of captured image is 256 x 256 pixels. In one embodiment, the thumbpod 200 provides a 0.5% FRR (False Rejected Rate) and a 0.01% FAR (False Accepted Rate).

[0102] Implementing the fingerprints minutiae detection and matching on an embedded platform such as the thumbpod 200 involves performance, speed, and low power tradeoffs, since the whole process needs to be finished in a relatively short time and the battery lifetime in such devices is limited.

APPL-1002
APPLE INC. / Page 299 of 419

[0103] Software optimization aims to reducing the cycle number of processors as well as the power consumption. To get better performance, the first step is to find out the hot-points of the system.

[0104] Figure 16 shows performance profiling results. The execution time of BINAR 1005 and DETECT 1006 are 11% and 12% of the total, respectively. They are not considered to be system bottlenecks. By contrast, MAPS 1004 occupies 74% of the total execution time. Therefore, the detail algorithm is checked to speedup the MAPS in the instruction level. Figure 17 shows the instruction-level profiling of MAPS. The number of instructions for multiply (Mult) and addition (Add) sum up to 56% of the total of the execution time due to the repetitive DFT calculation in creating the Direction Map. These Mult and Add instructions do not use any accesses to a memory. In other words, all accesses to the memory are included in Load and Store instructions that are 15% and 4%, as shown in Figure 17B. Based on the profiling results, software optimization and/or hardware acceleration should be considered for the DFT calculations in MAPS of the minutiae detection.

[0105] When considering the pattern of a fingerprint, the neighboring blocks tend to have a similar direction. In the example fingerprint map shown in Figure 18, the second row shows gradual change of the direction data, from 5 (left) to 12 (right). Taking advantage of the characteristic, the number of the DFT calculation is reduced significantly.

[0106] The first direction data, upper left in Fig. 18, is calculated in the same method as the original program. When deciding the direction of the right data, the DFT for θ = 4, 5, 6 is calculated first, because the result is most likely to be θ = 5. If the total energy for θ = 5 is greater than both its neighbors (θ = 4, 6) and a threshold value (E_{TH}), the direction data of θ = 5 is considered as the result. Otherwise, θ is incremented or decremented until the total energy for θ could have a peak with a greater value than E_{TH}. In other words, if the following three conditions are met, the calculation of the direction data is finished:

$$\sum_{k=1}^{4} E(k,\theta) > \sum_{k=1}^{4} E(k,\theta-1) \ [when\ \theta = 0,\ \theta - 1 = 15]$$
$$\sum_{k=1}^{4} E(k,\theta) > \sum_{k=1}^{4} E(k,\theta+1) \ [when\ \theta = 15,\ \theta + 1 = 0] \qquad (7)$$
$$\sum_{k=1}^{4} E(k,\theta) > E_{TH}$$

[0107] The execution speed as well as the matching error rate is measured when changing E_{TH} from 10M to 35M. The results are shown in Figure 19. From the figure 19, it is found that when E_{TH} is larger than 20, the error rate is within an acceptable range.

[0108] The software optimization reduces the number of DFT and results in significant speedup of the minutiae detection. However, there are still more than 7,000 times of DFT calculations for 256 x 256 pixels image, even if setting E_{TH} = 27M. Therefore, DFT hardware acceleration is useful in addition to the software optimization (Fig. 20).

[0109] The final specification of the accelerator is decided to deal with only Multiply/Accumulate (MAC) computations for sine and cosine part separately. In the Multiply operation, Canonic Signed Digit (CSD) is used for saving hardware resources. The energy calculation part is not included because it needs square operation of 16 bits data, which requires a general multiplier.

[0110] As a result, the execution time of the minutia detection is reduced to about 4 sec and 3 sec for E_{TH} is 27M and 10M, respectively as shown in Figure 21. In the meantime, the energy consumption is reduced from 5,187mJ to 2,500mJ in case of $E_{TH} = 27M$ (Figure 22).

[0111] Figure 23 shows the instruction cycle number distribution of the matching algorithm. Analysis of the profiling result shows that large part of the computation (52.2%) is used for finding the reference points for the input image and the template image. The reason for this is that when trying to find out which pair is the reference pair, thorough search

APPL-1002
APPLE INC. / Page 301 of 419

for each (i, j) pair is conducted, where $i = 1...p$ and $j = 1...q$. Totally $p \times q$ times of similarity level $sl(i, j)$ need to be calculated. To obtain all of these $sl(i, j)$, local feature vector M for each minutia in the input fingerprint as well as the template fingerprint needs to be calculated. Detailed study of one typical case shows that among all the $sl(i, j)$, 89% of them is "0", which means these pairs have total different neighborhoods and by no means can be the reference pair. In the process of calculating local feature vector M, the most time consuming part is finding the angles $(\theta_1, \theta_2, \varphi_1, \varphi_2)$ between the minutia and its neighborhood. To make the matching system more efficient, for those (i, j) pair whose $sl(i, j)$ is 0, an earlier decision about whether this is a reference pair can to be made.

[0112] Thus in one embodiment of the thumbpod 200, a modified algorithm is implemented. In the modified algorithm, before calculating the real local feature vector, one additional module called "Pre-Checking" is added. For each pair of minutiae, the weighted difference $|M_I(i) - M_T(j)|_W$ is calculated. In the Pre-Checking module, define $W = W_d = (1,1,0,0,0,0,0,0,0,0,0,0)$, which means only the distance information is needed in this procedure. If the weighted distance $|M_I(i) - M_T(j)|_{W_d}$ is within the pre-set threshold $M_{TH} = A(W_d)$, then the computation of the complete local feature vector needed; otherwise, the complete local feature is not needed.

[0113] The computation time after adding the Pre-Checking module and the result degrade depends on the value of the threshold M_{TH}. The relationship between M_{TH} and the performance is shown in Figure 24. As shown in Figure 24, M_{TH} @ 20 reduces computation time significantly, and yet provides a relatively low error rate.

[0114] During the regular process of setting flags to the possible multiple-used matching level $ml(i, j)$, one loop with a size of $p \times q \times (p + q)$ is used, where q and p is the number of minutiae in the input and template fingerprints, respectively. For a sample case, where $p = 37$ and $p = 39$, the instruction cycle number to finish this process is 1.4M (million), which is 38.9% of the entire matching process. The value $ml(i, j)$ is calculated from the local

feature difference of the ith minutia in the input fingerprint and the jth minutia in the template fingerprint. For most of the pairs (i, j), the local feature vector is so different that $ml(i, j)$ is 0, which means that it contributes nothing to the overall matching score. Based on this characteristic, the process of marking possible multiple-used $ml(i, j)$ can be optimized. Whenever the $ml(i, j)$ is "0", all the remaining comparison steps can be skipped and the process can advance straight to the next pair. After the above optimizations, the total cycle number is 1.34M. Hence the execution time is reduced to 26.80ms, as shown in Figure 25A and the energy consumption decreases from 37.88mJ to 15.14mJ , as shown in Figure 25B.

[0115] Thus, by implementing optimized minutiae detection and matching algorithms, as well as DFT hardware accelerator, execution time for the minutiae detection and matching process can be substantially reduced

Hardware/Software Acceleration Transparency

[0116] Figures 26A-26F show various embodiments of hardware or software acceleration transparency. In one embodiment, Java is used for its portability and security advantages. The issue of portability is important in embedded systems because of their high processor heterogeneity. Java's security advantages—such as a safe memory model, byte-code verification, cryptographic interface libraries, and the sandbox model—are important in the design of secure systems.

[0117] However, though advantages exist in these domains, Java is slower than its counterpart in C, and much slower than its counterpart in pure hardware. An example of Java's performance drawback can be seen in Table 1, where the 128 bit input, 128 bit key Rijndael function in Electronic Code Book (ECB) is performed. The Java (KVM) and C figures are on a 1 mW / 1 MHz Sparc processor. This configuration is used to emulate an embedded environment. The ASIC figures are based on an ASIC configured to implement the algorithm. As can be seen in the table, a hardware solution is five orders of magnitude superior in both performance and energy consumption (as measured in Gb/s per Watt). For

streaming encryption applications described in the previous section, pure embedded software solutions are inadequate. Hardware acceleration is used.

Platform	Throughput	Power	Gb/s / W
Java	450 bits/s	120 mW	0.00042
C	345 Kbits/s	120 mW	0.029
0.18 □m ASIC	2.29 Gb/s	56 mW	35.7

Table 1.

[0118] In order to incorporate software and hardware acceleration and simultaneously allow for incremental refinement in the design flow process, it is advantageous to use a technique called hardware software acceleration transparency. Hardware/software acceleration transparency is described below in further detail and involves three related items: 1) incremental acceleration, 2) Java function emulation, and 3) interface transparency.

[0119] The first principle of acceleration transparency is incremental refinement acceleration. In the example shown in Figure 26A, a Java application calls a Rijndael method. Based upon profiling results, if the performance of the pure Java solution is inadequate, it can be accelerated using a C function, as shown in Figure 26B. Rather than designing a custom interface to the C Rijndael function, as shown in the dotted line in Figure 26B, the application accesses the function through the Java Native Interface (JNI). If profiling and comparison with system specifications determine that hardware acceleration is used, a crypto-processor can be designed and interfaced to the Java application. However, this crypto-processor does not directly interface with the Java application (as shown in the dotted line in Figure 26C) but is accessed via assembly instructions by a skeletal C function, which itself is accessed by the Java application via the JNI. Though it seems wasteful in terms of overhead to use these interfaces, incremental refinement allows for a smoother design flow than creating custom

interfaces at each of the design levels. Methods for the design of domain-specific co-processors can be found in.

[0120] Hardware/software acceleration transparency also includes Java function emulation, a term used to describe the interface relationship between the Java application and the accelerated function. For example, a Java application wishes to access a Rijndael function via a function call rijndael(). From the above discussion, the Java application has one of three alternatives to obtain the implementation: 1) a Java function, 2) a C function, or 3) hardware acceleration.

[0121] Hardware/software acceleration transparency means that, to the Java application, each of these alternatives is accessed with the same Java function signature. In the pure Java case, this is already apparent: A Java Rijndael function is accessed by the Java application with a simple function call rijndael(). For C acceleration, interfaces are constructed such that the Java application can access the C Rijndael function with the same function call rijndael(). For hardware acceleration, HW/SW interfaces to the crypto-processor are designed such that Rijndael functionality is again accessed by the same function call rijndael(). In this way, from the Java application vantage point, each of these alternatives "looks" exactly the same. To the application, each of the three alternatives takes in the same input, produces the same output, and is accessed by the same Java function and hence functionally is the same, as seen in Figure 26D, Figure 26E, and Figure 26F.

[0122] Part of the previously mentioned Java function emulation is the concept of interface transparency. This is also illustrated in Figures 26A-F. Interface transparency means that to the Java application, all the interfaces in between it and the acceleration implementation are transparent. In other words, the Java application can directly "see" the acceleration implementation (which looks to it like a Java function) regardless of the number of interfaces. Interface transparency essentially raises co-processor control a number of abstraction layers directly to the Java application level.

APPL-1002
APPLE INC. / Page 305 of 419

[0123] The use of hardware/software acceleration transparency, allows the designer to build interfaces incrementally. Instead of tearing down the previous interface and starting from scratch at each abstraction level, the next interface incrementally refines the previously constructed interface. Thus, the interface design flow is smooth and continuous. Acceleration transparency allows for system performance modeling at each abstraction level. As each accelerated function is placed into the overall system, the hybrid system can be re-benchmarked and the performance gains ascertained. As the system progresses from software to hardware, the original Java application needs only minor modification. Using acceleration transparency implies that each of the acceleration modules "looks" like the initial Java function in the original application; hence, the original Java application can remain the same (or relatively unchanged) from the beginning functional simulation to the final HW/SW system implementation. Once the interface hierarchy is constructed, a new acceleration module can be appended to the system through the pre-designed interfaces. A system can thus be reconfigured in a systematic way.

[0124] The following example shows HW/SW acceleration transparency and gives performance measurements for interface overhead. The simulation environment used for the example includes a cycle-true LEON-Sparc simulator. C code is compiled with the GNU C compiler gcc V3.2 with full optimization (-O2). Java byte-code is interpreted on the KVM embedded virtual machine from the Java2 Micro Edition. Thus, cycle counts for Java are cycles of the target LEON-Sparc which runs KVM that in turn runs the Java program.

[0125] The example begins with the aforementioned interface specification of the Rijndael in Java and C. A 128-bit key and 128-bit data block are used in the example.

[0126] The intefaces are as follows:

- Java: int[] rijndael(int[] key, int []din)
- C: void rijndael(int din[4], int key[4], int dout[4])

[0127] A pure Java implementation for Rijndael on top of KVM takes 301,034 cycles, as shown in Figure 27. All numbers in the figure are for one iteration of the Rijndael

algorithm, starting from the Java function call. Startup overhead, such as setting up the C or Java runtime environments, is not included.

[0128] A first refinement to the pure Java model is to substitute the pure Java implementation with a native implementation in C. A native method in Java is shown in Figure 26A. The corresponding C implementation is shown in Figure 26B. A function renaming is used in order to reflect the position of the native method in the Java class hierarchy. The C implementation then can forward control to the implementation of the rijndael() function.

[0129] The rijndael() function of Figure 26B can, at first, call an implementation of the Rijndael algorithm in C. When the NIST reference code is used, the figures as shown in the second column of Figure 27 are obtained. There are 44,430 cycles per Rijndael call, of which 367 can be attributed to the interfacing part (Figure 26A and B) and the rest to native implementation. Overall a performance gain of 6.8X is seen.

[0130] The next step is to substitute the C implementation with a native hardware implementation of the Rijndael algorithm. A hardware coprocessor is used that completes a 128-bit encryption in 11 clock cycles. This hardware processor is interfaced to the co-processor interface of the Sparc, and programmed as shown in Figure 26C. The 128-bit key and data are provided with two double-word move instructions. In this case, the resulting performance was 903 cycles. Here, the interfaces turn out to consume the major part of the cycle budget. The actual encryption takes only 11 cycles; going from Java to hardware consumes 892 cycles. The performance gain in going from Java to hardware is now 333X.

[0131] While the performance gain of moving from Java to native implementation is substantial, it is not completely overhead-free. This overhead is primarily caused by moving data across the hierarchy levels in the model. This overhead can be reduced by treating data-flow and control-flow separately. In any case, the incremental refinement of the model is a major advantage from the design-flow point-of-view.

[0132] The design of the thumbpod 200 uses a number of abstraction levels, with each abstraction level based on design decisions and interface construction. The smooth transition from one model to another allows for successive refinement of the system. Figure 28A is a block diagram showing a functional model of hardware/software accelerator design. The functional model models the thumbpod functional protocol on a PC environment (e.g., Pentium processor) in Java. As shown in Figure 28A, this model includes an encryption function performed in Java. A C function is also used to perform fingerprint verification signal processing. A C function rather than Java is used here in order to incorporate the NIST standard fingerprint detection algorithms given in C code. This function interfaces with the application via JNI. Communication between modules (thumbpod 200, register 401, and authentication server 310) is performed in a sequential main method.

[0133] Figure 28B is a block diagram showing a benchmarking functional model of hardware/software accelerator design. In this abstraction level in Figure 28B the encryption function is accelerated as a C function for benchmarking purposes. An interface is constructed which allows the C encryption function to interface with the application via JNI. encryption performance measurements are compared with the functional model.

[0134] Figure 28C is a block diagram showing a transaction-level model of hardware/software accelerator design. In this abstraction level the communication between modules is modified to allow objects to communicate with one another in a transaction level manner, instead of being controlled by a sequential main method. The transaction-level applications communicate to one another via socket programming models.

[0135] Figure 28D is a block diagram showing an embedded software implementation model functional model of hardware/software accelerator design for a personal computer implementation. Since the goal of the project is to implement the thumbpod 200 on an embedded hardware platform, the next abstraction level is the embedded software implementation model. In this model, the thumbpod 200 application operates on

KVM (an embedded virtual machine) rather than JVM, and communicates with the accelerated C functions through a customized KNI (JNI for KVM) interface, rather than a standard JNI interface. In this model the effects of the constrained embedded environment can be ascertained.

[0136] Figure 28E is a block diagram showing an embedded software implementation model of software accelerator design for a board-level implementation. In this abstraction level, the thumbpod 200 application is moved entirely onto an embedded hardware platform. In one embodiment, the application runs on top of KVM operating on a C backbone on a LEON 32-b Sparc processor (FPGA). The acceleration continues to be performed in C. The FPGA board communicates with the PC via a UART and Java server proxy.

[0137] Figure 28F is a block diagram showing an embedded software implementation model of hardware/software accelerator design for a board-level implementation. In this abstraction level, hardware acceleration is introduced both for biometric signal processing and for encryption. The hardware co-processors (implemented within an FPGA) interface with the Java application via a C interface and KNI. This abstraction level demonstrates the applicability and performance of HW/SW acceleration transparency.

[0138] Figure 29 shows one embodiment of a thumbpod architecture. The software architecture is built upon an embedded Java virtual machine (KVM) which has been extended with appropriate platform specialization. The KVM executes on top of a LEON Sparc processor, which in turn is configured as a soft-core in a Virtex XC2V1000 FPGA. The system has three levels of configuration: Java, C, and hardware. The prototyping environment is an Insight Electronics development board, which contains besides the FPGA also a 32 MByte DDR RAM.

[0139] The LEON/Sparc core provides two interfaces: a high-speed AMBA bus interface (AHB) and a co-processor interface (CPI). Each interface has specific advantages toward domain-specific co-processors. The CPI offers an instruction- and register-set that is visible from within the Sparc instruction set, and allows a close integration of a domain-specific processor and the Sparc. The AMBA bus uses mapping of a co-processor through the abstraction of a memory interface. The CPI provides two 64-bit data ports and a 10-bit opcode port.

[0140] The high speed AMBA bus contains a memory interface and a bridge to the peripheral bus interface (APB). The memory interface includes an interface to a 32 MByte DDR RAM memory. The AMBA peripheral bus (APB) contains the fingerprint processor and two UART blocks. One connection is used to attach a fingerprint sensor 202, while the second one is used to connect an application server. This server is used to download and debug applications, as well as to experiment with the security protocol.

[0141] Although the preceding description contains much specificity, this should not be construed as limiting the scope of the invention, but as merely providing illustrations of embodiments thereof. Many other variations are possible within the scope of the present invention. For example, one of ordinary skill in the art will recognize that the thumbpod can be implemented using a variety of virtual machine and/or operating environments, such as, for example, Windows CE, TinyOS, PALM OS, Linux. etc. Although JAVA is described as being used in one or more embodiments, other languages can be used as well, such as, for example, high-level languages, low-level languages, C/C++, lisp, assembly language, etc. Thus, the scope of the invention is limited only by the claims.

WHAT IS CLAIMED IS:

1. A secure system for biometric signal processing, comprising:

a secure communication protocol configured to localize biometric data, wherein said protocol provides authentication without transmission of said biometric data; and

a key generation function based on a dynamic key generator and static biometric components.

2. A secure system for biometric signal processing, comprising:

a fingerprint image sensor;

a cryptographic module configured to encrypt and decrypt data using a secret key known to said cryptographic hardware accelerator and to an authentication server; and

a communication protocol module configured to receive an authentication vector from said authentication server, verify an identity of said authentication server, and to provide authentication of a user to said authentication server without transmission of biometric data .

3. The system of Claim 2, further comprising a communication port.

4. The system of Claim 2, wherein a biometric verification process is performed within the secure system.

5. The system of Claim 2, wherein a fingerprint verification process is performed within the secure system using minutia detection and matching algorithms.

6. The system of Claim 2, wherein access to said cryptographic hardware accelerator is substantially transparent to a JAVA program.

7. A method for providing secure communications, comprising

sending an identification code to a transaction terminal;

forwarding said identification code and transaction data from said transaction terminal to an authentication server;

generating a first authorization vector;

encrypting at least a portion of said first authorization vector using a first secret key to produce a first encrypted authorization vector;

sending said first encrypted authorization vector to said transaction terminal;

forwarding said first encrypted authorization vector from said transaction terminal to a biometric identification device comprising a biometric identification sensor;

decrypting said first encrypted authorization vector to create a first decrypted authorization vector;

verifying an identity of said authorization server using at least portion of said first decrypted authorization vector;

sensing biometric data using said biometric identification sensor;

examining said biometric data to verify an identity of a user of said biometric identification device;

generating a second authorization vector;

encrypting at least a portion of said second authorization vector using a second secret key to produce a second encrypted authorization vector;

sending said second encrypted authorization vector to said transaction terminal;

forwarding said first encrypted authorization vector from said transaction terminal to said authentication server;

decrypting said first encrypted authorization vector to create a second decrypted authorization vector; and

verifying an identity of said user using at least a portion of said second decrypted authorization vector.

8. The method of Claim 7, further comprising:

profiling a JAVA application module of said biometric identification device;

converting relatively moderately-used portions of said JAVA application to a C language portion and accessing said C language portion without substantially modifying said JAVA application module; and

converting relatively heavily-used portions of said JAVA application into hardware and accessing said hardware through an interface without substantially modifying said JAVA application module.

9. The method of Claim 7, wherein said first secret key and said second secret key are substantially identical.

10. The method of Claim 7, wherein said sending an identification code comprises wireless transmission.

11. The method of Claim 7, wherein said sending an identification code comprises infrared transmission.

12. The method of Claim 7, wherein said sending an identification code comprises radio-frequency wireless transmission.

13. The method of Claim 7, wherein said encrypting said at least a portion of said first authorization vector comprises a Rijndael algorithm.

14. The method of Claim 7, wherein said biometric sensor comprises a fingerprint sensor.

15. The method of Claim 7, wherein said biometric sensor comprises an RFID sensor.

16. The method of Claim 7, wherein said biometric sensor comprises a retina scan sensor.

17. The method of Claim 7, wherein said biometric data comprises image data.

18. The method of Claim 7, wherein said biometric data comprises fingerprint image data.

19. The method of Claim 7, wherein said verifying an identity of said user comprises identifying minutiae in a fingerprint scan.

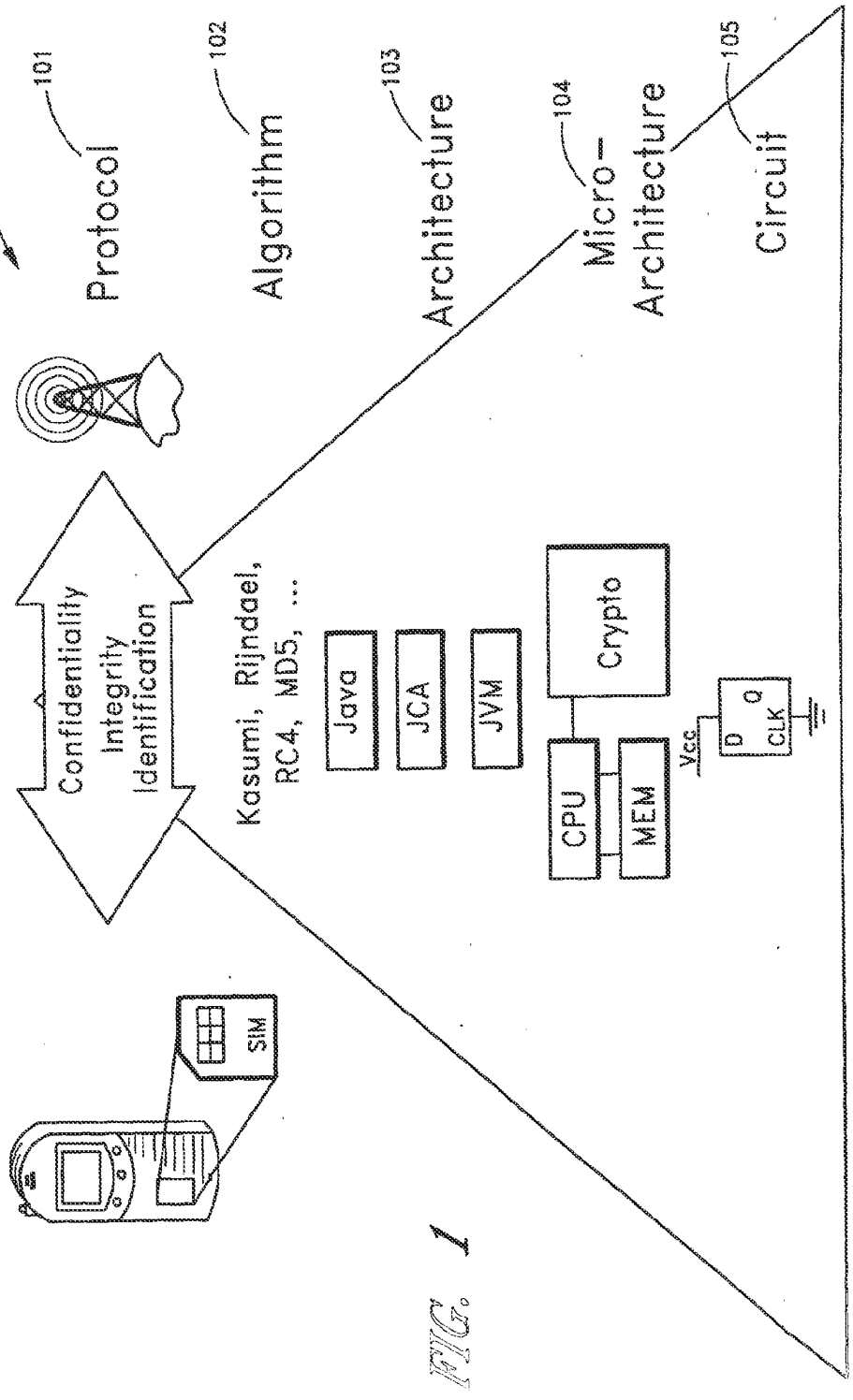

100
101
Protocol
102
Algorithm
103
Architecture
104
Micro-
Architecture
105
Circuit
Confidentiality
Integrity
Identification
Kasumi, Rijndael,
RC4, MD5, ...
Java
JCA
JVM
Crypto
CPU
MEM
Vcc
D
Q
CLK
SIM

FIG. 1

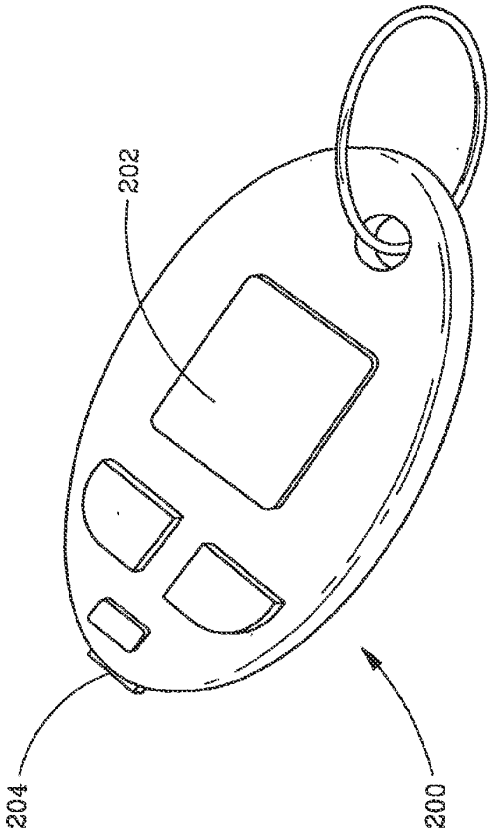


FIG. 2

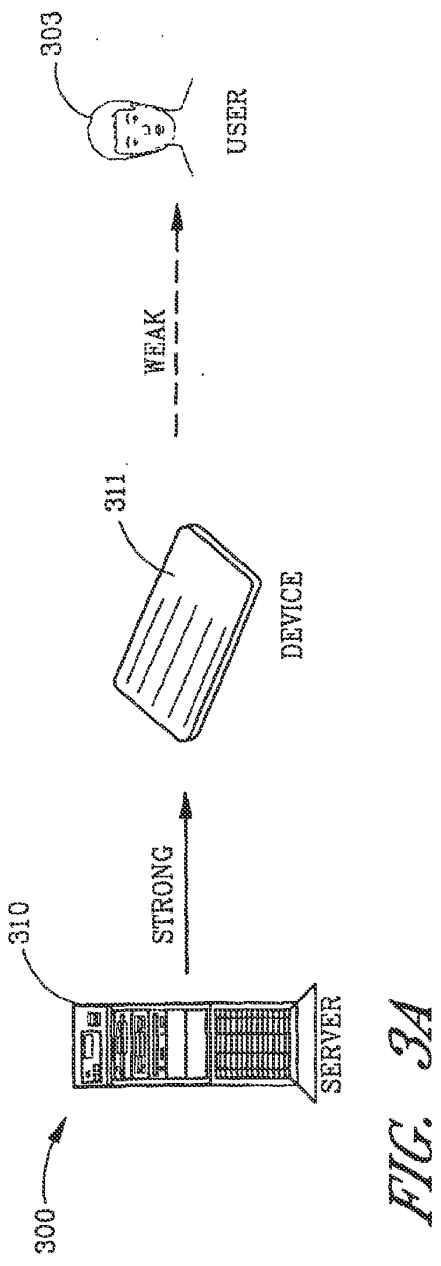

303
USER
WEAK
311
DEVICE
STRONG
310
SERVER
300

FIG. 3A

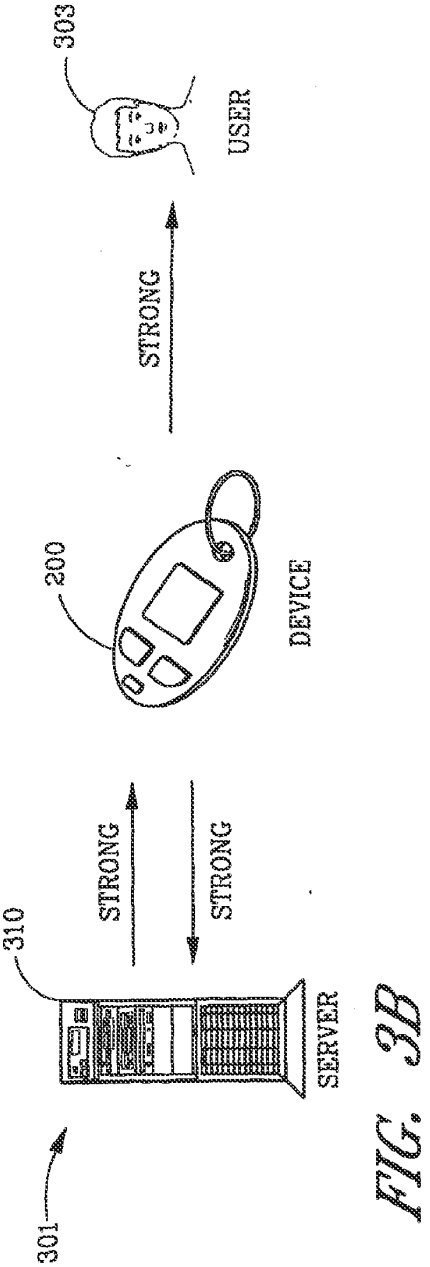

303
USER
STRONG
200
DEVICE
STRONG
STRONG
310
SERVER
301

FIG. 3B

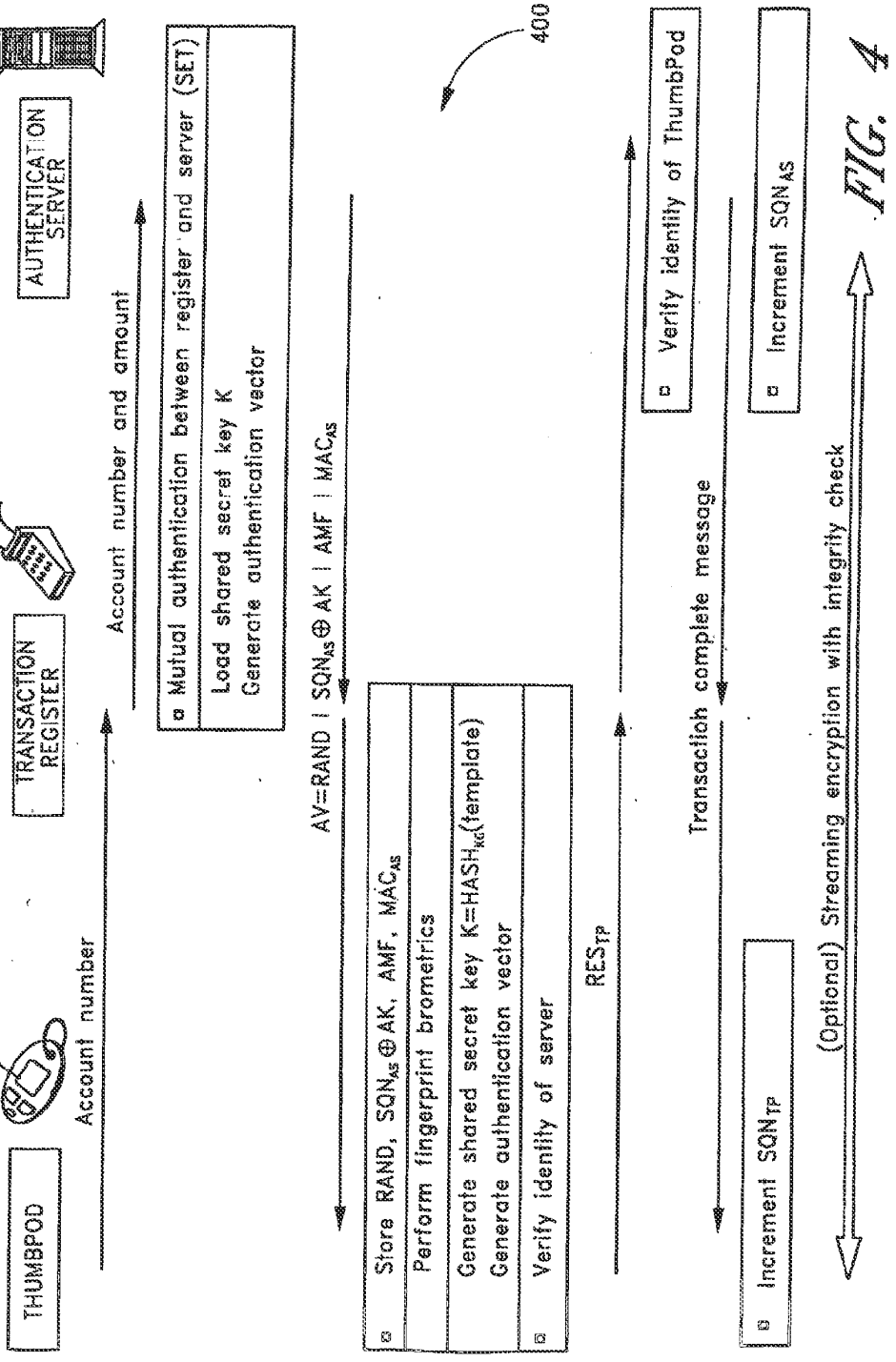

THUMBPOD
200
Account number
TRANSACTION REGISTER
401
AUTHENTICATION SERVER
310
Account number and amount
Mutual authentication between register and server (SET)
Load shared secret key K
Generate authentication vector
AV=RAND | SQNAS ⊕ AK | AMF | MACAS
400
Store RAND, SQNAS ⊕ AK, AMF, MACAS
Perform fingerprint biometrics
Generate shared secret key K=HASHKd(template)
Generate authentication vector
Verify identity of server
RESTP
Verify identity of ThumbPod
Transaction complete message
Increment SQNAS
Increment SQNTP
(Optional) Streaming encryption with integrity check

FIG. 4

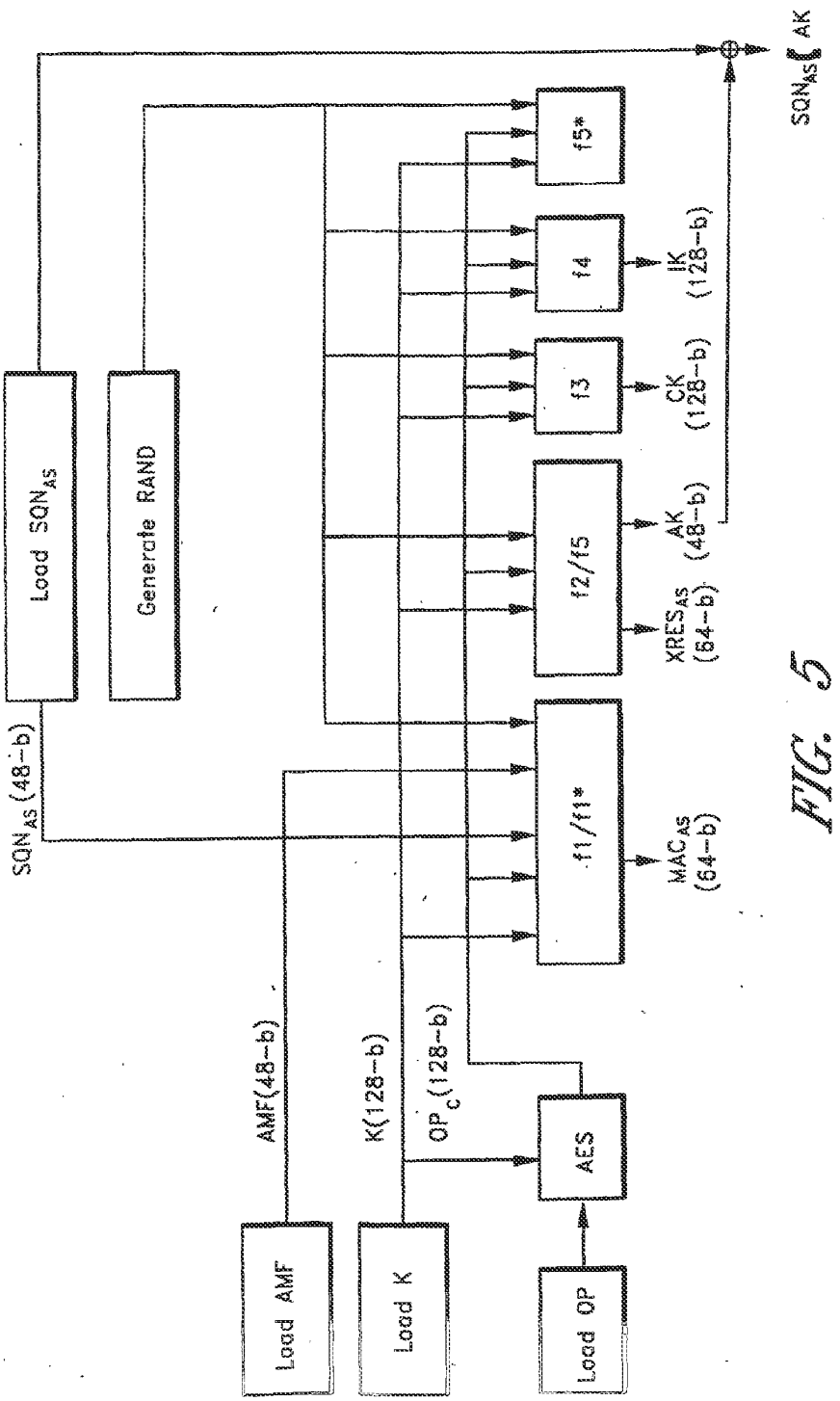

Load SQN_AS
Generate RAND
SQN_AS (48-b)
AMF(48-b)
K(128-b)
OP_c(128-b)
Load AMF
Load K
Load OP
AES
f1/f1*
f2/f5
f3
f4
f5*
MAC_AS (64-b)
XRES_AS (64-b)
AK (48-b)
CK (128-b)
IK (128-b)
SQN_AS ⊕ AK

FIG. 5

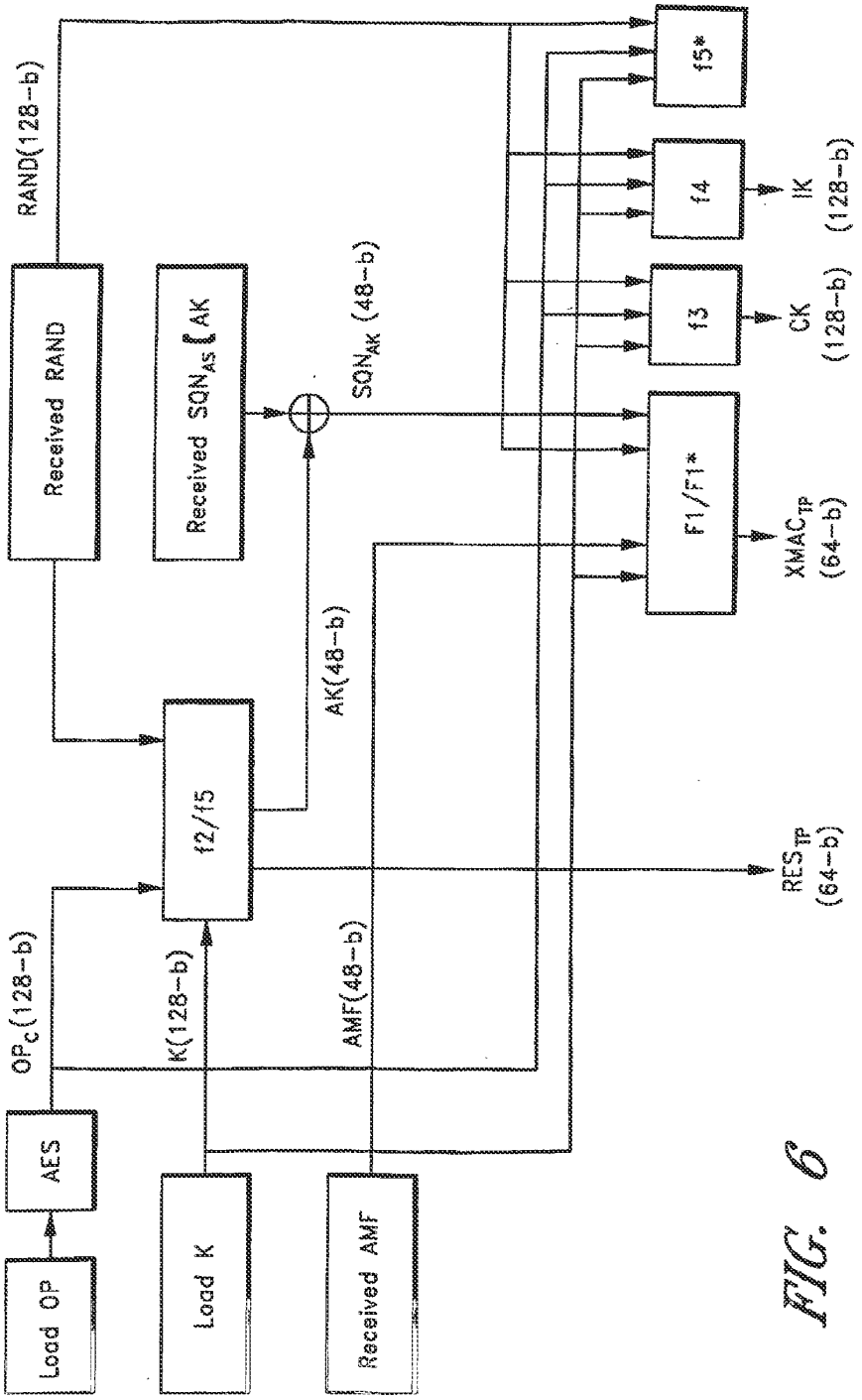
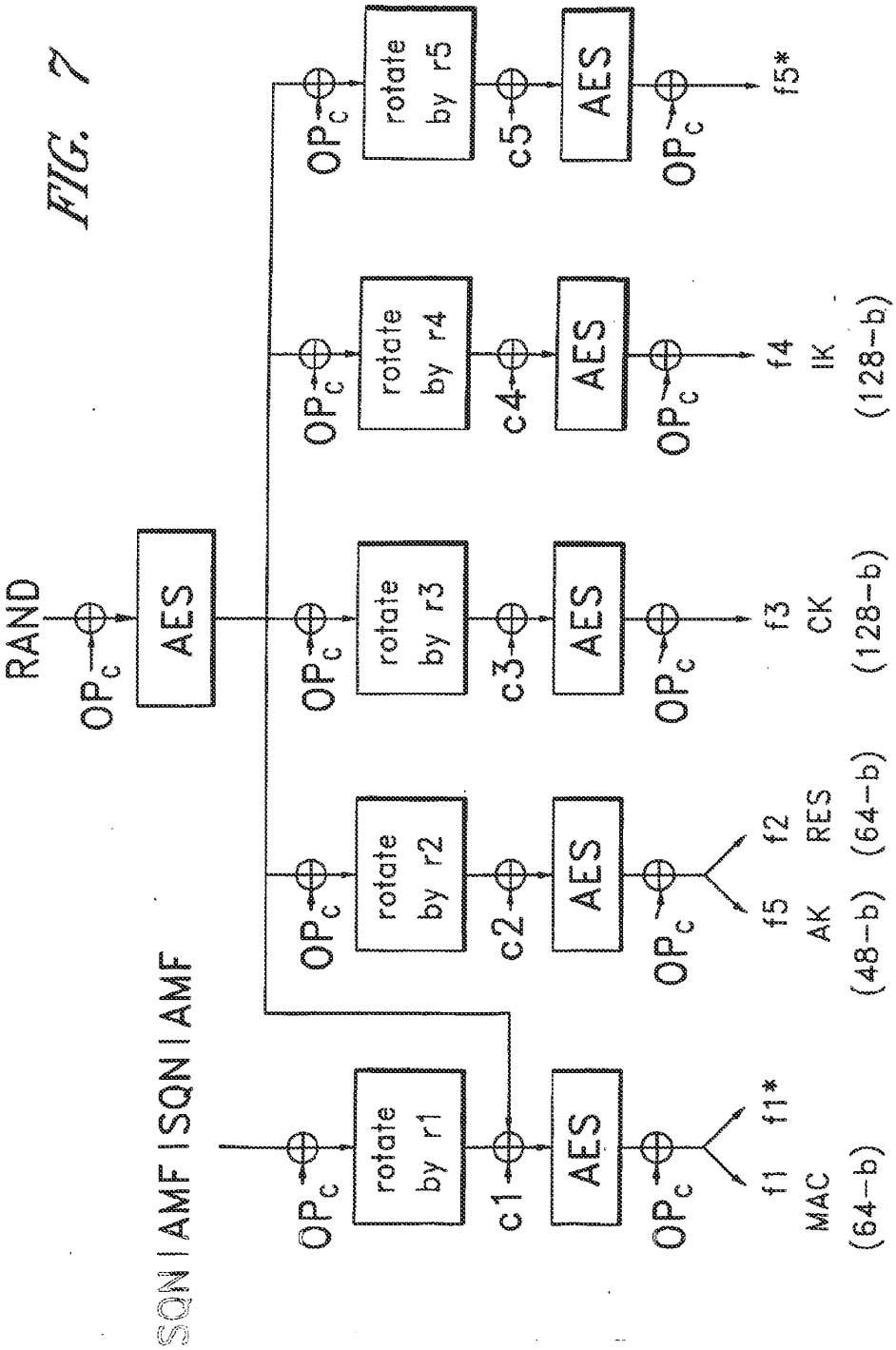

RAND(128-b)
Received RAND
Received SQN$_{AS}$ ⊕ AK
SQN$_{AK}$ (48-b)
f5*
f4
IK (128-b)
f3
CK (128-b)
F1/F1*
XMAC$_{TP}$ (64-b)
AK(48-b)
f2/f5
RES$_{TP}$ (64-b)
OP$_C$(128-b)
K(128-b)
AMF(48-b)
AES
Load OP
Load K
Received AMF

FIG. 6

FIG. 7


RAND
SQN | AMF | SQN | AMF
AES
rotate by r1
rotate by r2
rotate by r3
rotate by r4
rotate by r5
c1
c2
c3
c4
c5
OPc
f1 f1*
MAC
(64-b)
f5 f2
AK RES
(48-b) (64-b)
f3
CK
(128-b)
f4
IK
(128-b)
f5*

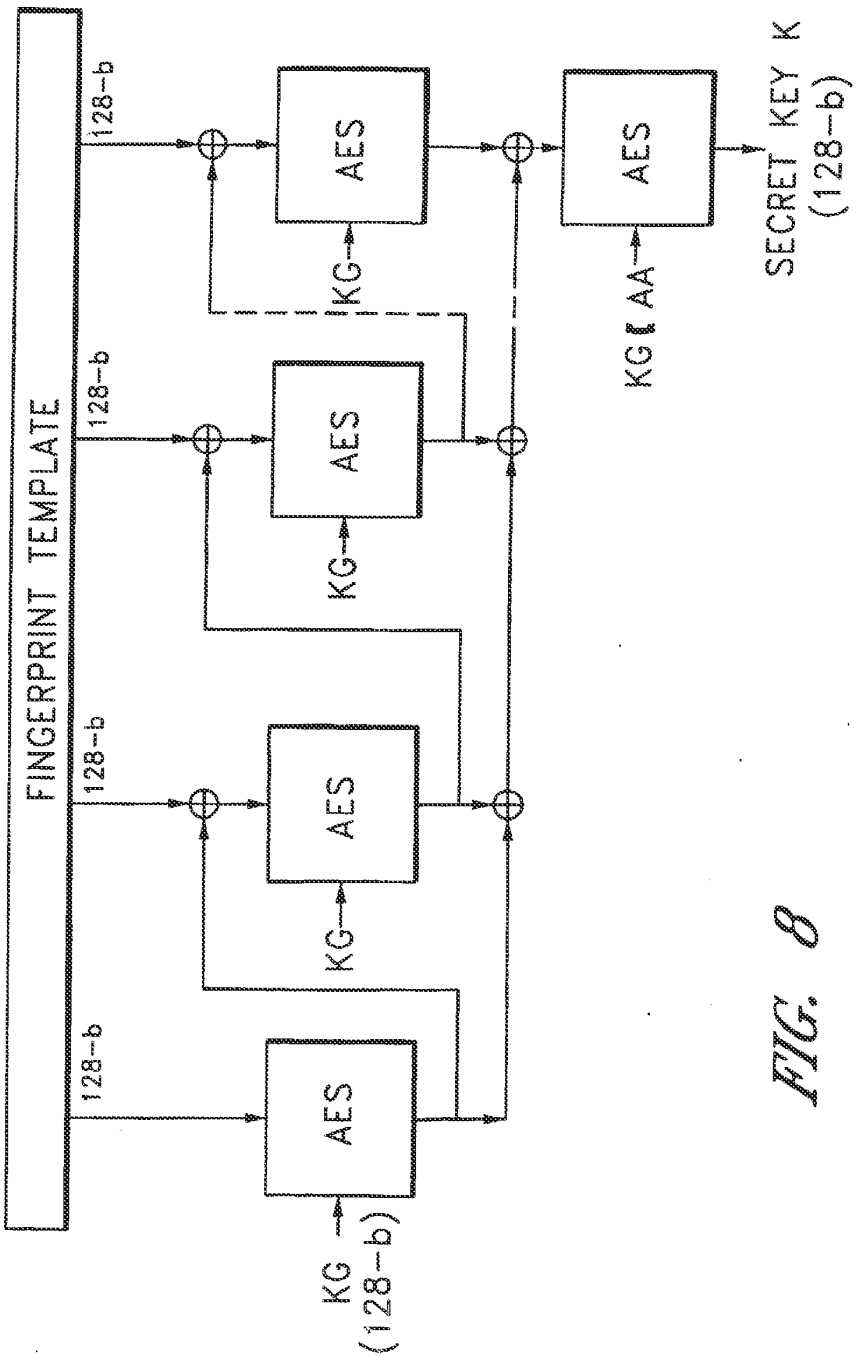
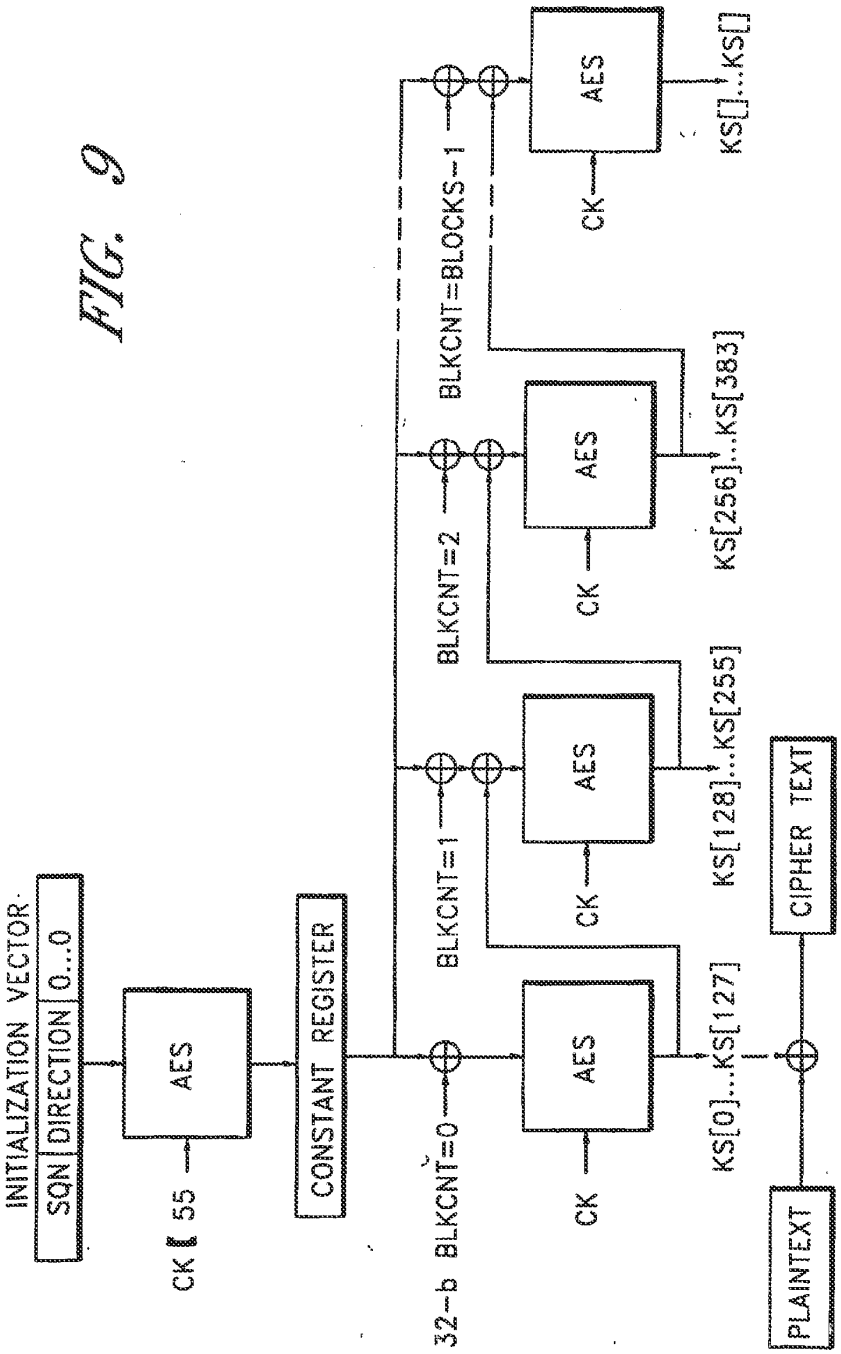

FINGERPRINT TEMPLATE
128-b
128-b
128-b
128-b
AES
AES
AES
AES
KG
KG
KG
KG
(128-b)
KG & AA
SECRET KEY K
(128-b)

FIG. 8

FIG. 9


INITIALIZATION VECTOR
SQN
DIRECTION
0...0
AES
CK [55
CONSTANT REGISTER
32-b BLKCNT=0
BLKCNT=1
BLKCNT=2
BLKCNT=BLOCKS-1
AES
CK
KS[0]...KS[127]
KS[128]...KS[255]
KS[256]...KS[383]
KS[]...KS[]
CIPHER TEXT
PLAINTEXT

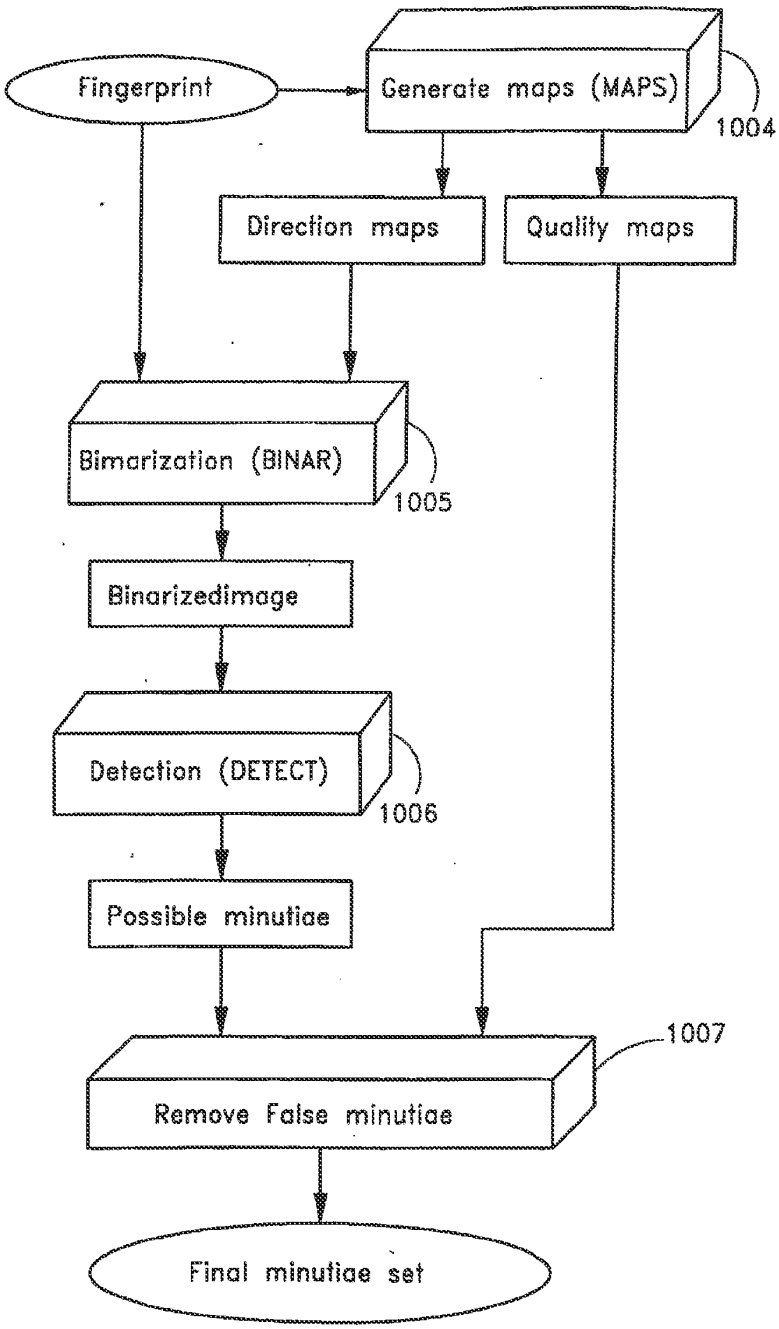
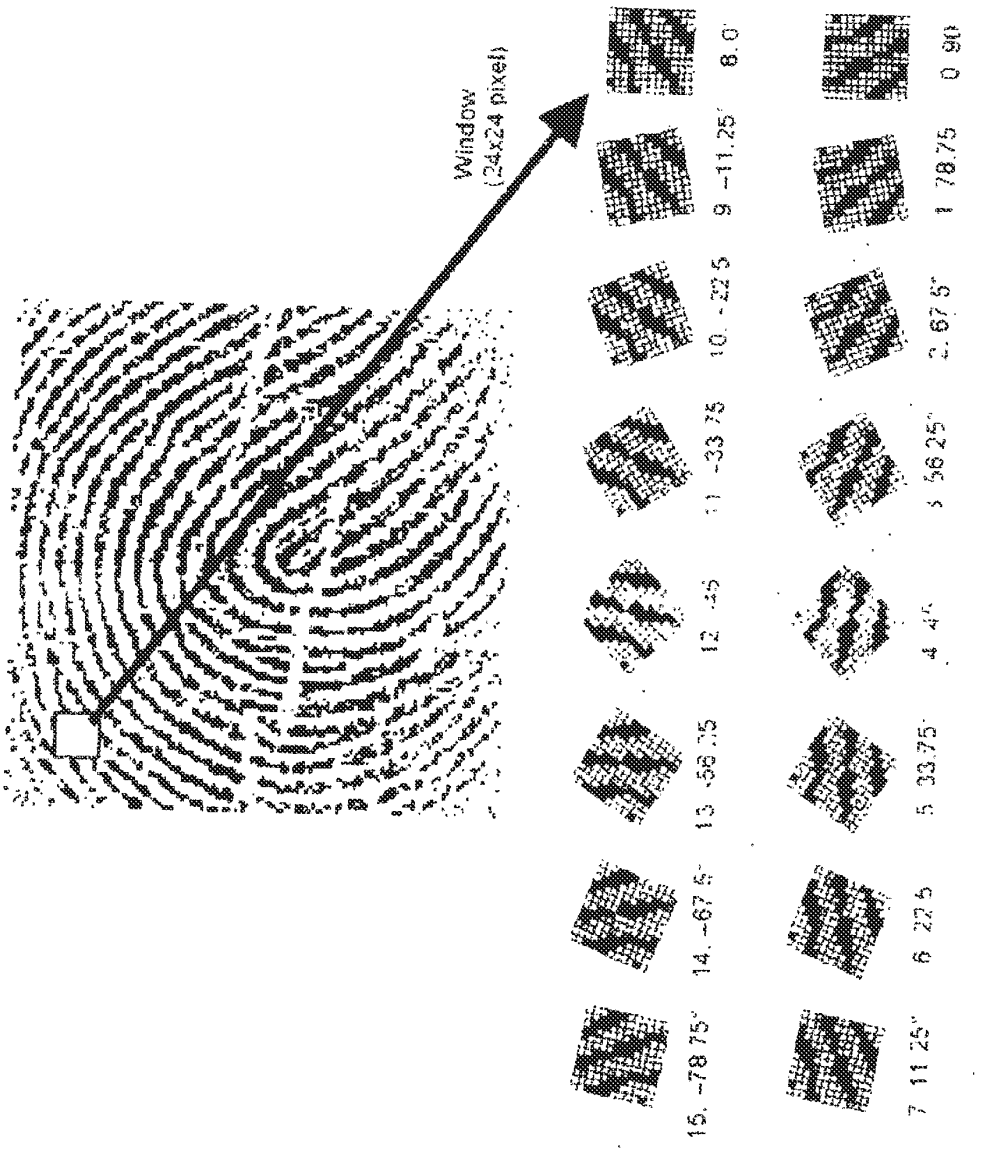

Fingerprint
Generate maps (MAPS)
1004
Direction maps
Quality maps
Bimarization (BINAR)
1005
Binarizedimage
Detection (DETECT)
1006
Possible minutiae
1007
Remove False minutiae
Final minutiae set

FIG. 10

FIG. 11


Window
(24x24 pixel)
8. 0°
9. -11.25°
10. -22.5
11. -33.75
12. -45
13. -56.75
14. -67.5°
15. -78.75°
0. 90
1. 78.75
2. 67.5°
3. 56.25°
4. 45°
5. 33.75°
6. 22.5
7. 11.25°

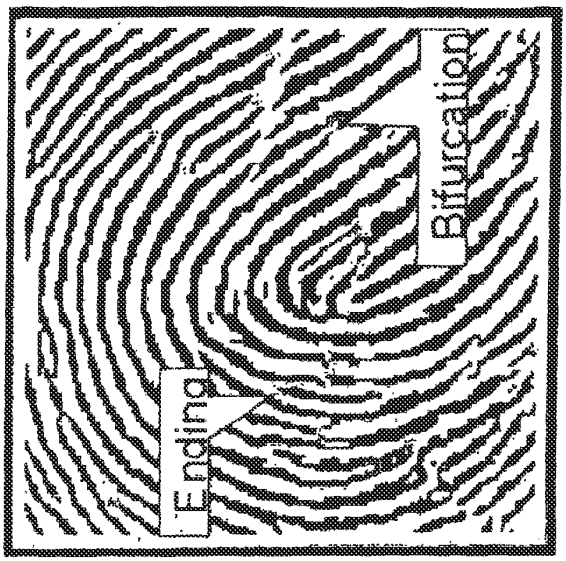


FIG. 13



FIG. 12

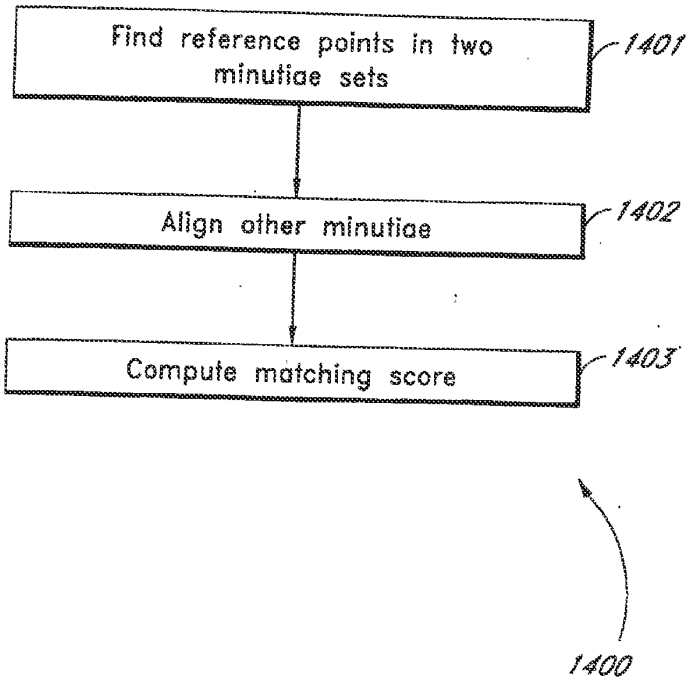

Find reference points in two minutiae sets
1401
Align other minutiae
1402
Compute matching score
1403
1400

FIG. 14

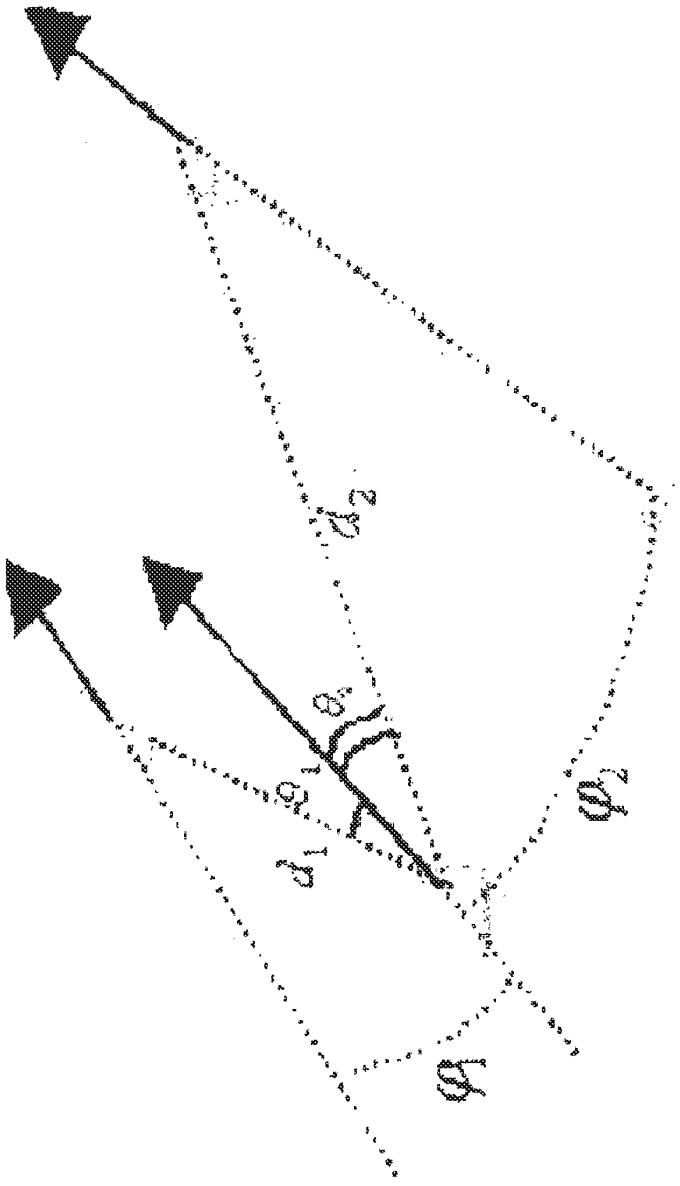


FIG. 15

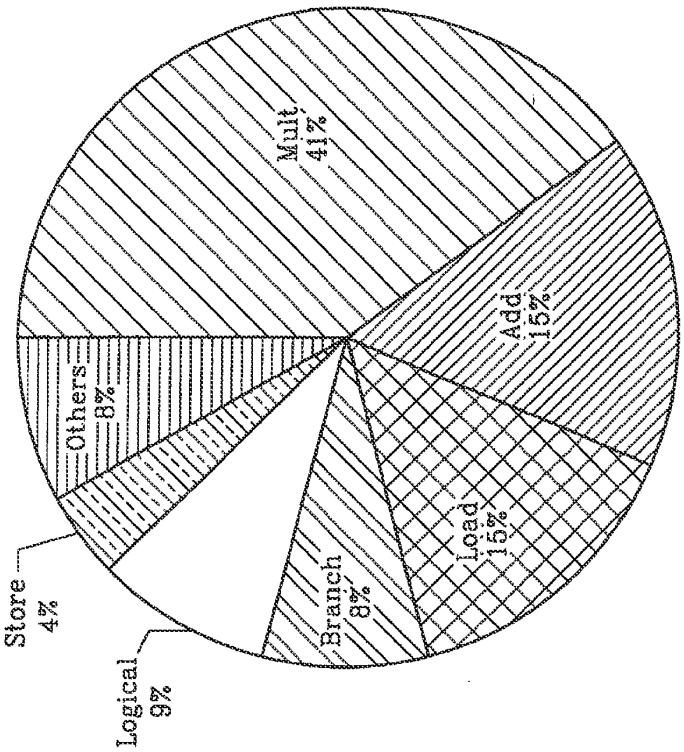

Mult
41%
Add
15%
Load
15%
Branch
8%
Logical
9%
Store
4%
Others
8%

FIG. 17

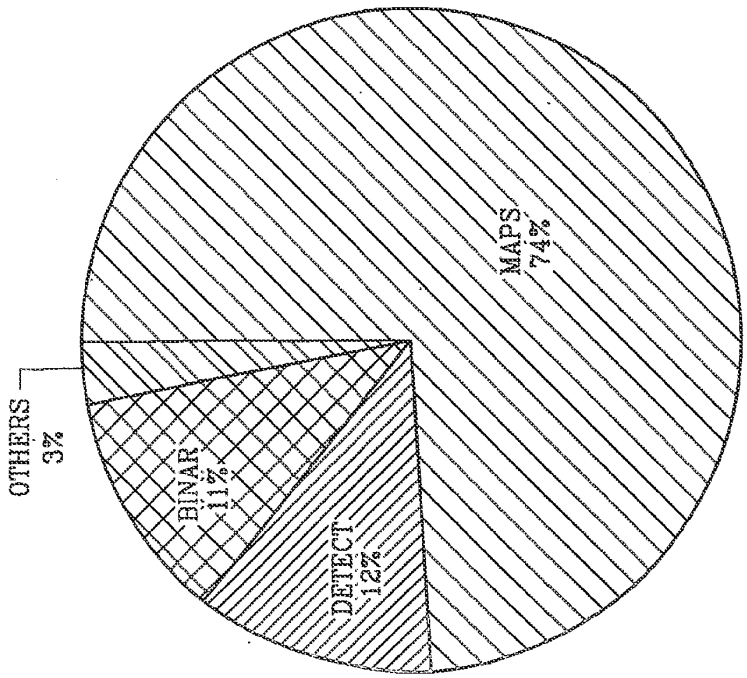
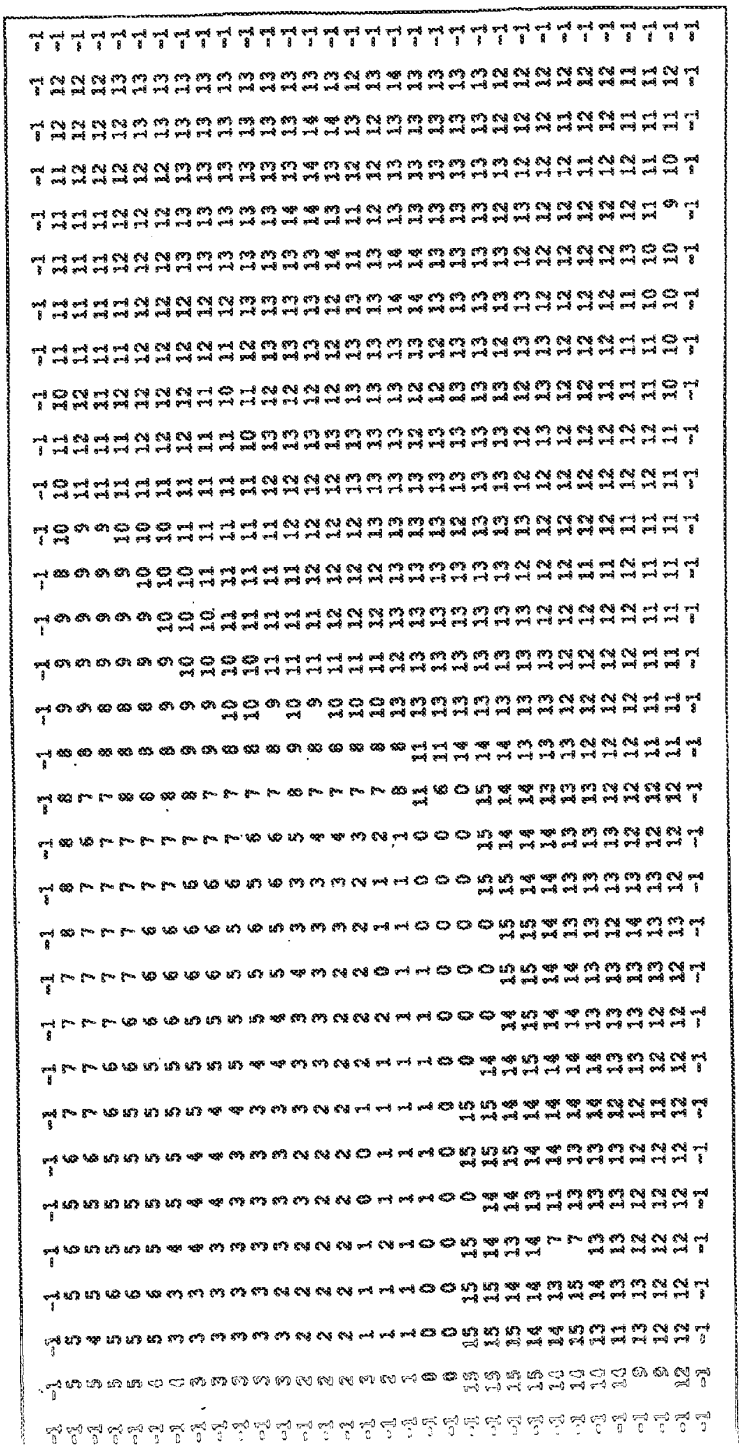

MAPS
74%
DETECT
12%
BINAR
11%
OTHERS
3%

FIG. 16

FIG. 18



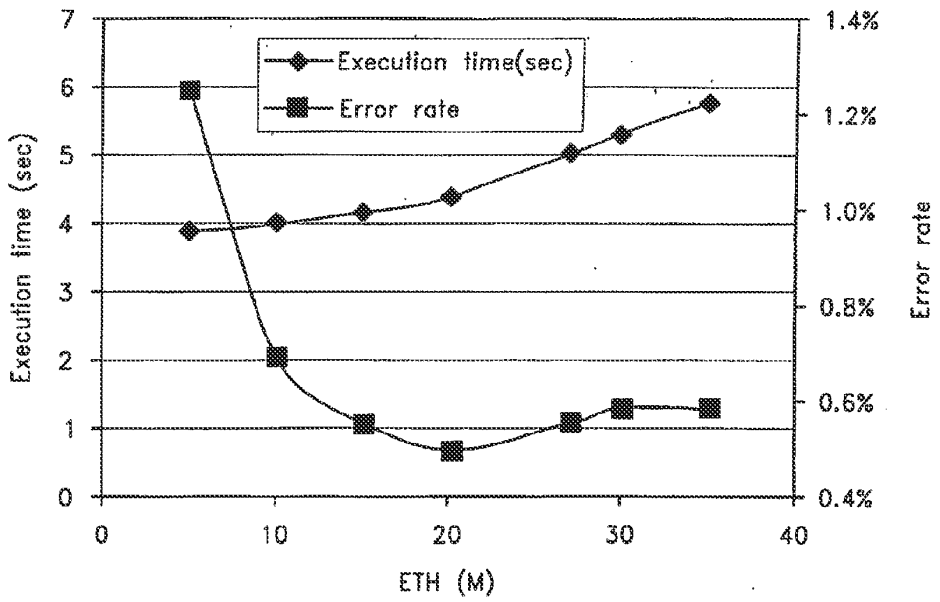

Execution time(sec)
Error rate
Execution time (sec)
Error rate
ETH (M)
0
1
2
3
4
5
6
7
0
10
20
30
40
0.4%
0.6%
0.8%
1.0%
1.2%
1.4%

FIG. 19

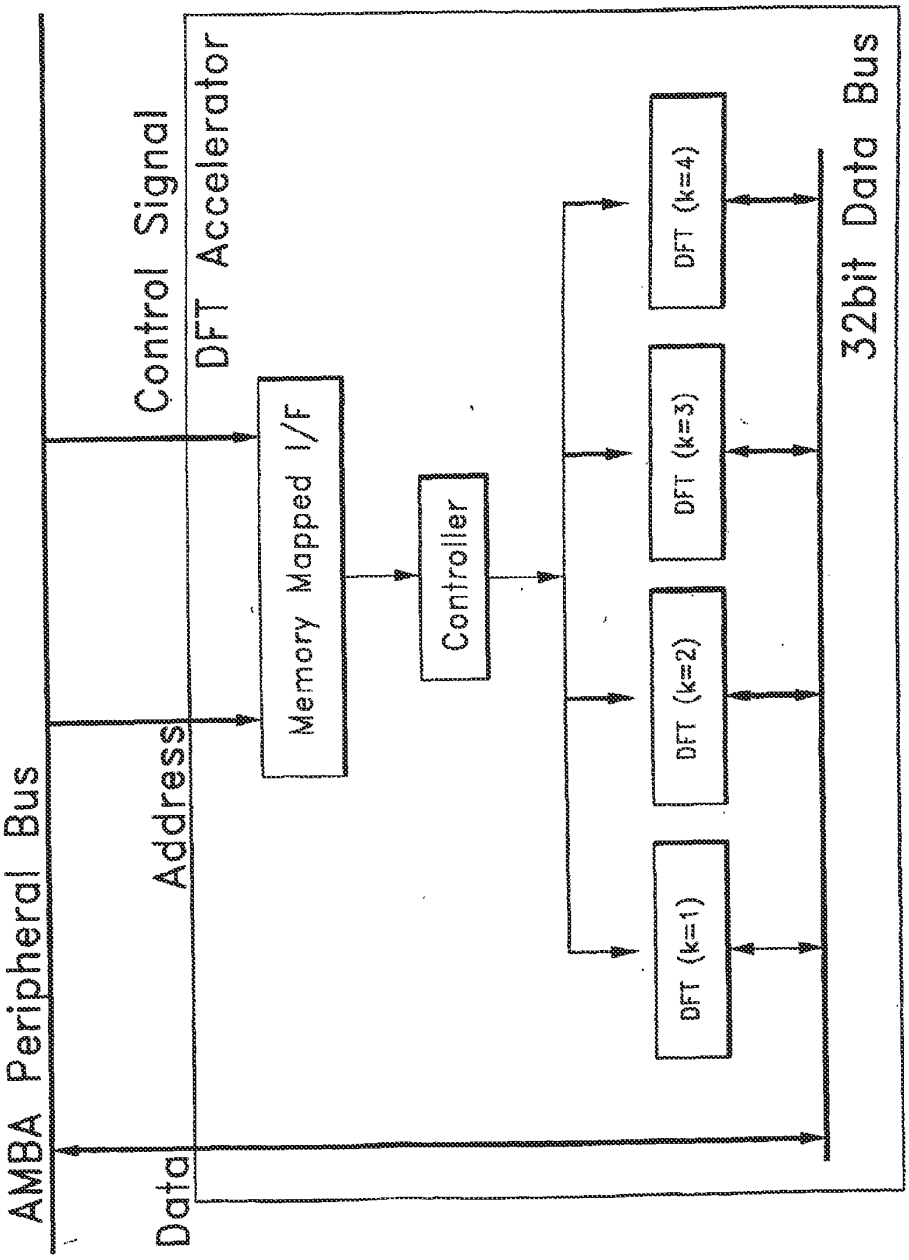

AMBA Peripheral Bus
Data
Address
Control Signal
DFT Accelerator
Memory Mapped I/F
Controller
DFT (k=1)
DFT (k=2)
DFT (k=3)
DFT (k=4)
32bit Data Bus

FIG. 20

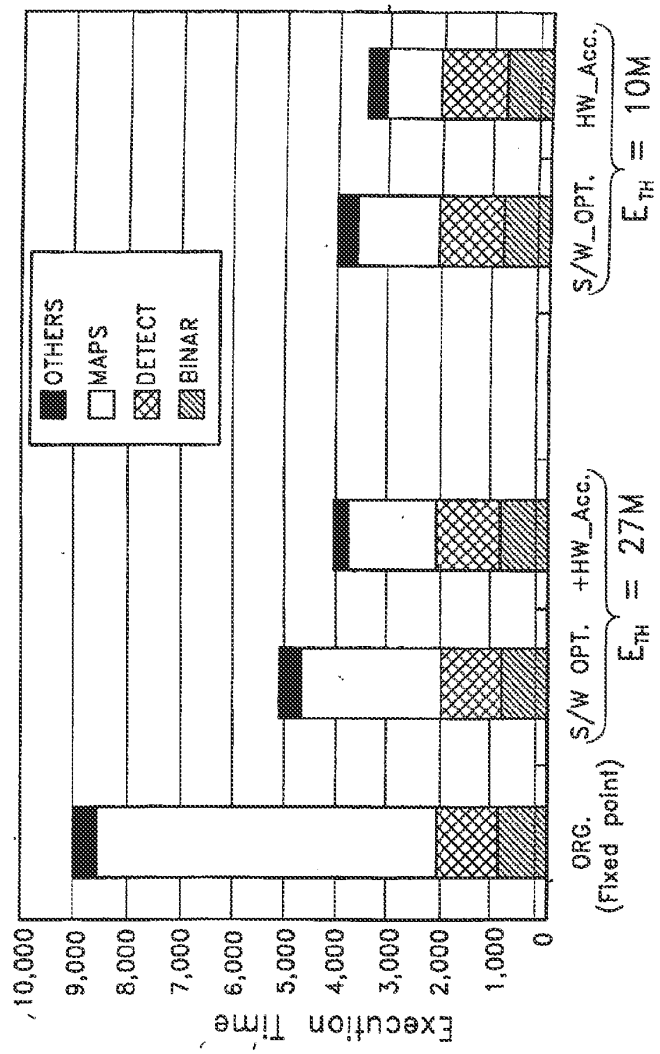

Execution Time
10,000
9,000
8,000
7,000
6,000
5,000
4,000
3,000
2,000
1,000
0
OTHERS
MAPS
DETECT
BINAR
ORG. (Fixed point)
S/W OPT. +HW_Acc. E_TH = 27M
S/W_OPT. HW_Acc. E_TH = 10M

FIG. 21

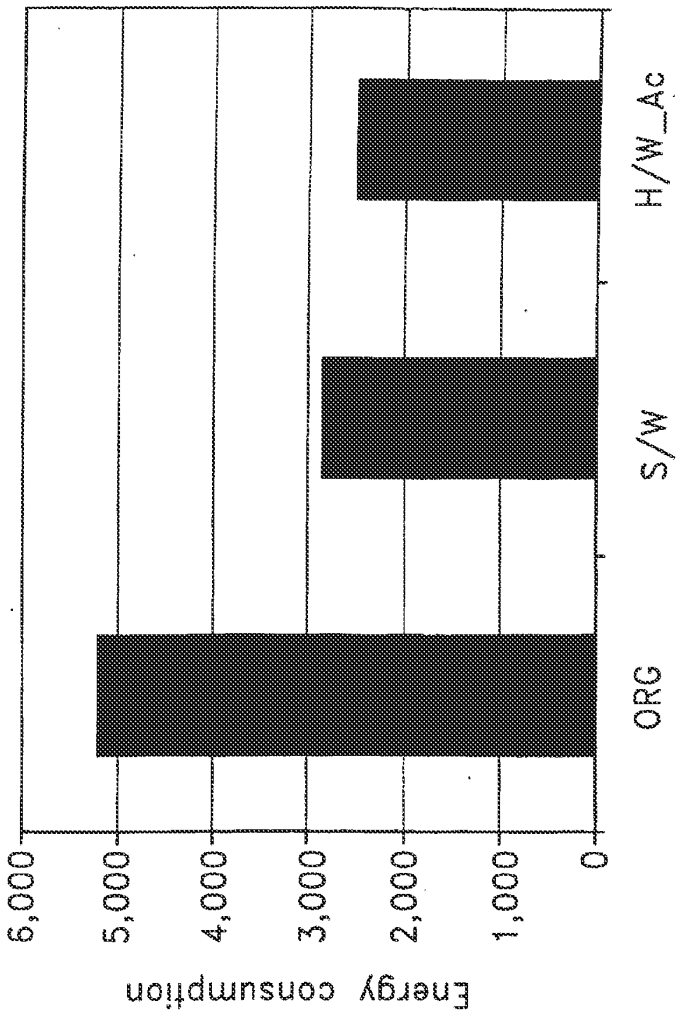

Energy consumption
6,000
5,000
4,000
3,000
2,000
1,000
0
ORG
S/W
H/W_Ac

FIG. 22

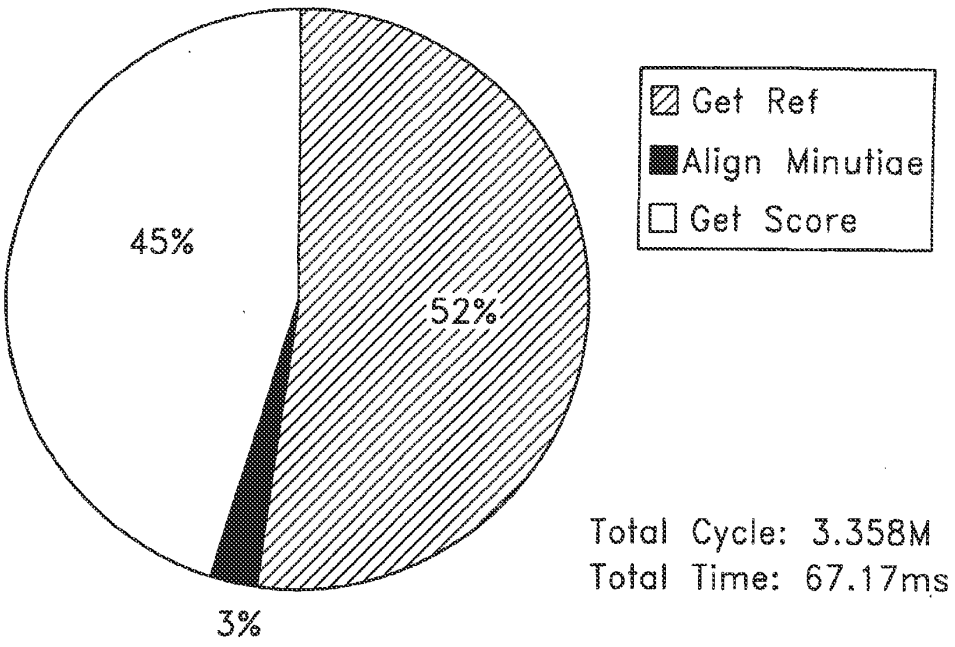

Get Ref
Align Minutiae
Get Score
45%
52%
3%
Total Cycle: 3.358M
Total Time: 67.17ms

FIG. 23

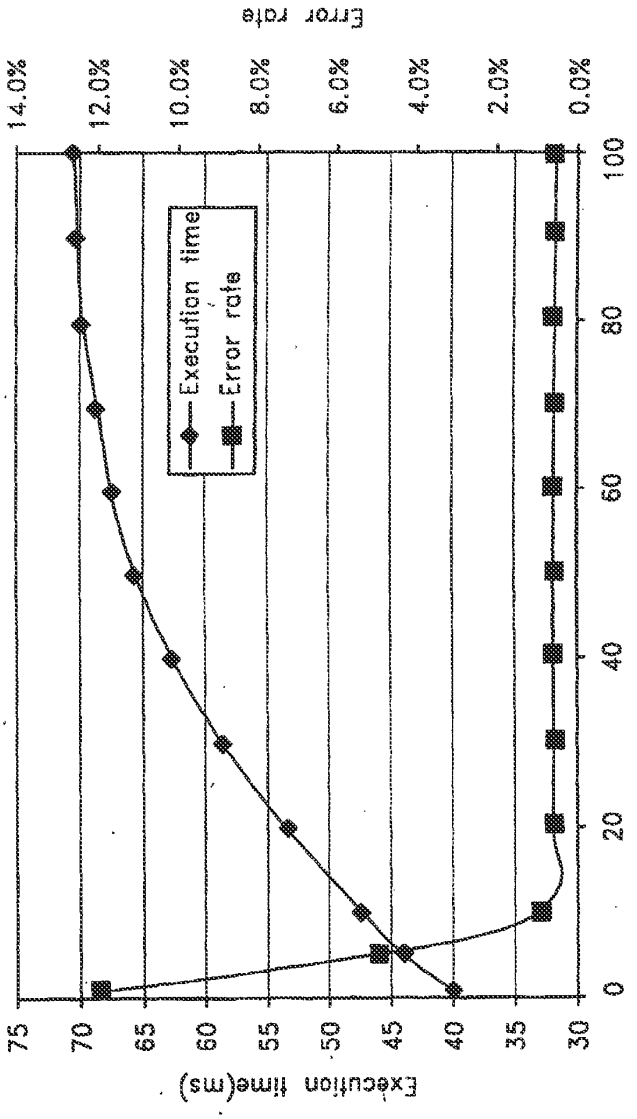

Error rate
14.0%
12.0%
10.0%
8.0%
6.0%
4.0%
2.0%
0.0%
Execution time
Error rate
Execution time(ms)
75
70
65
60
55
50
45
40
35
30
0
20
40
60
80
100
Pre-Checking threshold

FIG. 24

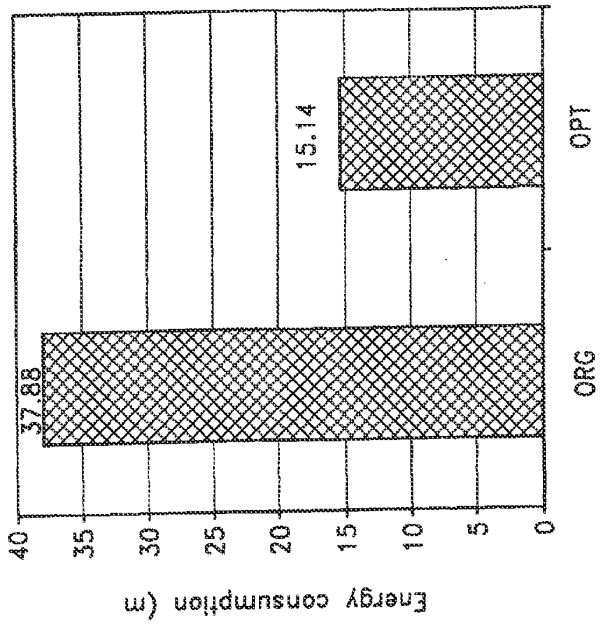


FIG. 25B

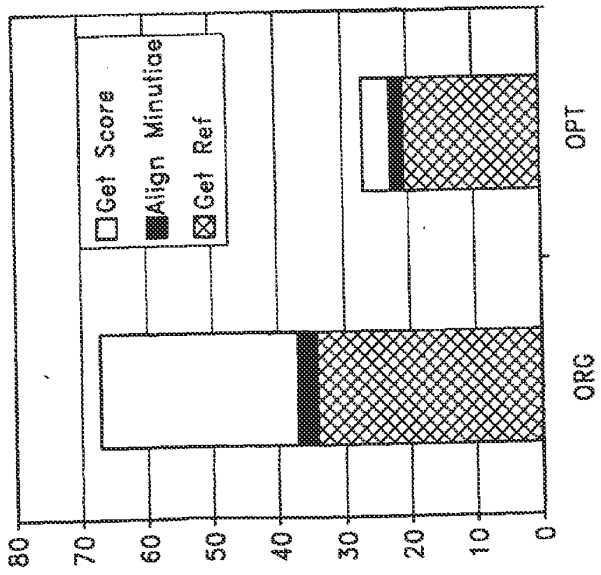


FIG. 25A

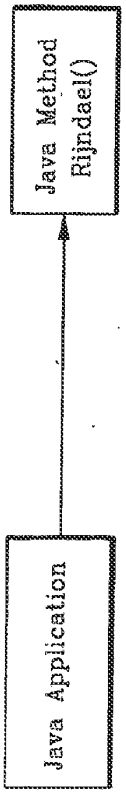


FIG. 26A

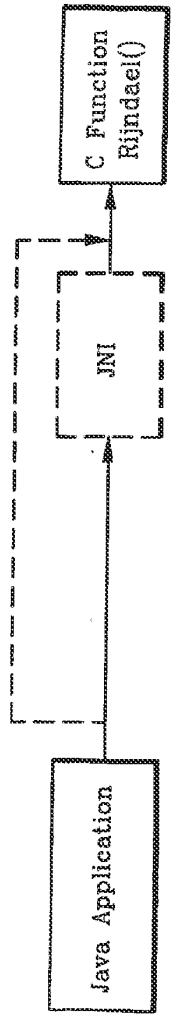


FIG. 26B

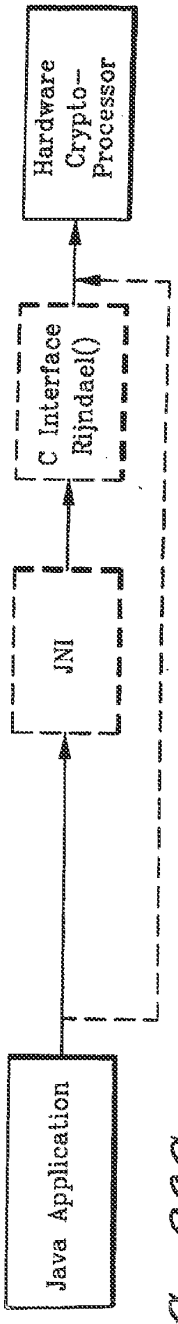


FIG. 26C

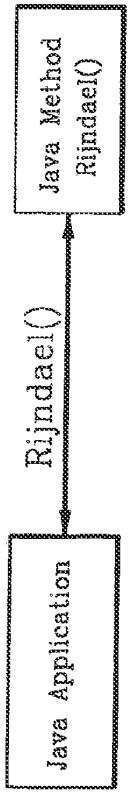


FIG. 26D

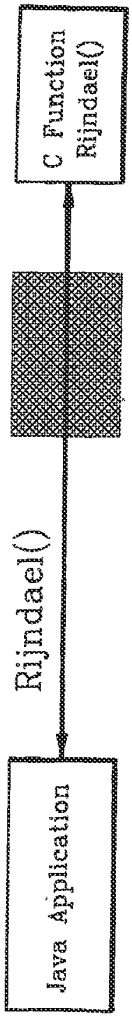


FIG. 26E

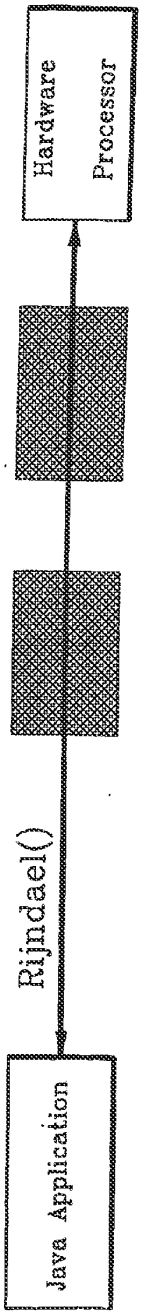


FIG. 26F

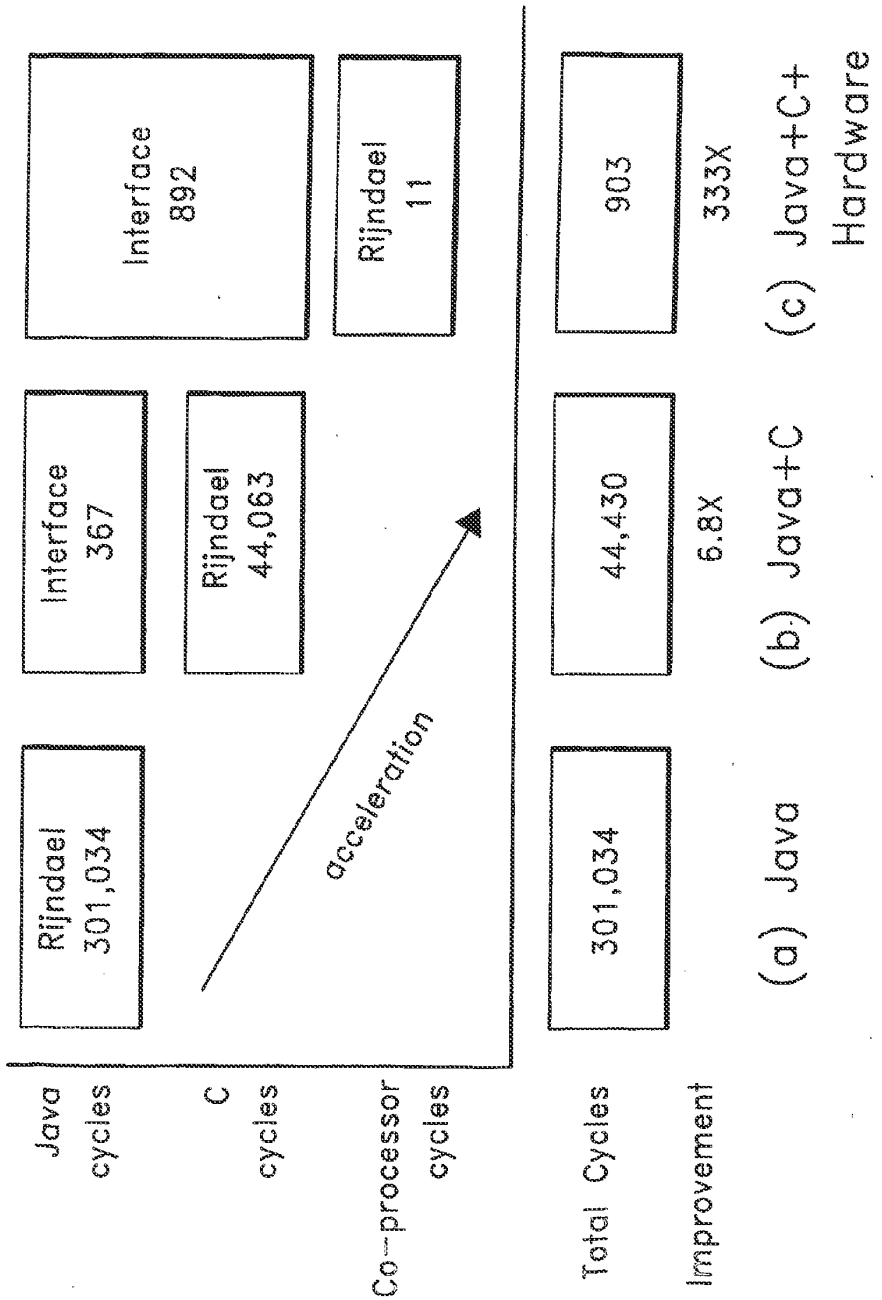

Java cycles
C cycles
Co-processor cycles
Total Cycles
Improvement
Rijndael 301,034
Interface 367
Rijndael 44,063
Interface 892
Rijndael 11
acceleration
301,034
44,430
903
6.8X
333X
(a) Java
(b) Java+C
(c) Java+C+ Hardware

FIG. 27

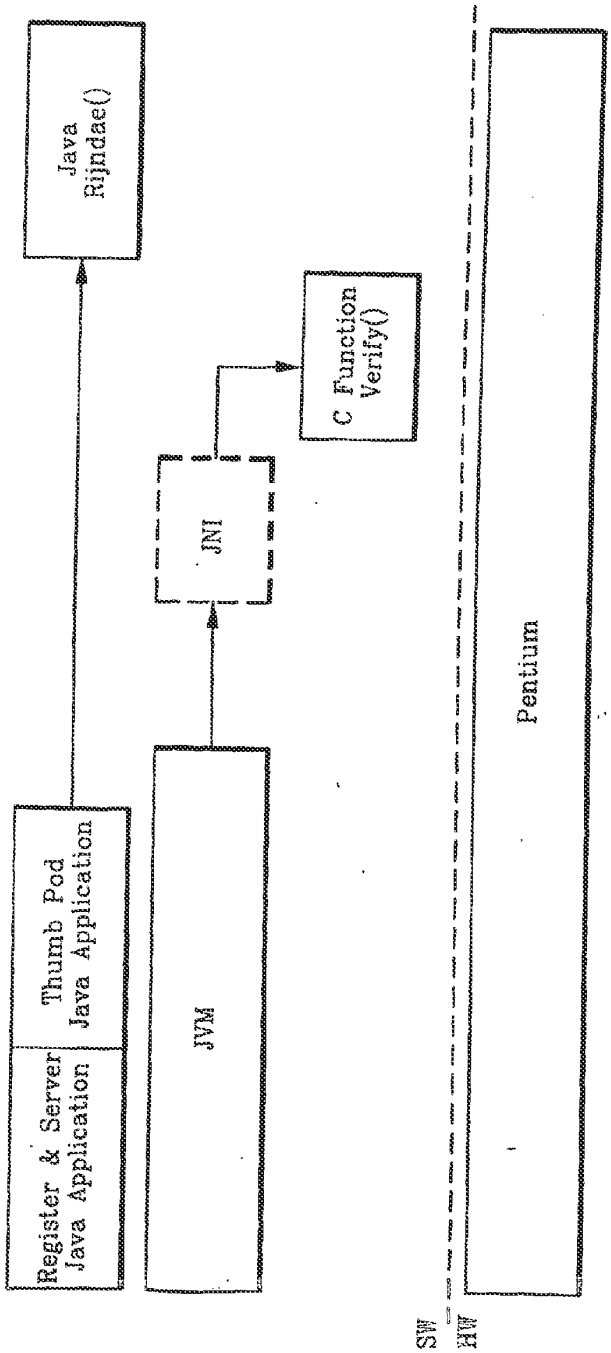

Java Rijndael()
C Function Verify()
JNI
Register & Server Java Application
Thumb Pod Java Application
JVM
Pentium
SW
HW

FIG. 28A

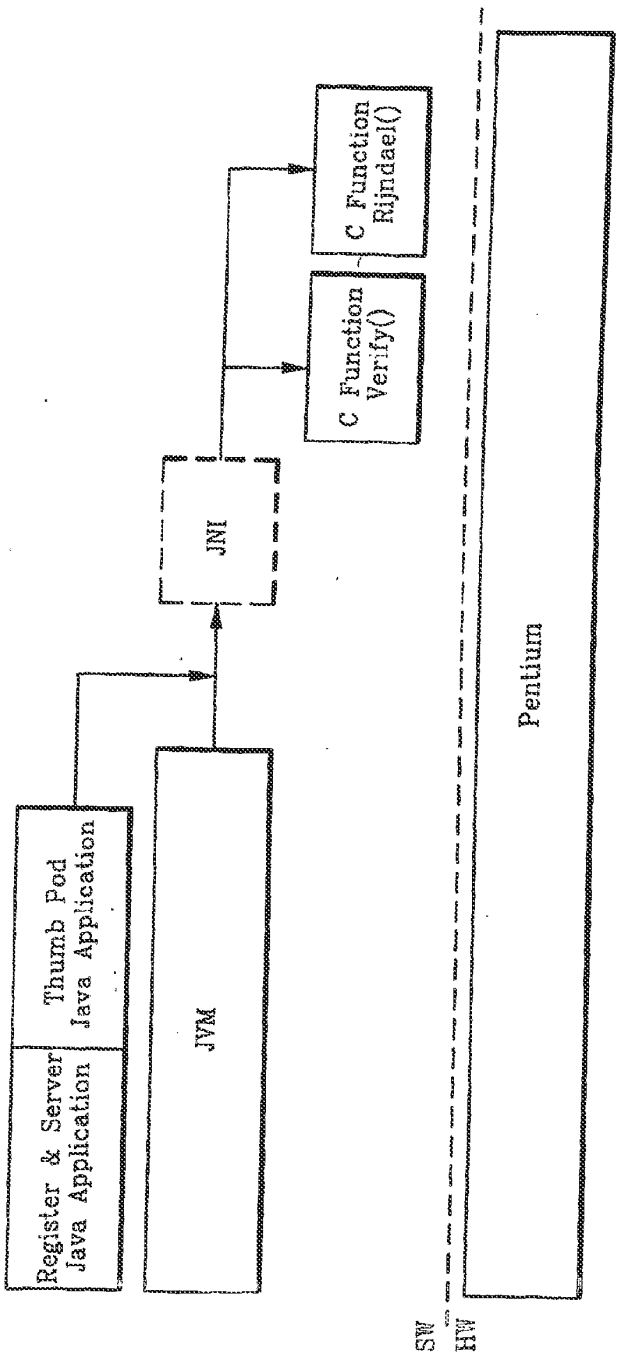

Register & Server Java Application
Thumb Pod Java Application
JVM
JNI
C Function Verify()
C Function Rijndael()
Pentium
SW
HW

FIG. 28B

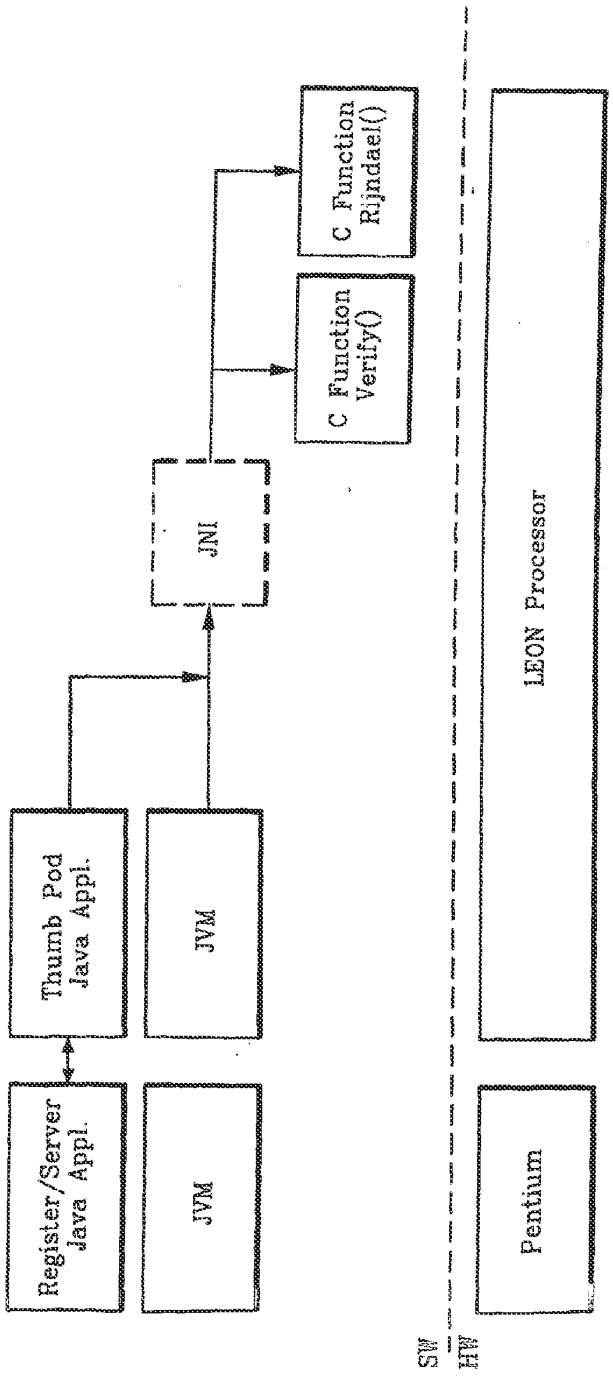

Register/Server Java Appl.
Thumb Pod Java Appl.
JVM
JVM
JNI
C Function Verify()
C Function Rijndael()
Pentium
LEON Processor
SW
HW

FIG. 28C

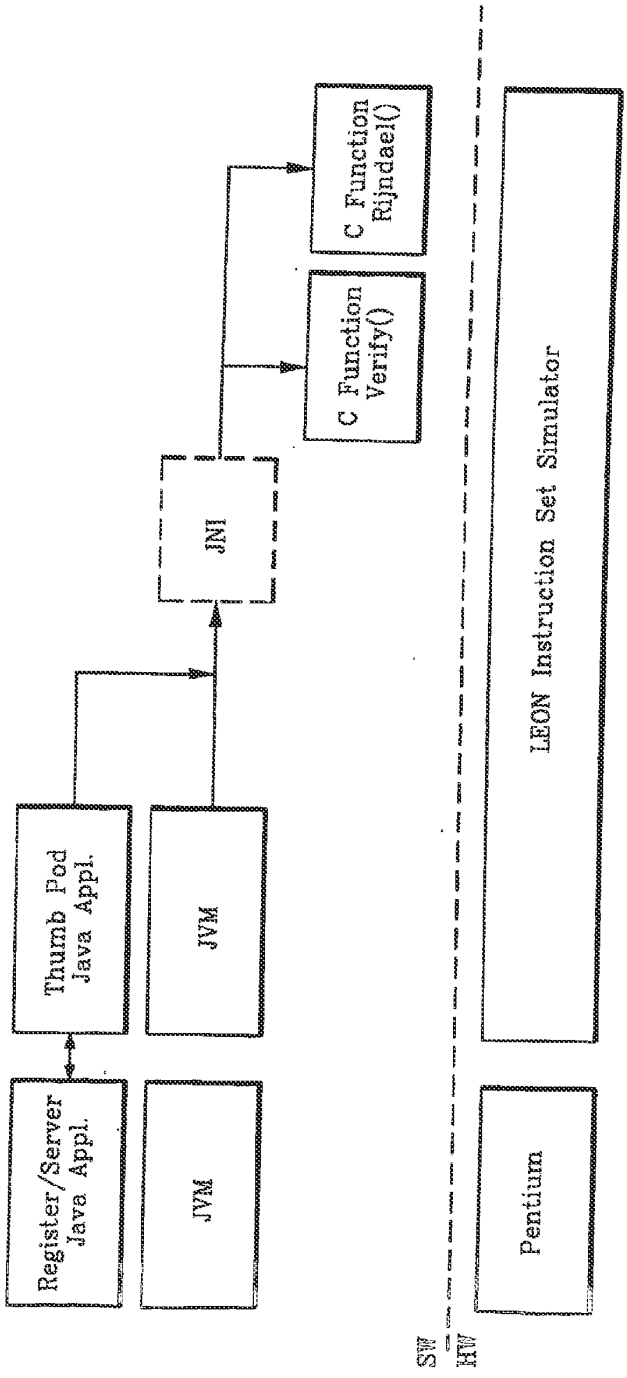

Register/Server Java Appl.
Thumb Pod Java Appl.
JVM
JVM
JNI
C Function Verify()
C Function Rijndael()
Pentium
LEON Instruction Set Simulator
SW
HW

FIG. 28D

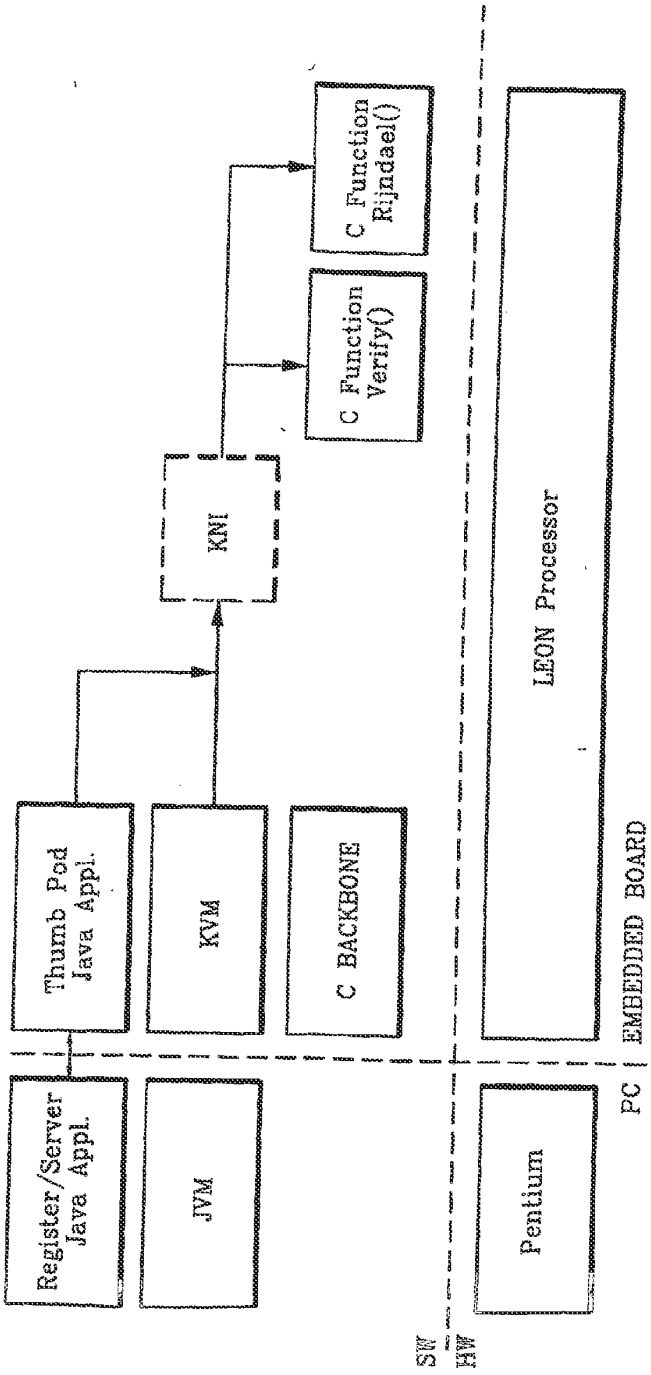

Register/Server Java Appl.
Thumb Pod Java Appl.
JVM
KVM
C BACKBONE
KNI
C Function Rijndael()
C Function Verify()
Pentium
LEON Processor
SW
HW
PC
EMBEDDED BOARD

FIG. 28E

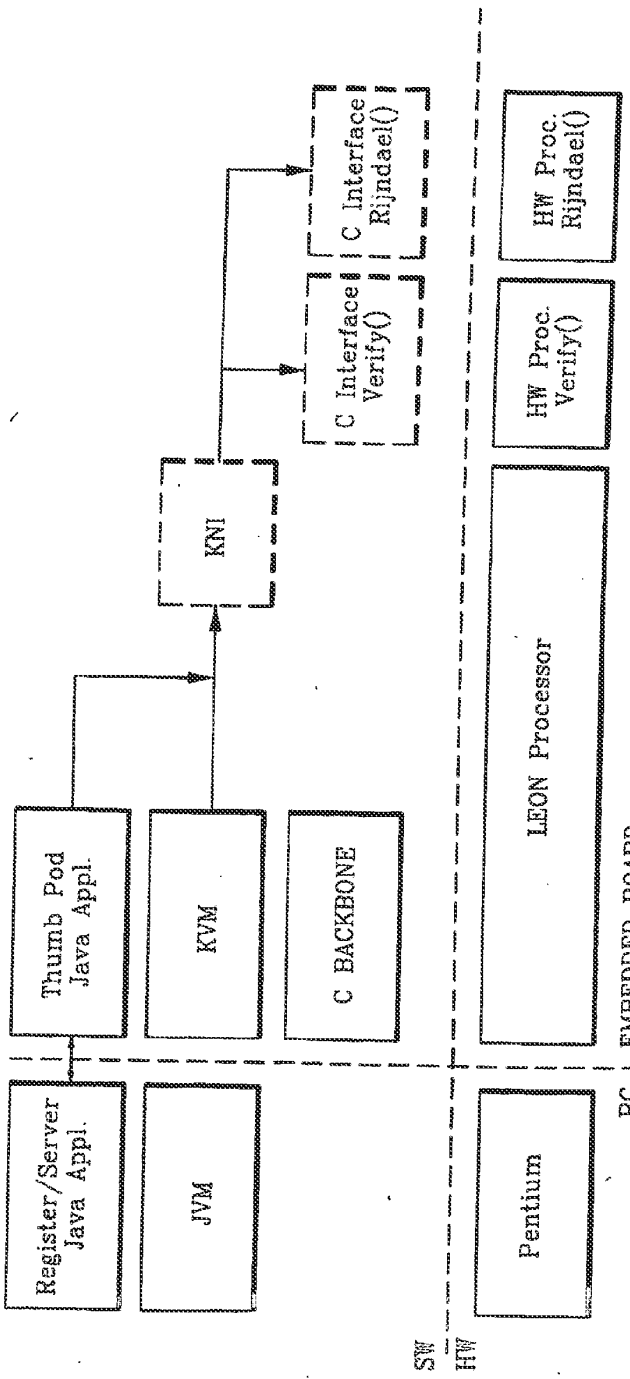

Register/Server Java Appl.
JVM
Thumb Pod Java Appl.
KVM
C BACKBONE
KNI
C Interface Verify()
C Interface Rijndael()
Pentium
LEON Processor
HW Proc. Verify()
HW Proc. Rijndael()
PC
EMBEDDED BOARD
SW
HW

FIG. 28F

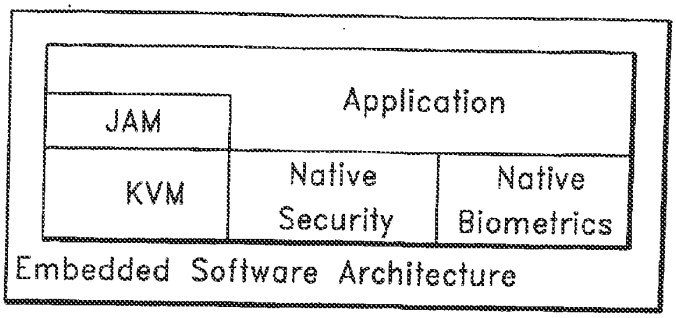


FIG. 29A

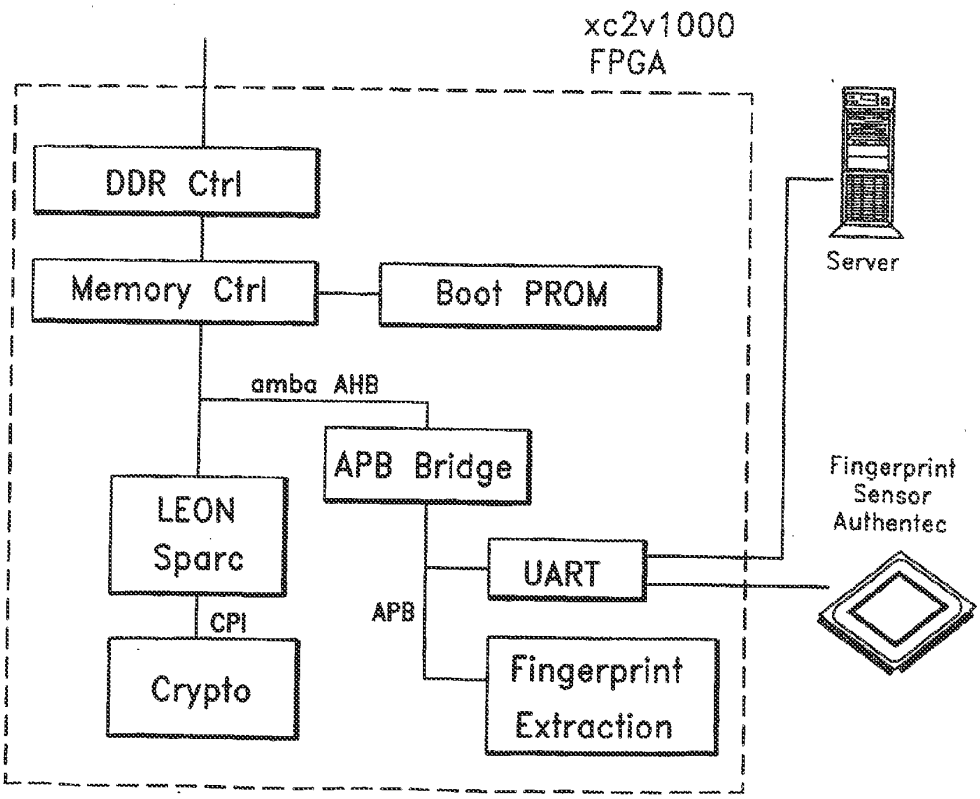


FIG. 29B

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/17545

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : G06K 9/00; H04K 1/00; H04L 9/00
US CL : 713/186; 382/115-125
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/186; 382/115-125

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 2002/0124176 A1 (Epstein) 05 September 2002) Breif Summary of the Invention and Paragraph 0022 Paragraphs 0004-0005, and 0022	1 --- 2-19
Y	US 5,602,918 (Chen et al.) 11 February 1997) Abstract, Col. 4 Lines 24-25, Col. 5 Paragraph 1, and Figs. 3A and 3B	2-19
Y	US 3,611,290 (Luisi, James) 03 June 1968 (03.06.1968) Col. 1 Lines 54-58	5, 19
Y	"Meeting Embedded Needs with Java" (Wong, William) 13 May 2002 (13.05.2002) Whole Article	6, 8
Y	US 6,705,520 B1 (Pitroda et al.) 16 March 2004 Abstract	10-12
Y	"AES Proposal: Rijndael" (Daemen et al.) 09 March 1999 (09.03.1999) Page 41 csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf	13
Y	"Radio Frequency identification (RFID) White Paper", ACCENTURE, 16 November 2001 (16.11.2001) Page 4 Paragraph 6	15

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
09 November 2004 (09.11.2004)

Date of mailing of the international search report
26 NOV 2004

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
Facsimile No. (703) 305-3230

Authorized officer
Matthew T Henning Peggy Harrod
Telephone No. (703)305-3900

Form PCT/ISA/210 (second sheet) (January 2004)

Electronic Acknowledgement Receipt

EFS ID:	41410873
Application Number:	17123018
International Application Number:	
Confirmation Number:	1102
Title of Invention:	AUTHENTICATION TRANSLATION
First Named Inventor/Applicant Name:	Bjorn Markus Jakobsson
Customer Number:	21912
Filer:	Yeu-Ting George Cheng/Elaine Nguyen
Filer Authorized By:	Yeu-Ting George Cheng
Attorney Docket Number:	MJAKP026
Receipt Date:	16-DEC-2020
Filing Date:	
Time Stamp:	21:40:43
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	MJAKP026_IDS_01_SB08.pdf	1054595 a4501a7bc2358b5ac282a24877fdb6f832da5688	no	6

Warnings:

Information:					
2	Foreign Reference	WO2004051585.pdf	3578264 8715602740 2a88c2d845ed0f73d5f019d11e0aff	no	74
Warnings:					
Information:					
3	Foreign Reference	WO2005001751.pdf	2476614 2905f4719af8c9f962b80b9e5fb1f76681de6904	no	76
Warnings:					
Information:					
4	Non Patent Literature	Managing_Authorization_and_Access_Control_2005-11-03.pdf	1390206 cc53d83dfbb57b3b783097a3252db4e9460c3517	no	12
Warnings:					
Information:					
5	Non Patent Literature	BRANDS_ET_AL_Distance_Bounding_Protocols_1994-01-28.pdf	723819 1ac3a57c7e2839cdabe382478e9d9f4be818b918	no	16
Warnings:					
Information:					
6	Non Patent Literature	Hammer_Lahav_Ed_The_OAuth_1_0_Protocol_2020-04.pdf	135818 1cad51385d3e5e39e1505acb82a625472cdfaf2c	no	39
Warnings:					
Information:					
7	Non Patent Literature	JAKOBSSON_ET_AL_Proving_Without_Knowing_1996-07-24.pdf	701228 f7f7823c45029455d73275dbf32d70e90751b655	no	15
Warnings:					
Information:					
8	Non Patent Literature	MONROSE_ET_AL_Using_Voice_to_Generate_Cryptographic_Keys_2001-05-13.pdf	307139 9d4c27c0698d3b58e9ff896ac1aa9954425b0466	no	6
Warnings:					
Information:					

9	Non Patent Literature	SESHADRI_ET_AL_Pioneer_Verifying_Code_Integrity_2005-10-23.pdf	395507 394e8151298c5debddea0fccaab105d3981d57ee	no	16
Warnings:					
Information:					
			Total Files Size (in bytes):	10763190	

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

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

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	MJAKP026
	Application Number	
Title of Invention	AUTHENTICATION TRANSLATION	

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

Secrecy Order 37 CFR 5.2:

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

Inventor Information:

Inventor 1 — Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Bjorn	Markus	Jakobsson	

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

City	Portola Valley	State/Province	CA	Country of Residence	US

Mailing Address of Inventor:

Address 1	118 Ramona Rd.
Address 2	

City	Portola Valley	State/Province	CA
Postal Code	94028	Country	US

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

Correspondence Information:

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

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

Customer Number	21912		
Email Address		Add Email	Remove Email

Application Information:

Title of the Invention	AUTHENTICATION TRANSLATION		
Attorney Docket Number	MJAKP026	Small Entity Status Claimed	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	15	Suggested Figure for Publication (if any)	

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

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	MJAKP026
	Application Number	
Title of Invention	AUTHENTICATION TRANSLATION	

Filing By Reference:

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

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

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

Publication Information:

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

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

Representative Information:

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

Please Select One:	● Customer Number	US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	21912		

Domestic Benefit/National Stage Information:

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

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Continuation in part of	17027481	2020-09-21

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

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	MJAKP026
	Application Number	
Title of Invention	AUTHENTICATION TRANSLATION	

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
17027481	Continuation of	16773767	2020-01-27

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
16773767	Continuation of	16563715	2019-09-06	10824696	2020-11-03

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
16563715	Continuation of	16273797	2019-02-12	10521568	2019-12-31

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
16273797	Continuation of	15042636	2016-02-12	10360351	2019-07-23

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
15042636	Continuation of	13706254	2012-12-05	9294452	2016-03-22

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13706254	Claims benefit of provisional	61587387	2012-01-17

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13706254	Claims benefit of provisional	61569112	2011-12-09

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

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

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

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	MJAKP026
	Application Number	
Title of Invention	AUTHENTICATION TRANSLATION	

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

Remove

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

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

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

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

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	MJAKP026
	Application Number	
Title of Invention	AUTHENTICATION TRANSLATION	

Authorization or Opt-Out of Authorization to Permit Access:

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

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

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

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

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

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

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

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

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

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

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

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

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	MJAKP026
	Application Number	
Title of Invention	AUTHENTICATION TRANSLATION	

Applicant Information:

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

Applicant 1 Remove

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

Clear

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

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

Name of the Deceased or Legally Incapacitated Inventor:

If the Applicant is an Organization check here. ☒

Organization Name	RightQuestion, LLC		
Mailing Address Information For Applicant:			
Address 1	118 Ramona Rd.		
Address 2			
City	Portola Valley	**State/Province**	CA
Country	US	Postal Code	94028
Phone Number		Fax Number	
Email Address			

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

Assignee Information including Non-Applicant Assignee Information:

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

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

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	MJAKP026
	Application Number	
Title of Invention	AUTHENTICATION TRANSLATION	

Assignee 1

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

Remove

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

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

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

Remove

Signature:

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

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

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

Signature	/Yeu-Ting George Cheng/			Date (YYYY-MM-DD)	2020-12-15
First Name	Yeu-Ting George	Last Name	Cheng	Registration Number	69408

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

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

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	MJAKP026
	Application Number	
Title of Invention	AUTHENTICATION TRANSLATION	

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

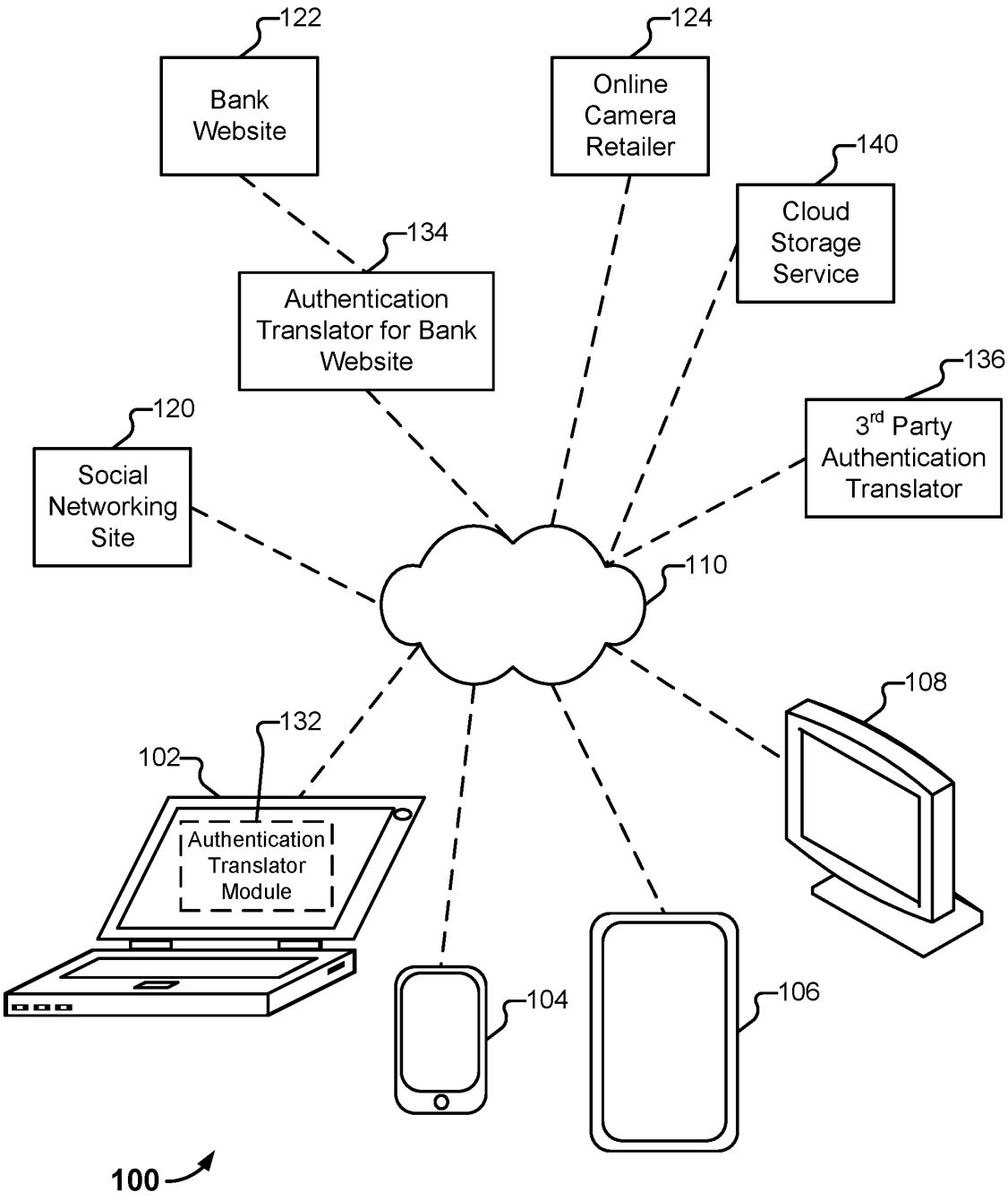

122
Bank Website
124
Online Camera Retailer
140
Cloud Storage Service
134
Authentication Translator for Bank Website
136
3rd Party Authentication Translator
120
Social Networking Site
110
108
132
102
Authentication Translator Module
104
106
100

FIG. 1

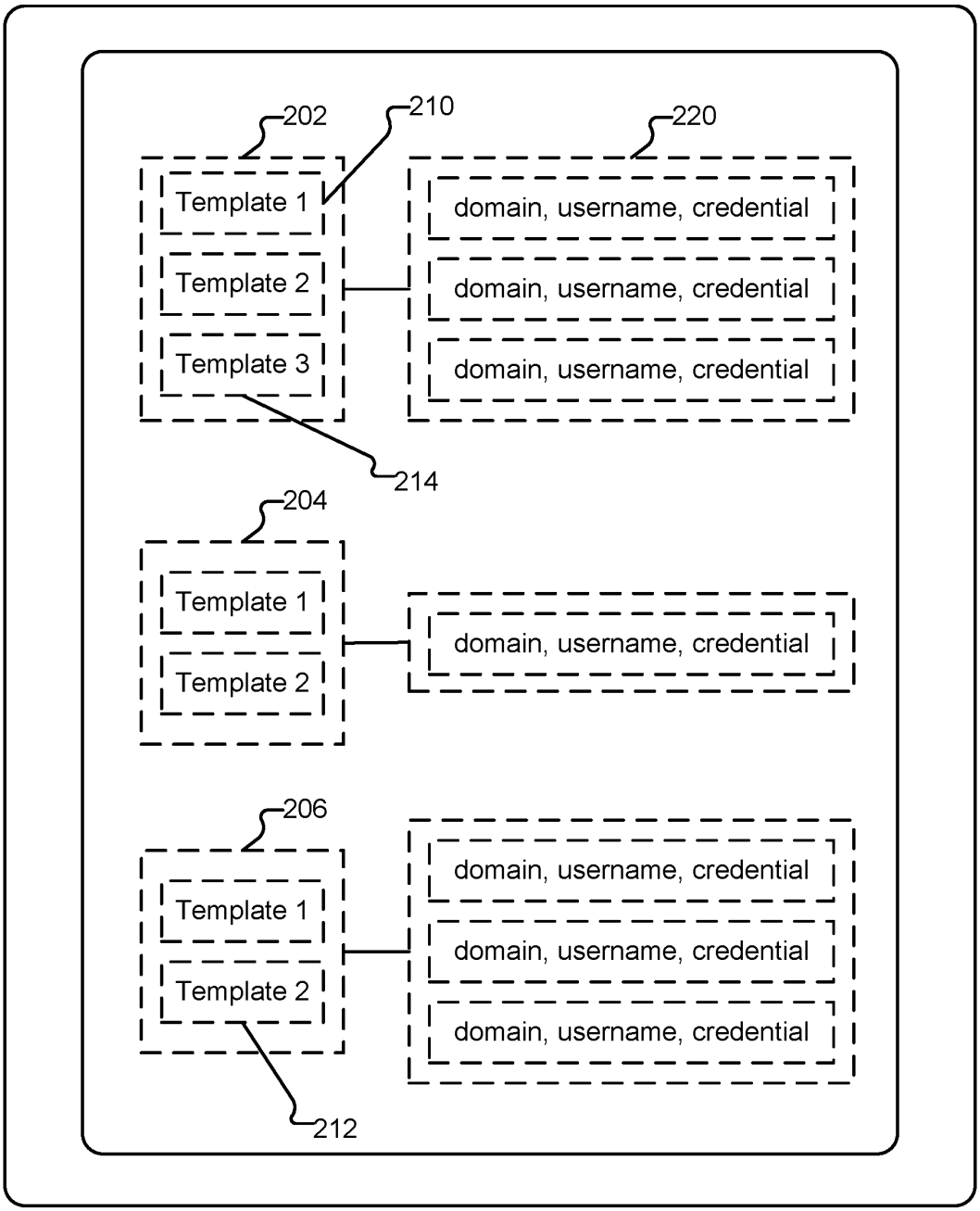

202
210
220
Template 1
Template 2
Template 3
domain, username, credential
domain, username, credential
domain, username, credential
214
204
Template 1
Template 2
domain, username, credential
206
Template 1
Template 2
domain, username, credential
domain, username, credential
domain, username, credential
212
200

FIG. 2

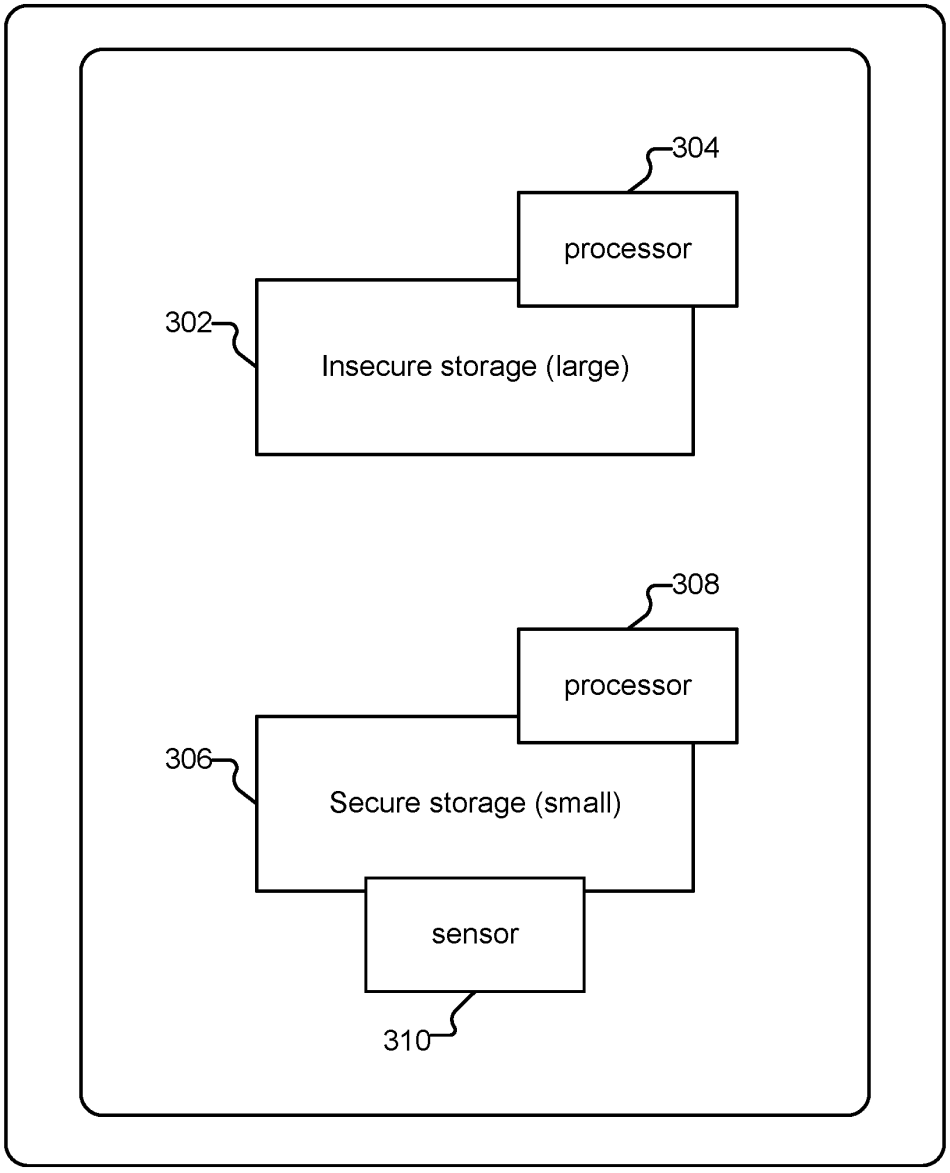

304
processor
302
Insecure storage (large)
308
processor
306
Secure storage (small)
sensor
310
300

FIG. 3

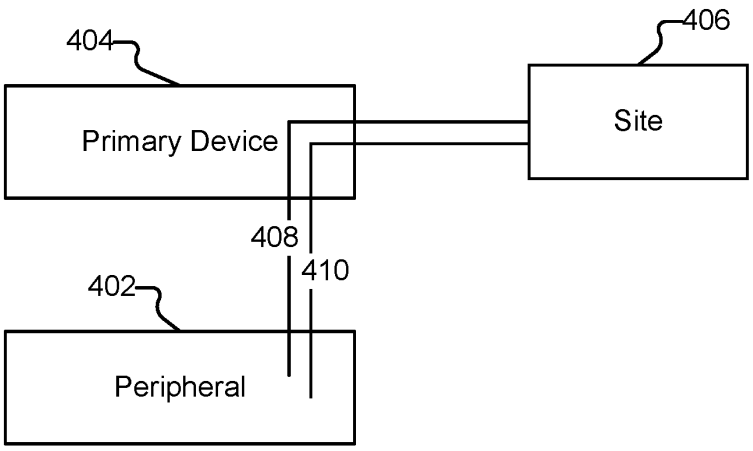


FIG. 4

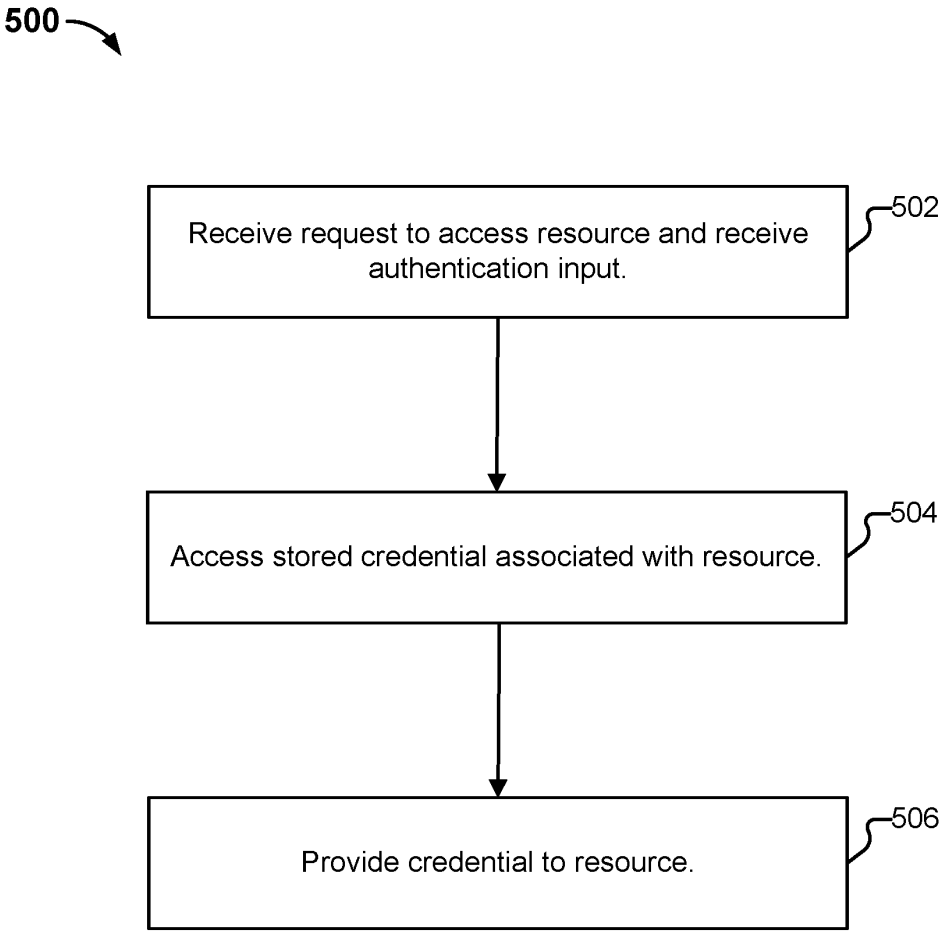

500
Receive request to access resource and receive authentication input.
502
Access stored credential associated with resource.
504
Provide credential to resource.
506

FIG. 5

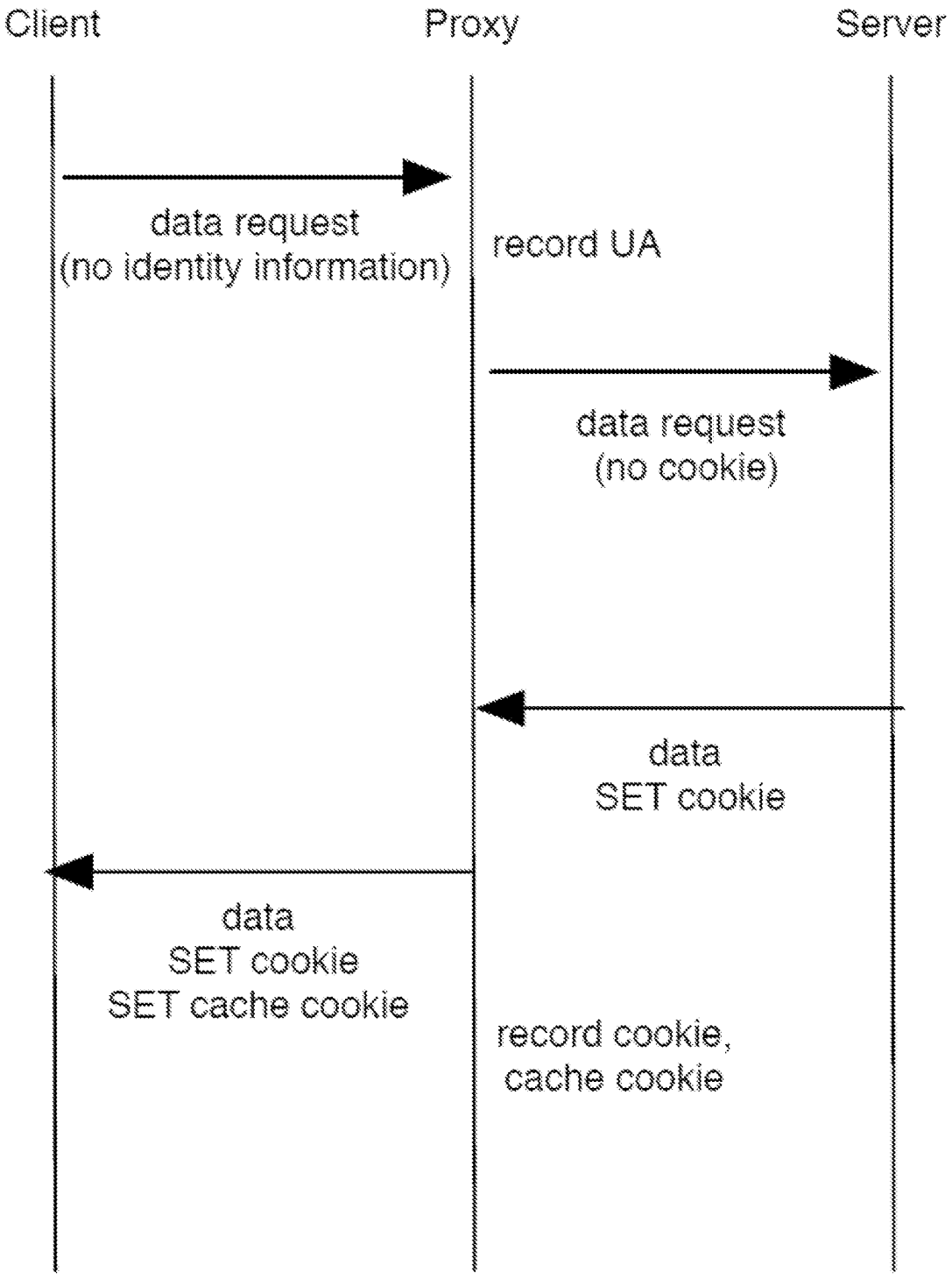

Client
Proxy
Server
data request
(no identity information)
record UA
data request
(no cookie)
data
SET cookie
data
SET cookie
SET cache cookie
record cookie,
cache cookie

FIG. 6

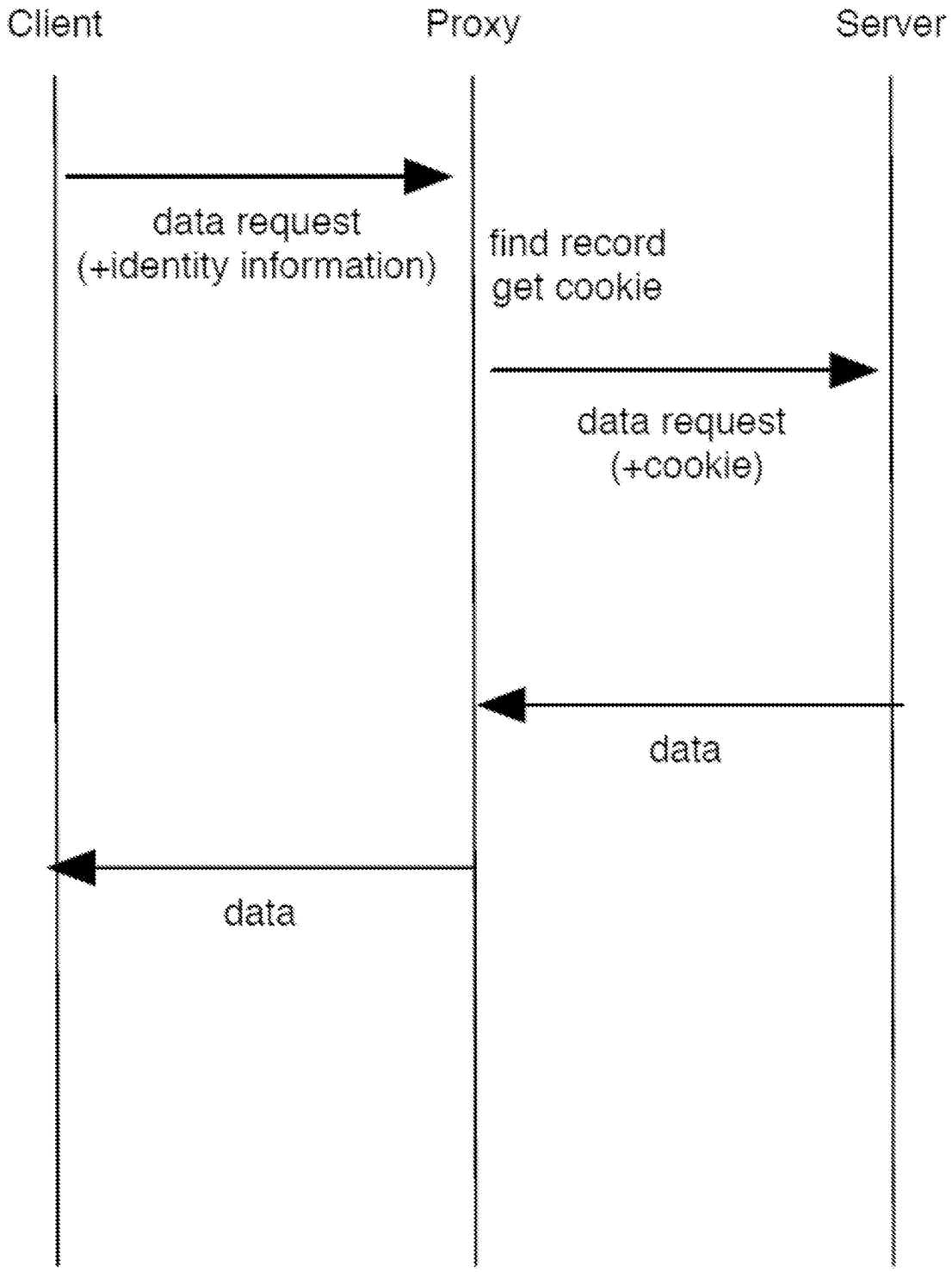

Client
Proxy
Server
data request
(+identity information)
find record
get cookie
data request
(+cookie)
data
data

FIG. 7

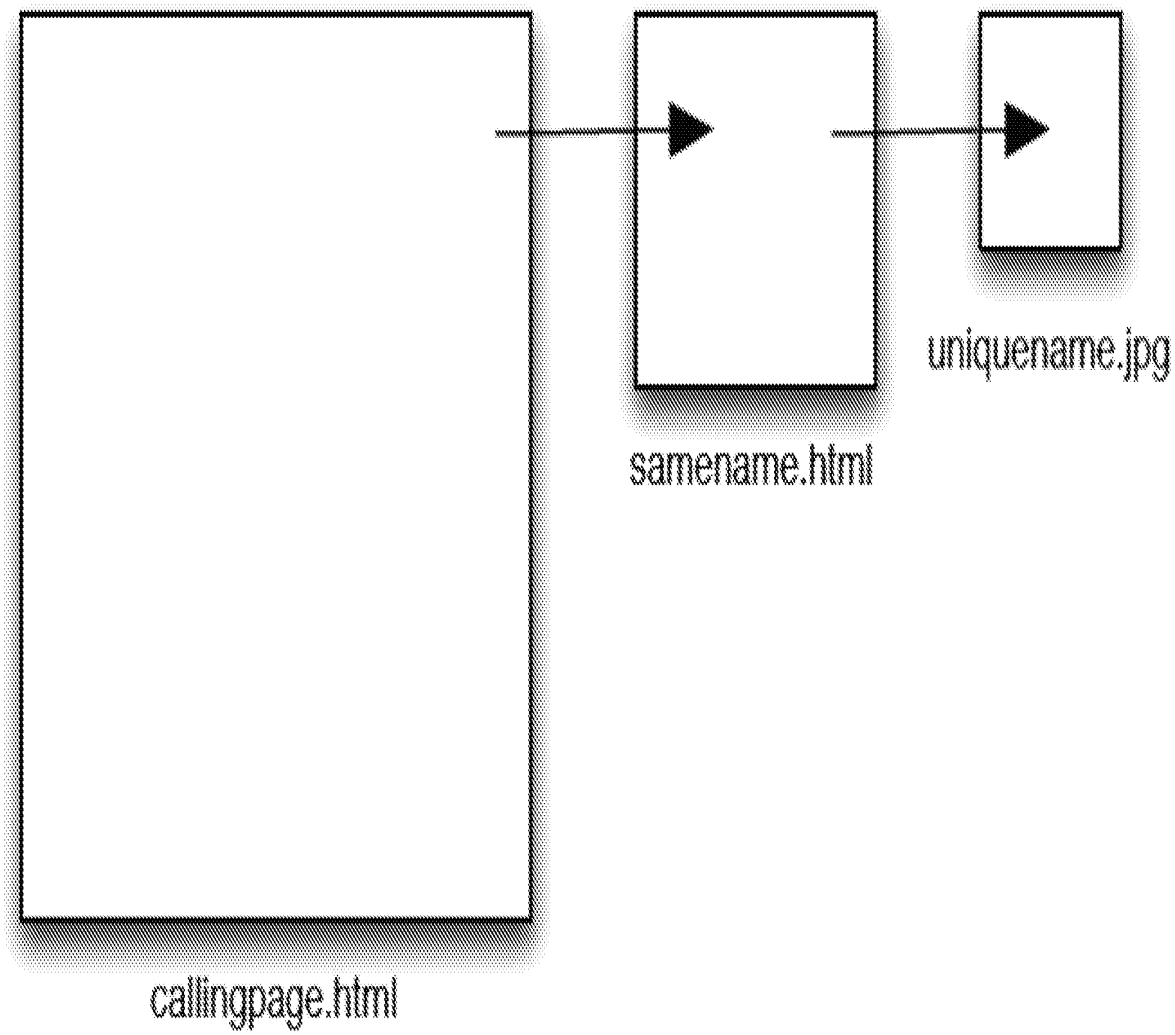


FIG. 8

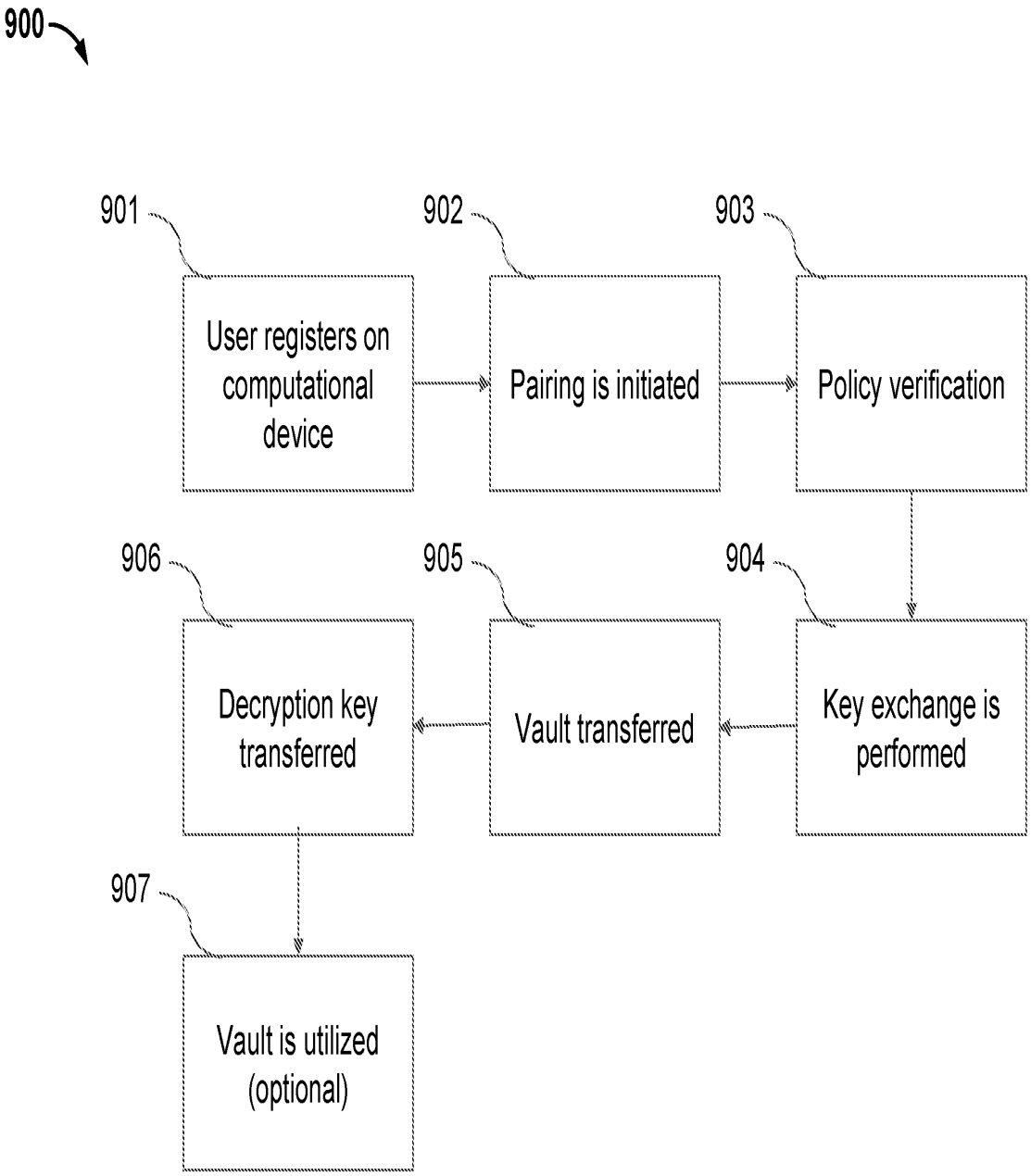

900
901
User registers on computational device
902
Pairing is initiated
903
Policy verification
904
Key exchange is performed
905
Vault transferred
906
Decryption key transferred
907
Vault is utilized (optional)

FIG. 9

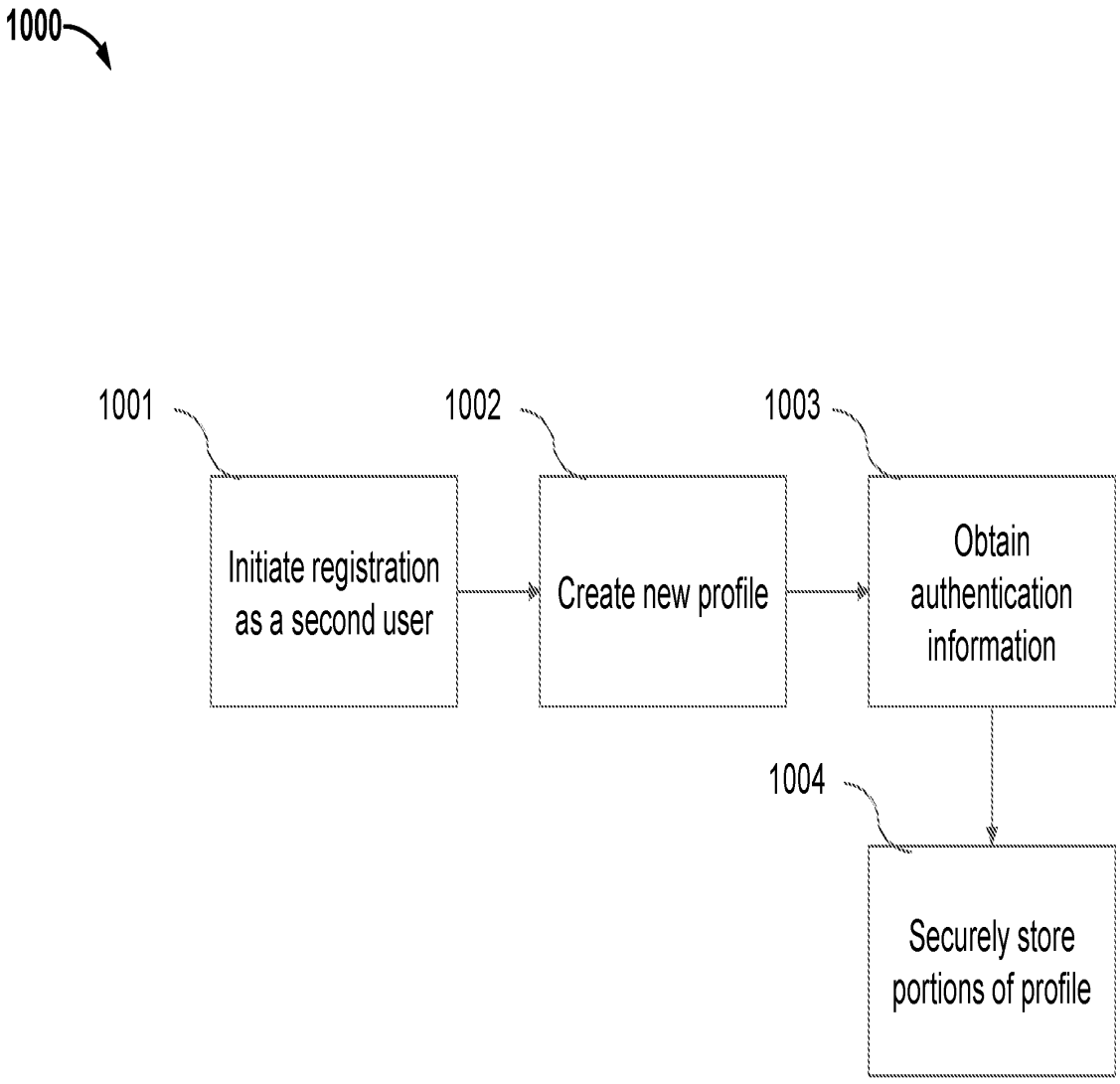

1000
1001
1002
1003
Initiate registration as a second user
Create new profile
Obtain authentication information
1004
Securely store portions of profile

FIG. 10

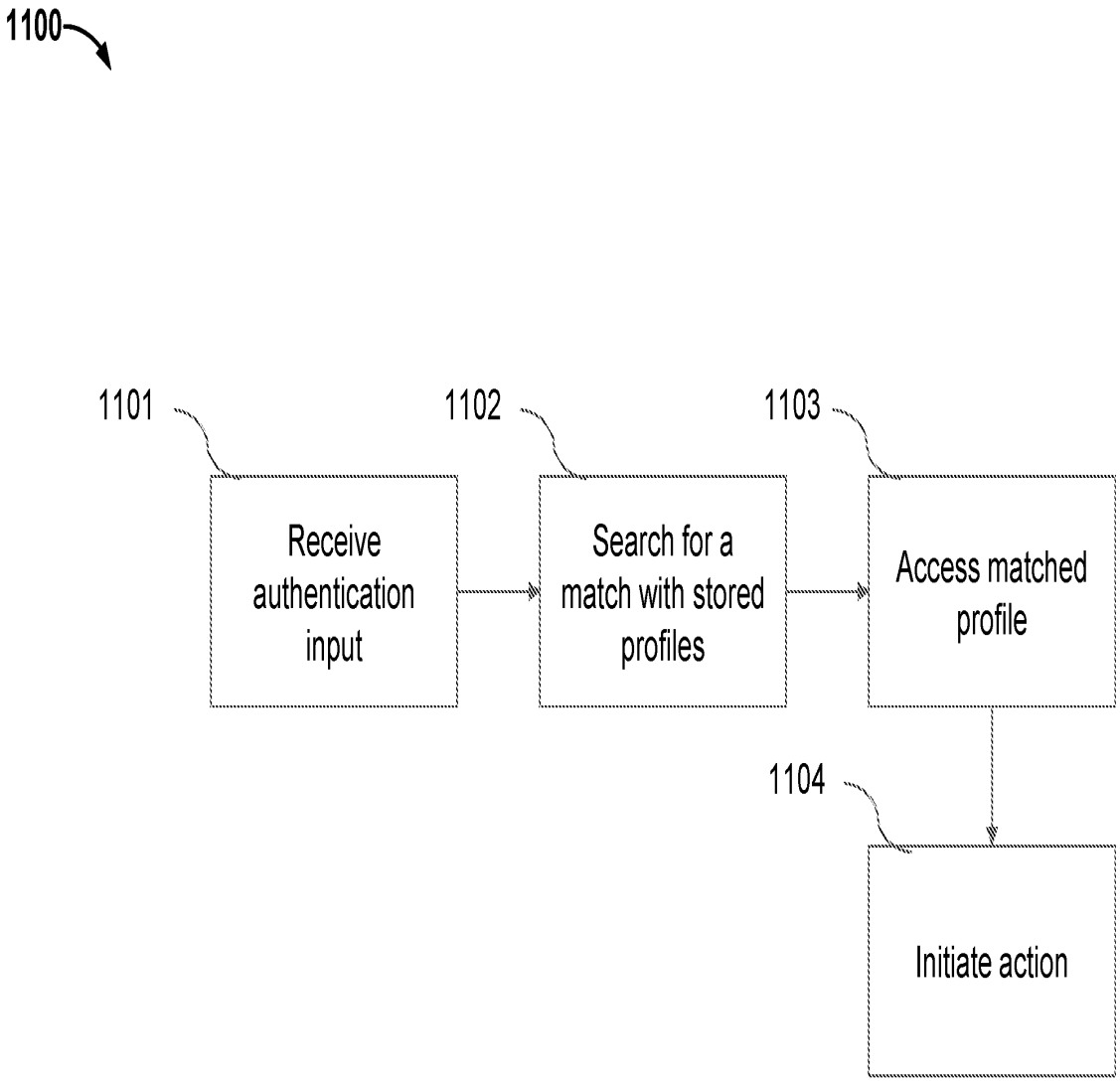

1100
1101
1102
1103
Receive authentication input
Search for a match with stored profiles
Access matched profile
1104
Initiate action

FIG. 11

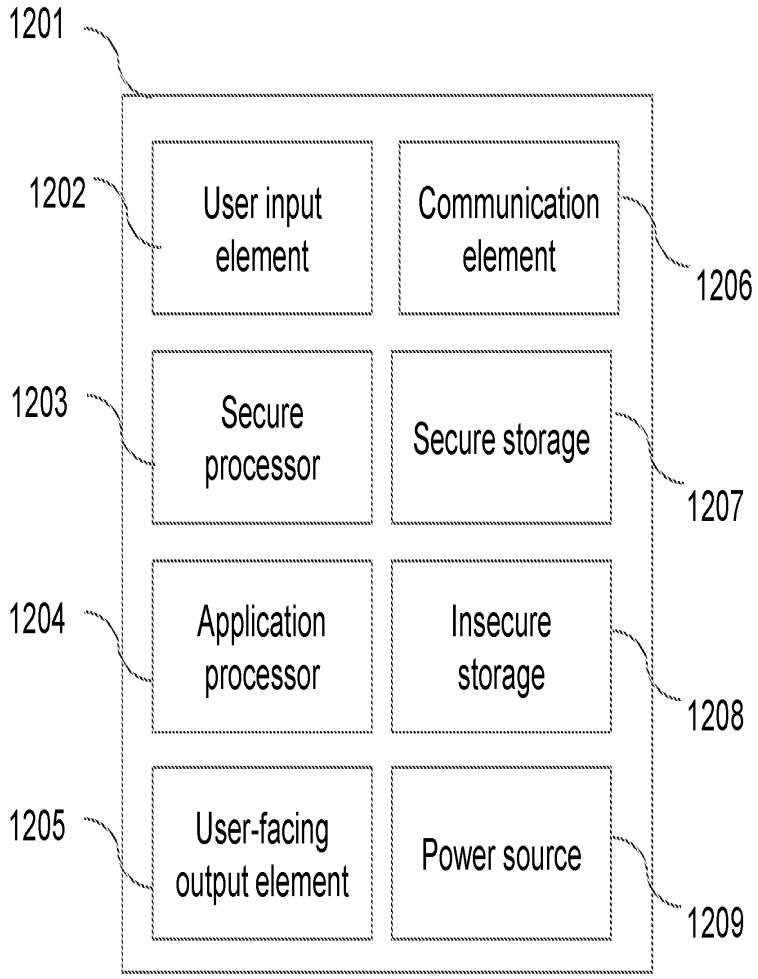

1201
1202
User input element
Communication element
1206
1203
Secure processor
Secure storage
1207
1204
Application processor
Insecure storage
1208
1205
User-facing output element
Power source
1209

FIG. 12

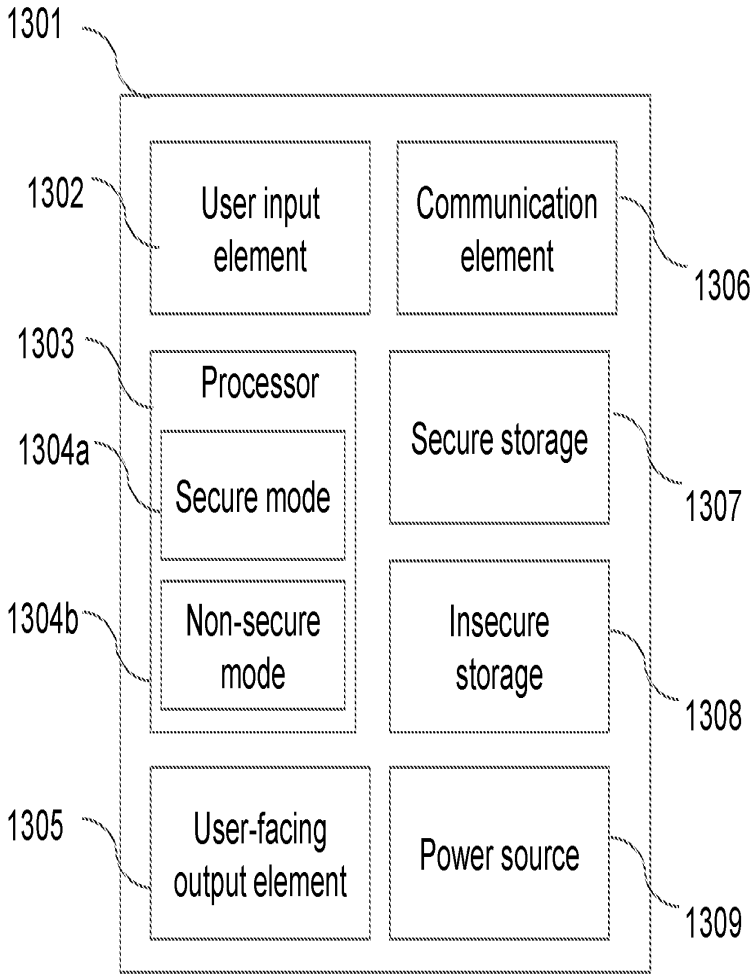
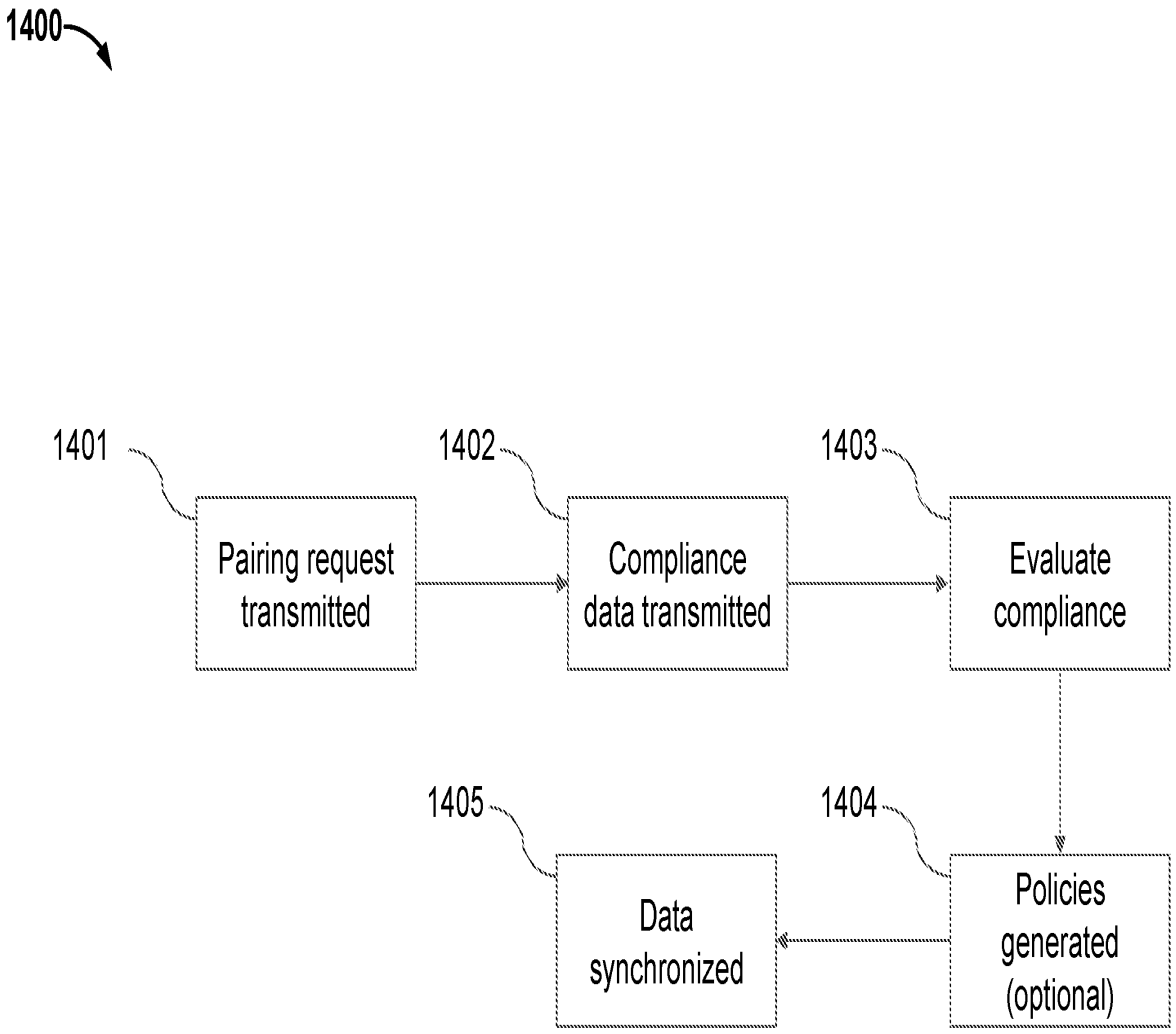

1301
1302
User input element
Communication element
1306
1303
Processor
1304a
Secure mode
Secure storage
1307
1304b
Non-secure mode
Insecure storage
1308
1305
User-facing output element
Power source
1309

FIG. 13


1400
1401
Pairing request transmitted
1402
Compliance data transmitted
1403
Evaluate compliance
1404
Policies generated (optional)
1405
Data synchronized

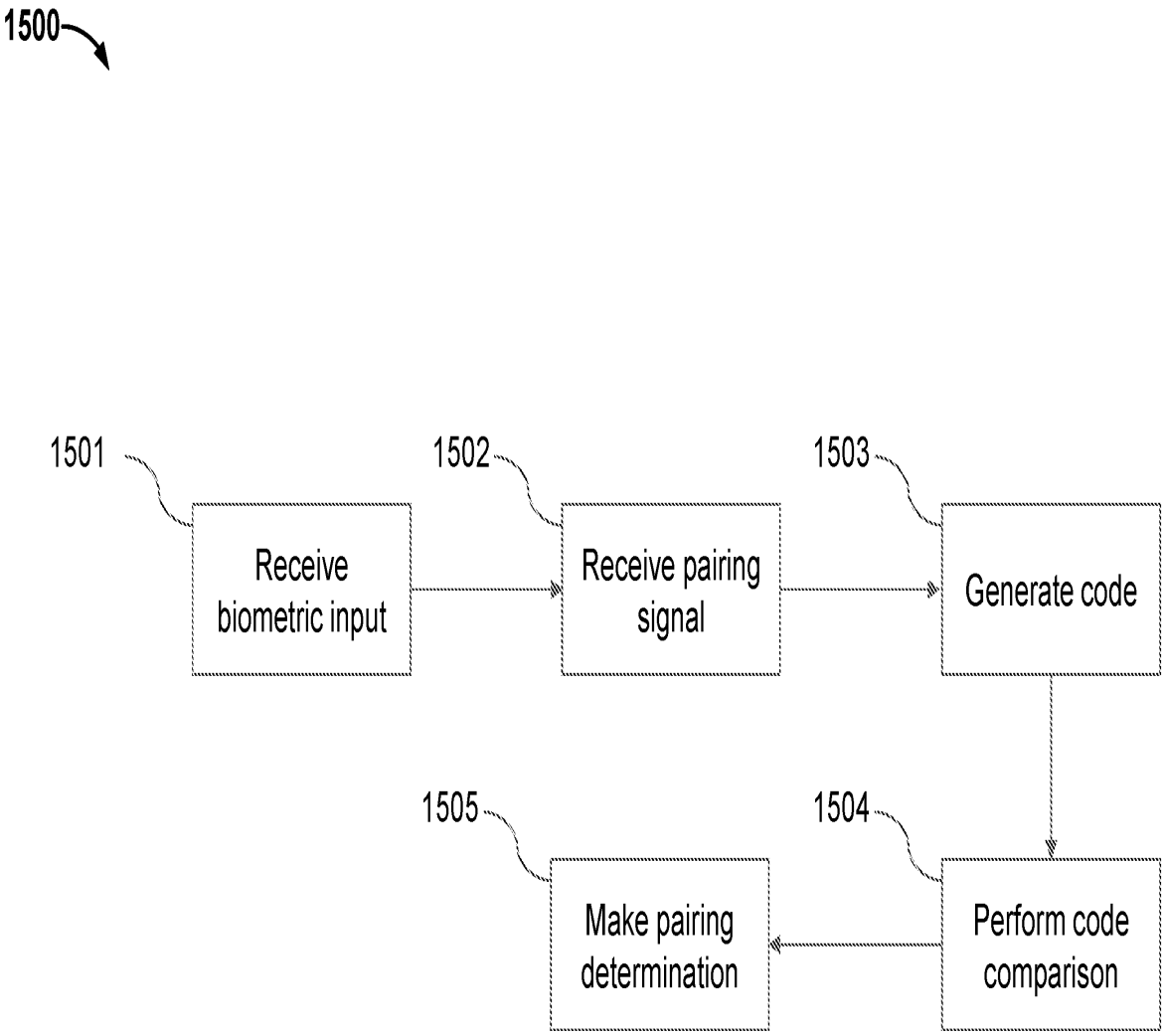

1500
1501
Receive biometric input
1502
Receive pairing signal
1503
Generate code
1504
Perform code comparison
1505
Make pairing determination

FIG. 15

Electronic Acknowledgement Receipt

EFS ID:	41396677
Application Number:	17123018
International Application Number:	
Confirmation Number:	1102
Title of Invention:	AUTHENTICATION TRANSLATION
First Named Inventor/Applicant Name:	Bjorn Markus Jakobsson
Customer Number:	21912
Filer:	Yeu-Ting George Cheng/Elaine Nguyen
Filer Authorized By:	Yeu-Ting George Cheng
Attorney Docket Number:	MJAKP026
Receipt Date:	15-DEC-2020
Filing Date:	
Time Stamp:	20:43:38
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	MJAKP026_ADS.pdf	1227106 6da91f63e9649f06a6f250768945bc8445e46457	no	9

Warnings:

Information:					
2	Specification	MJAKP026_APP.pdf	216788 004688174c02f2f87d34157595a24d7c34d1691d	no	42
Warnings:					
Information:					
3	Drawings-only black and white line drawings	MJAKP026_APP_Figures.pdf	478470 dfda84f44b129bcb5968fbde0b340690e963baf4	no	15
Warnings:					
Information:					
			Total Files Size (in bytes):	1922364	

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.

Attorney Docket No. MJAKP026

APPLICATION FOR UNITED STATES PATENT

AUTHENTICATION TRANSLATION

By Inventor(s):

Bjorn Markus Jakobsson
Portola Valley, CA
A Citizen of the United States of America

Assignee: RightQuestion, LLC

VAN PELT, YI & JAMES LLP
10050 N. Foothill Blvd., Suite 200
Cupertino, CA 95014
Telephone (408) 973-2585

AUTHENTICATION TRANSLATION

CROSS REFERENCE TO OTHER APPLICATIONS

[0001] This application is a continuation in part of pending U.S. Patent Application No 17/027,481 entitled AUTHENTICATION TRANSLATION filed September 21, 2020, which is incorporated herein by reference for all purposes, which is a continuation of U.S. Patent Application No. 16/773,767, entitled AUTHENTICATION TRANSLATION filed January 27, 2020 which is incorporated herein by reference for all purposes, which is a continuation of U.S. Patent Application No. 16/563,715, entitled AUTHENTICATION TRANSLATION filed September 06, 2019, now U.S. Patent No. 10,824,696, which is incorporated herein by reference for all purposes, which is a is a continuation of U.S. Patent Application No. 16/273,797, entitled AUTHENTICATION TRANSLATION filed February 12, 2019, now U.S. Patent No. 10,521,568, which is incorporated herein by reference for all purposes, which is a is a continuation of U.S. Patent Application No. 15/042,636, entitled AUTHENTICATION TRANSLATION filed February 12, 2016, now U.S. Patent No. 10,360,351, which is incorporated herein by reference for all purposes, which is a continuation of U.S. Patent Application No. 13/706,254, entitled AUTHENTICATION TRANSLATION filed December 5, 2012, now U.S. Patent No. 9,294,452, which is incorporated herein by reference for all purposes, which claims priority to U.S. Provisional Application No. 61/587,387, entitled BIOMETRICS-SUPPORTED SECURE AUTHENTICATION SYSTEM filed January 17, 2012 which is incorporated herein by reference for all purposes. U.S. Patent Application No. 13/706,254 also claims priority to U.S. Provisional Patent Application No. 61/569,112 entitled BACKWARDS COMPATIBLE ROBUST COOKIES filed December 9, 2011, which is incorporated herein by reference for all purposes.

BACKGROUND OF THE INVENTION

[0002] Providing credentials to a service, whether via a mobile or other device, is often a tedious experience for a user. Unfortunately, to make authentication easier for themselves, users will often engage in practices such as password re-use, and/or the selection of poor quality passwords, which render their credentials less secure against attacks. Accordingly,

improvements in authentication techniques would be desirable. Further, it would be desirable for such improvements to be widely deployable, including on existing/legacy systems.

APPL-1002
APPLE INC. / Page 380 of 419

BRIEF DESCRIPTION OF THE DRAWINGS

[0003] Various embodiments of the invention are disclosed in the following detailed description and the accompanying drawings.

[0004] Figure 1 illustrates an embodiment of an environment in which authentication translation is provided.

[0005] Figure 2 illustrates an embodiment of credential information stored on a device.

[0006] Figure 3 illustrates an embodiment of a device with secure storage.

[0007] Figure 4 illustrates an example of a renegotiation.

[0008] Figure 5 illustrates an embodiment of a process for performing authentication translation.

[0009] Figure 6 illustrates an example of what occurs when a client device first visits the site of a legacy server via an authentication translator.

[0010] Figure 7 illustrates an example of what occurs when a device subsequently visits the site of a legacy server via an authentication translator.

[0011] Figure 8 shows the structure of an example of a cache cookie used in some embodiments.

[0012] Figure 9 is a flow diagram illustrating an embodiment of a backup process.

[0013] Figure 10 is a flow diagram illustrating an embodiment of a process of a user registering as a second user on a computational device.

[0014] Figure 11 is a flow diagram illustrating an embodiment of a process an authentication attempt on a computational device.

[0015] Figure 12 illustrates an embodiment of a computational device.

[0016] Figure 13 illustrates an embodiment of a computational device.

[0017] Figure 14 is a flow diagram illustrating an embodiment of a backup process between two computational devices.

[0018] Figure 15 is a flow diagram illustrating an embodiment of a pairing process.

DETAILED DESCRIPTION

[0019] The invention can be implemented in numerous ways, including as a process; an apparatus; a system; a composition of matter; a computer program product embodied on a computer readable storage medium; and/or a processor, such as a processor configured to execute instructions stored on and/or provided by a memory coupled to the processor. In this specification, these implementations, or any other form that the invention may take, may be referred to as techniques. In general, the order of the steps of disclosed processes may be altered within the scope of the invention. Unless stated otherwise, a component such as a processor or a memory described as being configured to perform a task may be implemented as a general component that is temporarily configured to perform the task at a given time or a specific component that is manufactured to perform the task. As used herein, the term 'processor' refers to one or more devices, circuits, and/or processing cores configured to process data, such as computer program instructions.

[0020] A detailed description of one or more embodiments of the invention is provided below along with accompanying figures that illustrate the principles of the invention. The invention is described in connection with such embodiments, but the invention is not limited to any embodiment. The scope of the invention is limited only by the claims and the invention encompasses numerous alternatives, modifications and equivalents. Numerous specific details are set forth in the following description in order to provide a thorough understanding of the invention. These details are provided for the purpose of example and the invention may be practiced according to the claims without some or all of these specific details. For the purpose of clarity, technical material that is known in the technical fields related to the invention has not been described in detail so that the invention is not unnecessarily obscured.

[0021] Figure 1 illustrates an embodiment of an environment in which authentication translation is provided. In the example shown, a variety of client devices 102-108 connect, via one or more networks (represented as a single network cloud 110) to a variety of services 120-124 (also referred to herein as sites 120-124). In particular, client device 102 is a notebook computer owned by a user hereinafter referred to as Alice. Notebook 102 includes a camera, a microphone, and a fingerprint sensor. Client device 104 is a smartphone, also owned by Alice.

Client device 104 includes a camera. Client device 106 is a tablet owned by Bob, and sometimes used by Bob's son Charlie. Client device 106 includes a camera and a fingerprint sensor. Client device 108 is a kiosk located in the lobby of a hotel. Kiosk 108 includes a camera and a microphone. The techniques described herein can be used with or adapted to be used with other devices, as applicable. For example, the techniques can be used in conjunction with gaming systems, with peripheral devices such as mice, and with embedded devices, such as door locks.

[0022] Service 120 is a social networking site. Service 122 is a website of a bank. Service 124 is the online store of a boutique camera retailer. Each of services 120-124 requires a username and password (and/or a cookie) from a user prior to giving that user access to protected content and/or other features. As will be described in more detail below, using the techniques described herein, users need not type such usernames and passwords into their devices whenever required by a service. Instead, users can authenticate themselves to an "authentication translator" via an appropriate technique, and the authentication translator will provide the appropriate credentials to the implicated service on the user's behalf. Also as will be described in more detail below, authentication translators can be located in a variety of places within an environment. For example, notebook computer 102 includes an authentication translator module 132 that provides authentication translation services. The other devices 104-108 can also include (but need not include) their own respective authentication translator modules. The owner of bank website 122 also operates an authentication translator 134 associated with the bank. Finally, authentication translator 136 provides authentication translation services to a variety of businesses, including online camera retailer 124.

[0023] Figure 2 illustrates an embodiment of credential information stored on a device. In particular, device 200 stores three user profiles 202-206, each of which contains a username and one or more templates (e.g., template 210) associated with the user. In various embodiments, a template is a collection of biometric features. Using fingerprints as an example type of biometric, a corresponding template includes a collection of patterns, minutia, and/or other features that can be matched against to determine if a person's fingerprint matches the fingerprint of the registered user (i.e., the owner of a given user profile). A representation of a single fingerprint may be included in multiple templates (e.g., in different resolutions, in accordance with different protocols, as captured during warm vs. cold conditions, and/or by itself

or in combination with multiple fingerprints). When other biometrics are employed (e.g., facial recognition, voiceprint, or retina scan technology), features appropriate to those types of biometrics are included in the template. Other types of features can also be included in templates. As one example, a user's typing speed and/or accuracy can be measured by a device, such as device 102, and used to distinguish between multiple users of a device. For example, suppose Alice types at 100 words per minute and rarely makes mistakes. A representation of this information can be stored in template 212. Also suppose Alice's niece, who sometimes uses Alice's laptop computer when visiting Alice types at 20 words per minute and makes many mistakes. In some embodiments, the fact that a user was recently (e.g., within the last 5 minutes) typing on laptop 102 at 90 words per minute is evidence of a match against template 212. In this case, the typing speed of 90 words per minute is similar enough to Alice's typical behavior, it is considered a match. Various policies can be included in a profile that govern how matches are to be performed. For example, policies can specify thresholds/tolerances for what constitutes a match, and can specify that different levels of matches can result in different levels of access to different resources.

[0024] A profile is associated with a vault (e.g., vault 220). The vault, in turn, contains triples specifying a service provider/domain, a username, and a credential. The vault can also contain other sensitive user information, such as account numbers, address/phone number information, and health care data. The credential for a service provider/domain can be a password (e.g., for legacy servers), and can also take alternate forms (e.g., a cryptographic key for service providers supporting stronger authentication methods).

[0025] In some embodiments, profiles, templates, and vaults (collectively "authentication information") are stored entirely in an unprotected storage area, and are stored in the clear. In other embodiments, secure storage techniques are used to secure at least a portion of the authentication information.

[0026] One example of a device with secure storage is illustrated in Figure 3. In the example shown, a mobile phone 300 includes a large and insecure storage 302 attached to a fast processor 304, and a smaller but secure storage 306 attached to a dedicated processor 308 and a sensor 310 (e.g., a camera or a fingerprint reader). Users (and applications) can read from and

write to the insecure storage area. However, users cannot access the secure storage area, and the fast processor can only communicate with the dedicated processor/sensor via a restricted API. As another example, a unique decryption key associated with a given vault can be stored in a profile. The vault is an encrypted and authenticated container that can be stored on insecure storage, e.g., on the device, and also backed up (e.g., to a cloud storage service 140 or to an alternate form of external storage). As needed, authentication information or portions thereof can be loaded into secure storage and decrypted. For example, one can use AES to encrypt the files one by one, using a key stored on the secured storage. A message authentication technique, such as HMAC, can be used for authenticating the encrypted files to provide tamper prevention. Profiles and vaults can be updated while in secure storage; if this occurs, they are encrypted and MACed before being written back to the insecure storage, which may in turn propagate them to external backup storage. In yet other embodiments, profiles and vaults are stored entirely in secure storage, in plaintext, which allows them to be both read and written -- and in particular, searched.

[0027] **Example Transaction Types**

[0028] A variety of transaction types can take place in the environment shown in Figure 1, examples of which are discussed in this section.

[0029] Initial Registration

[0030] In order to begin using the techniques described herein, users perform some form of initial registration. As one example, suppose Alice launches an enrollment program installed on laptop 102. She uses the program to capture various biometric information (e.g., fingerprints, photographs of her face, etc.). A user profile is created for Alice, and the biometric information captured about her is encoded into a plurality of templates, such as templates 210 and 214. In some embodiments, Alice is also explicitly asked to supply credential information for services she would like to use, such as by providing the domain name of social networking site 120, along with her username and password for site 120. In other embodiments, domain/username/credential information is at least passively captured on Alice's behalf and included in one or more vaults such as vault 220. Credential information can also be important from a browser password manager already in use by Alice or other appropriate source. In some

embodiments, Alice also registers with cloud storage service 140, which will allow her to back up her authentication information and to synchronize it across her devices (e.g., 102 and 104), as described in more detail below.

[0031] Other registration approaches can also be used. For example, registration can be integrated into the experience the first time a device is used. Thus, when Bob first turns on tablet 106, he may be prompted to take a picture of his face (with a profile/templates being created in response). Similarly, the first time Charlie uses tablet 106, the techniques described herein can be used to determine that Charlie does not yet have a profile (e.g., because none of the templates already present on tablet 106 match his biometrics) and Charlie can be prompted to enroll as a second user of the device.

[0032] Authentication

[0033] Suppose Alice wishes to authenticate to banking website 122. Using a fingerprint reader incorporated into her laptop, she performs a fingerprint scan, which causes her biometric features to be extracted and compared to any stored templates residing on her computer. If a match is found, an associated decryption key is selected, and the associated vault is loaded and decrypted. The vault is scanned for an entry that matches the selected service provider (i.e., website 122). If a matching entry is found, the associated domain, username, and site credential are extracted from the vault. In some embodiments, the validity of the domain name mapping is verified at this point to harden the system against domain name poisoning. Next, a secure connection is established between Alice's computer and the service provider, and Alice is authenticated. For service providers supporting strong user authentication, mutual SSL can be used, for example. A variety of policies can be involved when performing matching. For example, to access certain domains, Alice's print may need only match template 210. To access other domains, Alice may need to match multiple templates (e.g., both 210 and 214). As another example, in order to access social networking site 120, Alice may merely need to be sitting in front of her computer, which has an integrated webcam. Even in relatively low light conditions, a match can be performed against Alice's face and features stored in a template. However, in order to access bank website 122, Alice may need a high quality photograph (i.e., requiring her to turn on a bright light) and may need to demonstrate liveness (e.g., by blinking or turning her

head). As yet another example, other contextual information can be included in policies. For example, if Alice's IP address indicates she is in a country that she is not usually in, she may be required to match multiple templates (or match a template with more/better quality features) in order to access retailer 124, as distinguished from when her IP address indicates she is at home.

[0034] In some embodiments, the biometric sensor used by a user may be a peripheral device (e.g., a mouse with an integrated fingerprint scanner that is connected to the user's primary device via USB). In such scenarios, the peripheral device may be responsible for storing at least a portion of authentication information and may perform at least some of the authentication tasks previously described as having been performed by Alice's computer. For example, instead of processors 304 and 308, and storages 302 and 306 being collocated on a single device (e.g., laptop 102), processor 304 and storage 302 may be present on a primary device, and processor 308 and storage 306 may be present on a peripheral device (e.g., that also includes a sensor, such as a fingerprint reader).

[0035] In such scenarios, once Alice's login to banking website 122 is successfully completed, the secure session can be handed over from the peripheral device to the primary device, in a way that does not allow the primary device retroactive access to the plaintext data of the transcripts exchanged between the peripheral device and the service provider. One way this can be accomplished is by renegotiating SSL keys between the peripheral device and the website, after which the newly negotiated key can be handed off from the peripheral device to the primary device. This avoids retroactive credential capture in a setting where the device is infected by malware.

[0036] An example of renegotiation is depicted in Figure 4. Specifically, after a user has successfully authenticated to a fingerprint reader, a login is performed to a service provider. Using the primary device (404) as a proxy, the peripheral fingerprint reader 402 negotiates a first SSL connection (408) with a service provider 406, over which credentials are exchanged. The proxy then renegotiates SSL (410), which replaces the old key with a new one. The new key is disclosed to the device, which then seamlessly takes over the connection with the service provider and performs the transaction protected by the authentication. The credentials exchanged during the first SSL connection cannot be accessed by device 404, since the key of the

renegotiated session is independent of the key of the original session; this provides protection against malware residing on the device. Renegotiation can be used when the primary device 404 is believed to be in a safe state when performing the negotiation of the SSL connection, but it is not known whether it is in a safe state during the transaction protected by the authentication. Renegotiation can also be used when a secure component of the primary device 404 performs the negotiation of the SSL connection and another and potentially insecure component of the primary device 404 is involved in the transaction protected by the authentication.

[0037] Figure 5 illustrates an embodiment of a process for performing authentication translation. The process begins at 502 when a request to access a resource is received, as is an authentication input. One example of the processing performed at 502 is as follows. Suppose Alice wishes to sign into social networking website 120. She directs a web browser application installed on client 102 to the social networking website. Authentication translator module 132 recognizes, from the context of Alice's actions (e.g., that she is attempting to access site 120 with her browser) that she would like to access a particular resource. Authentication translator module 132 prompts Alice (e.g., by a popup message or via a sound) to provide biometric information (e.g., to use the integrated fingerprint reader on her laptop). In some embodiments, the translator module does not prompt Alice, for example, because Alice has been trained to provide biometric information automatically when attempting to access certain resources. In yet other embodiments, the translator module only prompts Alice if she fails to provide acceptable biometric information within a timeout period (e.g., 30 seconds).

[0038] Module 132 compares Alice's supplied biometric data to the templates stored on her computer. If a suitable match is found, and if an entry for site 120 is present in the applicable vault, at 504, a previously stored credential associated with the resource is accessed. In particular, the username and password for the website, as stored in a vault, such as vault 220, are retrieved from the vault.

[0039] Finally, at 506, the credential is provided to the resource. For example, Alice's username and password for site 120 are transmitted to site 120 at 506. The credential can be transmitted directly (e.g., by the module or by Alice's computer) and can also be supplied

indirectly (e.g., through the use of one or more proxies, routers, or other intermediaries, as applicable).

[0040] Other devices can also make use of process 500 or portions thereof. For example, when Alice launches a banking application on phone 104, implicit in her opening that application is her desire to access the resources of website 134. The application can take Alice's picture and compare it to stored templates/vault information. If an appropriate match is found, a credential can be retrieved from the vault on her phone (or, e.g., retrieved from cloud storage service 140) and provided to website 134.

[0041] As another example, suppose Charlie is using tablet 106 and attempts to visit site 120, whether via a dedicated application or via a web browser application installed on the tablet. Charlie's photograph is taken, and then compared against the profiles stored on tablet 106 (e.g., both Bob and Charlie's profiles). When a determination is made that Charlie's photograph matches a template stored in his stored profile (and not, e.g., Bob's), Charlie's credentials for site 120 are retrieved from a vault and transmitted by an authentication translator module residing on client 106.

[0042] As yet another example, kiosk 108 can be configured to provide certain local resources (e.g., by displaying a company directory or floor plan on demand) when users speak certain requests into a microphone. Enrolled users (e.g., with stored voiceprint or facial recognition features) can be granted access to additional/otherwise restricted services in accordance with the techniques described herein and process 500.

[0043] New device

[0044] In some embodiments, to register a new device, a user provides an identifier, such as a username or an account number to the device. The new device connects to an external storage (such as cloud storage 140), provides the user identifier and credential, and downloads the user's templates/vaults from the service. In some embodiments, the templates/vaults are encrypted. Once downloaded, the template is decrypted and stored in a secure storage area, while the still encrypted vault can be stored in insecure storage. The decryption key can be generated from information the user has/knows, or from biometric data -- such as features

extracted from fingerprinting of all ten fingers. In some embodiments, more arduous fingerprinting is required for the setup of a new device than for regular authentication to avoid that a new device gets registered by a user thinking she is merely authenticating -- or worse still, simply touching the device. Moreover, it translates into higher entropy of the decryption keys.

[0045] Backup Authentication

[0046] Backup authentication allows a user, such as Alice, to access resources in the event she is unable to or unwilling to interact with a particular biometric sensor. As one example, instead of having a single template associated with her profile, Alice can have multiple templates associated with it, e.g., where the first template includes fingerprint features and the second template includes voice biometric, facial recognition, or iris detection features. As a second example, where the service Alice is connecting to is a legacy website (i.e., one that users authenticate to using usernames and passwords), such a service would allow the use of passwords and password reset mechanisms by Alice without requiring Alice to use a fingerprint reader.

[0047] In various embodiments, environment 100 supports the ability of users (e.g., under duress) to release the contents of their vaults. For example, if Alice was physically threatened with the loss of a finger by a criminal, Alice could instead release the contents of her vault(s) – the ultimate goal of the criminal. As one example, in the event Alice supplies all 10 fingerprints to the sensor, provides a special password, or supplies a fingerprint and a second identifier, a cleartext version of her vault(s) could be made available.

[0048] Access Policies

[0049] In various embodiments, cloud storage service 140 is configured to accept backups from multiple devices associated with a single account, and synchronize the updates so that all devices get automatically refreshed. For example, Alice's laptop 102 and phone 104 could both communicate with cloud storage service 140 which would keep their authentication information synchronized. Refreshes can also be made in accordance with user-configured restrictions. For example, Alice's employer could prevent privileged employer data from being stored on shared personal devices, or on any device that was not issued by the employer. As

another example, arbitrary policies can be defined regarding the access to and synchronization of software and data, and to tie a license or access rights to a person (and her fingerprint) rather than to a device. As yet another example, in some embodiments (e.g., where a device is made publicly available or otherwise shared by many users), no or a reduced amount of authentication information resides on a device, and at least a portion of authentication information is always retrieved from cloud storage service 140.

[0050] Remote wiping

[0051] Remote wiping of a user's authentication information (e.g., templates) can be used both to "unshare" previously shared devices (e.g., where Bob and Charlie both have user profiles on their shared tablet 106), and to avoid that criminals with physical component access to lost devices gain access to templates and vault contents. In some embodiments, polices such as ones where a template self-wipes if it is not matched within a particular duration of time are supported. Since user data can be frequently backed up to the cloud storage, and recovered from this using the new device registration process, inconvenience to the user will be minimized.

[0052] **Legacy Server Support**

[0053] New authentication schemes typically require changes to a significant codebase residing with service providers. If the code is well written and documented, such changes may be relatively simple. Commonly, though, this may not be so. The engineers who originally wrote the code of relevance may have long since left the company; the code they left behind may be poorly documented -- if documented at all. In severe cases, the legacy code may have been written in an outdated programming language or written in a way that does not follow guidelines for good code. This makes updates to the codebase impractical or virtually impossible in many common cases. Even if none of these challenges complicate the desired modifications, it is commonly a great bureaucratic burden to obtain permission to make modifications (e.g., to store an extra field in a backend database), because every affected part of the organization may need to review the request.

[0054] As will be described in the following section, the technologies described herein can be used in conjunction with legacy servers (e.g., existing servers that rely on usernames and

passwords to authenticate users), and in particular, can be used without requiring modification to such legacy servers.

[0055] Cookies

[0056] Cookies are commonly used by legacy servers for user authentication. Unfortunately, cookies have several problems. For one thing, they are sometimes deleted -- whether explicitly/intentionally by the end user or by the user's software. In addition, cookies are commonly stolen. Approaches such as cache cookies and identification using user agents can be more resistant to these problems, however, they have their own problems. For example, their use requires new code and new fields in the credential database stored by the server.

[0057] In some embodiments, authentication translators, such as translators 134 and 136 (also referred to herein as proxies) provide authentication translation services on behalf of associated services. Translators 134 and 136 are illustrated as single logical devices in Figure 1. In some embodiments, the translators comprise standard commercially available server hardware (e.g., a multi-core processor, 4+ Gigabytes of RAM, and one or more Gigabit network interface adapters) and run typical server-class operating systems (e.g., Linux). Translators 134 and 136 can also be implemented using a scalable, elastic architecture and may comprise several distributed components, including components provided by one or more third parties. For example, translators 134 and 136 may store user credential information or may task cloud storage service 140 with storing at least a portion of that information.

[0058] In the case of authentication translator 134, service is provided with respect to bank website 122 only. Authentication translator 134 is positioned between a legacy web server (122) and the Internet (110) -- and therefore between the legacy server and any client devices. Authentication translator 134 is configured to translate traffic between the legacy server and client devices so that the client devices (and respective users) perceive the new authentication mechanism, while the legacy server remains unchanged. Authentication translator 136 works similarly, but it provides authentication translation as a third party service to multiple providers, an example of which is online camera retailer 124.

[0059] Authentication translators 134 and 136 can also perform process 500. For example, when a device transmits a request to access website 122, the request is intercepted by translator 134, as is cookie/user agent information. The received information can be used to determine a username/password associated with the device, and that information can be passed by translator 134 to website 122 on behalf of the device.

[0060] Figure 6 illustrates an example of what occurs when a client device first visits the site of a legacy server via an authentication translator. The translator (referred to in the figure as a "proxy") fails to identify the client, and passes on the request to the legacy server. The legacy server responds to the request and sets a cookie. The proxy passes on the response, including the cookie and also a cache cookie. The proxy stores the information about both these types of identifiers, along with the user agent of the client device. This triplet of information is also referred to herein as an identifier.

[0061] Figure 7 illustrates an example of what occurs when a device subsequently visits the site of a legacy server via an authentication translator. In this scenario, the device's request is accompanied by some form of identifying information. The proxy uses this information to identify the associated cookie and passes this along to the legacy server, along with the request. In some embodiments, additional processing is also involved. For example, reading a cache cookie may require user interaction. Moreover, if not all of the identifying information is present in the request, the proxy can be configured to set the missing information again by sending a corresponding request to the client device.

[0062] The translation of cache cookies and user agent information to cookies involves a two-way translation. First, when the legacy server sets a cookie, the proxy will set the two types of cookies -- both an HTML cookie and a cache cookie -- and then create a new record in which the two cookies are stored, along with the user agent information of the client device. The user agent information can include quite a bit of data associated with a browser -- such as the browser type and version, the clock skew, and the fonts that are installed. While each of these pieces of information only contributes a small amount of entropy, the collection of items can be sufficient to identify the device in most cases. Moreover, while some of these types of data may change over time -- in fact, all of them may -- they do not typically change, and when one or two of

them do, the others typically do not. When the client device is used to visit a site controlled by the legacy server, the cookie, cache cookie and user agent information are read (if available), the record identified, and the request translated and sent to the legacy server. When a legacy server requests that the user password is updated (e.g., as part of an annual or other periodic requirement), the transmission of this request to the user can be suppressed -- in which case the database of the proxy is updated to create the illusion of an update. The user can be involved in authentication as needed, e.g., if, in addition to supplying a credential, a user must also solve a CAPTCHA, the CAPTCHA can be displayed to the user (with the user's credentials being handled in accordance with the techniques described herein).

[0063] Figure 8 shows the structure of an example of a cache cookie used in some embodiments. Cache cookies can be associated with a particular webpage, just like an HTML cookie can. In the example shown in Figure 8, the proxy wishes to associate a page "calling page.html" with a cache cookie. It embeds a request for a second object, "samename.html" in callingpage.html for every visitor. However, as the cache cookie is set for one visitor, a customized samename.html is served to this visitor. The page samename.html refers to an object with a different name for each user; that object is referred to as "uniquename.jpg." The cache cookie is set by embedding the request for samename.html in callingpage.html. The client browser attempts to render this, causing a request for samename.html from the server. The server configures samename.html to refer to a uniquely named file uniquename.jpg, and serves samename.html to the client. For the client browser to render samename.html, it requests the file uniquename.jpg, which is intentionally not served. That concludes the setting of a cache cookie. As a user returns to the page callingname.html, the browser again attempts to render the entire page, which causes it to load the object samename.html from its cache. As that is rendered, the client browser requests uniquename.jpg, which is not in its cache (since it was not served previously). The server still does not serve it, but takes note of the name of the file being requested, as it identifies the client device. Note that samename.html can be displayed in a zero-sized iframe, which makes the end user unaware of it being rendered.

[0064] A cache cookie is an implementation of the typical cookie functionality that uses the client device's browser cache. Unlike user agents, it does not change over time, and like standard HTML cookies, it cannot be read by a party other than that which set it. However, like

HTML cookies, it could be deleted -- by the user clearing his or her browser cache. Cache cookies are not automatically transmitted with GET requests, unless the cache elements are embedded in the referring pages. This adds a potential round of communication in some settings. By relying on user agent information, cache cookies, and HTML cookies to identify the client device, it is much more likely that a machine will be recognized than if only HTML cookies are used.

[0065] Additional Embodiments

[0066] A user-created vault may contain, for example, one or more credentials, such as cryptographic keys, passwords or cookies. Such credentials may be used to authenticate a user or a device to an external entity, such as a service provider. Keys can also be used to enable access to data that is encrypted. The contents of the vault may be very sensitive, and in some cases are therefore protected against unwanted access. The leak of a key, for example, could enable an attacker to impersonate a user or a device, or to access privileged data that the attacker does not have the right to access. Therefore, in some cases, the contents of vaults should be protected against any exposure.

[0067] A user may become unable to use a vault, for example, if they lose the device that stores the vault. This will hinder the user to perform tasks such as job duties, and may also cause problems to the user's personal life. For example, a key stored in the vault may be used to access a job-related resource, such as a human resource database. Resources can also be of a physical nature. For example, the job-related resource that the key in the vault grants access to may be an office building, where the key is used to open a door or enable a turnstile. Similarly, personal resources may also relate to access to data or computational services, or to physical objects or boundaries.

[0068] In some embodiments, to avoid problems associated with becoming unable to access a vault, backup of vaults, in full or in part, is performed. A user has several options. One example option is to back up vaults to a cloud database or other centralized database. This may be made available to the user from, for example, their employer, or directly to the user based on a subscription or membership basis. To gain access to the cloud database or other resource, the user may for example use one out of several enrolled devices, such as phones, wearable

computers, laptop computers, or other types of devices with processors. Such user devices are collectively referred to as "processing devices"; for illustrative purposes, individual instances of such processing devices will also be referred to in the examples and embodiments described herein.

[0069] For illustrative purposes, examples involving processing devices having a user input capability are described. In various embodiments, the user input capability is in the form of a keyboard, a touch screen, a camera, a fingerprint sensor, a microphone, or another sensor usable to collect input information, where in some embodiments this input information is usable to identify the user. For example, a keyboard can be used to input a user name and password. The keyboard may also be used to determine typing patterns that can be used to identify a user. Similarly, a camera can be used to scan QR codes, which can be used for authentication purposes in lieu of passwords; the camera can also be used to take photos of the user's face, which can be used for purposes of identification.

[0070] The exemplary processing devices described herein also have a communication capability in various embodiments. Examples of such communication capabilities include but are not limited to wireless communications, such as Bluetooth; standardized interfaces, such as USB interfaces; audio communication entities, such as microphones and speakers.

[0071] In some embodiments, the processing devices include a user-facing output capability, such as a screen, a light (such as an LED), a speaker, etc., that is used to convey information to a user. In other embodiments, the processing device does not have a user-facing output capability, but instead communicates with an external entity, such as an associated computer with a user-facing output capability, where a user-facing output is rendered or otherwise conveyed. In some embodiments, the user-facing output capability is used to convey information to the user, such that the processing device is operating; that the processing device is requesting a user input; that the processing device is in a requested operating state, etc.

[0072] Two processing devices can communicate with each other, whether directly or by using other devices as intermediaries. One example type of intermediary is a cloud storage entity, which can be used to convey information from one processing device to another processing device. One example type of information that may be conveyed from one processing device to

another processing device is a vault. In some embodiments, the information conveyed further includes information usable to access the vault, identify the type or ownership of the vault, and more. In some embodiments, a user backs up vault information from a first device to a second device by causing vault information to be conveyed directly from the first device to the second device, or by using the cloud storage entity or other centralized database as an intermediary that stores the vault sent by the first device, and later sends the vault to the second device. In some embodiments, the vault protects its contents from being illegitimately accessed by using encryption. For example, the first device creates the vault by encrypting credentials to be placed in the vault using an encryption key and associated encryption algorithms. For any other device to later access the vault, it would need the corresponding decryption key and decryption algorithms. Example encryption and decryption approaches include, but are not limited to, RSA encryption, ElGamal encryption, AES encryption, and more. Some implementations may use elliptic curve methods to enable a high degree of computational efficiency.

[0073] There are various ways of securely conveying vaults or vault contents from one computational device to another. In one example case involving an intermediary such as a cloud storage or other centralized database, the vault is stored centrally, (potentially or optionally) updated, and then redistributed to one or more computational devices. These devices need to be enabled to access the contents of the vault, which in some embodiments is facilitated by obtaining a key from an originating computational device; from the cloud storage or other centralized device; from third party trusted parties; from a user operating a computational device with access to the vault contents; or a combination of these. For example, when a vault is conveyed from a first computational device to a cloud storage, and then to a second computational device, the cloud storage may play the role of initiating the second computational device, where the initiation includes the delivery of a key usable to open the vault. In some embodiments, the cloud storage entity uses a policy to determine what second computational devices are allowed to be initiated and obtains a key usable to access the content of a vault. For example, this may be limited to computational devices that have a sufficient security level associated with them. The policy may be set by a user of the first computational device, an employer of such a person, or can be a system-wide policy, or a combination of such policies. For example, a user may set a policy that states that only computational devices that are associated with a given Internet Protocol (IP) range when requesting a vault from the cloud

storage may be approved. This may, for example, be an IP address from which the first computational device has previously been observed. In addition, the employer of the user may have a policy stating that only devices that are on the employer's approved list of devices may be used, where in various embodiments this approved list includes types or brands of devices, Media Access Control (MAC) address ranges, etc. Furthermore, in some embodiments, the system has a policy that states the minimum security level for allowing transfer of vaults, where in some embodiments, this policy is updated over time to account for new knowledge relating to security incidents. In some embodiments, a computational device is only enabled or allowed to access the contents of a vault it receives (e.g., from a cloud server) if it satisfies all of these policies associated with the vault. That is, the policies control the access and synchronization of data, such as the data stored in the vaults.

[0074] As another example, a first computational device with the capability to access the contents of a vault communicates a key to an approved second computational device after having performed a pairing with the second computational device. In various embodiments, the pairing comprises a verification of information describing the security level of the second computational device; the establishment of a secure channel; a distance-bounding process; a verification of user approval, or other security processes. An example of a verification of information describing a security level is the receipt of packets from the second computational device, the packets having headers, and the contents of the packets having a certificate related to a public key and a digital signature using a signing key associated with the public key in the certificate, the digital signature being associated with a message or a time stamp, where in some embodiments, the message is one or more packets or their contents, where these packets were received by the second computational device from the first computational device, and where in some embodiments, the contents include nonces, time indicators, and information related to the vault. In some embodiments, the time stamp is a value received from a third party, such as a trusted time keeper. In other embodiments, it is also the system clock of one of the two devices involved in the pairing, or a combination of such values, where in some embodiments the time values are exchanged in other packets exchanged between the first and the second computational devices. The certificate may be issued by a trusted third party such as a device manufacturer, an employer, or another party trusted by the user of the first computational device or the second computational device. Another example pairing method is the pairing method used to pair two

Bluetooth enabled devices, such as distance-bounding protocols. In some embodiments, verification of a user approval involves the display of a code on one of the computational devices, and the entry by a user of this code into the other computational device involved in the pairing. When one or both of the computational devices do not have a keyboard or a screen, an external keyboard and an external screen may be used (e.g., by the computational device being connected to a trusted device that has a keyboard and/or a screen). Two computational devices may also be paired using a line-of-sight approach. One example of such an approach is one in which one of the computational devices displays a code such as a QR code or barcode, etc., encoding a pairing message (i.e., data in place of one or more packets as described above), and the other computational device is used to photograph the QR code or barcode. Another example uses a device-to-device communication method such as infrared (IR), or short range radio signals such as Bluetooth. Alternative example pairing approaches include moving the two computational devices in unison, e.g., putting them on top of each other and shaking them. The coordinated movement may be detected using accelerometers, for example, where each device generates a value based on the detected time-series of acceleration measurements and uses the value to determine that the devices are moved together. This can be performed, for example, using a socialist-millionaires algorithm, where a comparison is performed to determine whether two values are identical without disclosing any other information about the values.

[0075] In one embodiment, after pairing has completed, or as part of the pairing process, key establishment takes place. In various embodiments, the key establishment uses key transport such as an RSA-based approach, or key exchange, such as a Diffie-Hellman based approach. In some embodiments, the key exchange is also performed as part of the socialist millionaires' process, where a tentative key and a pairing value held by one of the two computational devices is compared to the tentative key and pairing value held by the other of the two computational devices, the associated combinations of values being compared by the two entities. If the comparison completes with a match being determined, the tentative key is used to establish a secure channel. In some embodiments, the key establishment is also, whether in part or in full, performed by a user entering a code from one of the devices into the other device.

[0076] In some embodiments, a vault is associated with one or more policies, which tie what actions are allowed to be performed using the data in the vault, where in various

embodiments, such data includes credentials such as cryptographic keys, passwords, cookies, etc. For example, one policy may state that the vault may be stored on a shared device, but only for purposes of backup, and that it may not be used for purposes of authentication from that device. Therefore, to use the vault, a user would have to utilize the backup of such a vault to initialize a new computational device and transfer the vault to this device, after which its content may be used for purposes of authentication. Another example policy may state that the vault may be used for purposes of authentication on any computational device with a security level that exceeds a policy-mandated minimum. Thus, in this example, the security level may be expressed as a numeric value and the policy-mandated minimum as a threshold to compare the numeric value to. In some embodiments, the security level is determined by the hardware of the computational device (e.g., where a secure processor is utilized for accessing the vault). As another example, it is determined based on software (e.g., that the computational device is configured to auto-update software and download anti-virus definitions automatically). As another example, it is based on an action, such as having just been screened using a software-based attestation technique.

[0077] In one embodiment, a user needs to register on a computational device before a vault is transferred to the computational device. For example, as a user starts a new computational device, they are required to register. Similarly, a user wishing to use a friend's or colleague's computational device to store their vault would register on that computational device. In some embodiments, registration includes creating a record, at least part of which is either encrypted or stored in a secure storage. On example of secure storage is a storage that is only accessible using a restricted API, which is only available to selected processes. Another example of secure storage is a storage that is at least in part encrypted and/or authenticated. Yet another example of secure storage is a storage that is only accessible by one or more dedicated processors, such as a processor that evaluates biometric data against stored templates. In some embodiments, registration also includes data usable to authenticate one or more users associated with the registration. In some embodiments, the owner or user of the computational device on which the registration record is stored authenticates to the device and then indicates that they want to add a second user on the device. This second user would then be prompted to enroll, and the computational device stores the associated profile. This is therefore distinct from the owner of the device adding another fingerprint or other biometric verification technique to an existing profile of theirs, as the second user is associated with a new and different profile, but a new

fingerprint or other biometric verification technique of an already existing profile may be added to the same profile. In some embodiments, two different profiles have different policies associated with them, where example policies address the keys that would be associated with a user after a successful authentication to the computational device. In some embodiments, the matching of a profile is determined at least in part by the verification of authentication data such as at least one of a password, a PIN (personal identification number), biometric data, knowledge-based authentication, second factor authentication data, or other authentication data. The registration may have already been performed in the past, prior to the initiation of the vault transfer. For example, a user may already have access to the device to which a vault is to be transferred. In some embodiments, a profile is matched if an authentication attempt that includes one or more such authentication methods succeeds. Some profiles may require multiple associated users to successfully authenticate for the profile to be matched (e.g., at least three out of five). In some embodiments, based on what profile is matched, one or more records are selected. These records are associated with vaults. This selection of records and vaults in turn decides what privileges and access rights the user has when accessing services and data. These privileges and access rights may depend on policies associated with the record, the type of authentication method was used, and a score associated with the authentication. In some embodiments, the profile that is associated with a user is tied to one or more vaults, where such vaults may be associated with different policies (e.g., in terms of whether the vaults can be used for authentication on the computational device or only be used as a backup). In some embodiments, the policies also state what actions are to be taken by the system if there is a failure, such as a failure to authenticate. One example of such a policy requires that a vault is erased after a set number of failed attempts, such as ten attempts, or that a vault that initially was allowed to be used for authentication according to a policy associated with it is modified to only be used for backup purposes after a risk indication is observed, such as more than a threshold number of failed attempts within a selected time period, such as at least ten attempts within one day.

[0078] Figure 9 is a flow diagram illustrating an embodiment of a backup process. In this example, process 900 includes an example series of events associated with a backup process. The process begins at 901, when a user accesses a computational device. This may be the user's computational device, or it may belong to another user, in which case the user registering in step

901 is registering, for example, as a second user on the computational device. In this example, the registration process involves one or more prompts instructing the user what actions to take, where example actions include the creation of a biometric template (e.g., related to one or more of fingerprint features, voice biometric features, facial recognition features, or iris detection features). The template is part of the user profile created for the user. The profile also includes policies related to access to resources, policies related to vaults, as well as one or more vaults, which may be generated locally or obtained from an external source such as another computational device or a cloud storage entity. At 902, pairing is initiated between the computational device and an external resource that stores a vault to be synchronized (e.g., transferred to the computational device on which the user registered in step 901). Examples of external resources include another computational device, a cloud storage resource, etc. As part of the pairing between the computational device and the external resource storing the vault, the computational device sends information relating to its security level, which in various embodiments includes a certificate or another type of assurance from a party trusted by the external resource. At 903, the external resource determines that the requested vault is allowed to be transmitted to the computational device. If it is, pairing is completed. In some embodiments, the pairing requires the user to perform one or more actions, such as authenticating to one or more of the computational devices and the external resource. At 904, key exchange is performed, and a secure channel is established. At 905, the vault is transferred, for example over a secure channel, from the external resource to the computational device, and associated with the profile created by the user. At 906, the decryption key for the vault is transferred from the external resource to the computational device (e.g., over the secure channel or by the user obtaining and copying a code into the computational device). With the decryption key, the vault can be opened. In some embodiments, the vault is obtained without full security verification, but the decryption key can only be received after pairing, policy verification, and key exchange are performed. At 907, the vault is utilized by the user for authentication to a resource, or to create a new backup on yet another computational device, using a similar process. In some embodiments, the steps described in Figure 9 are performed in another order (e.g., performing policy verification after the key exchange is performed). Also, in some embodiments, some of the steps, such as pairing, are not performed, or some of its functionality is performed as part of another step, such as the key exchange step.

[0079] One example of synchronization is to copy new data from a first computational device to a second computational device, where the first and second computational devices have been associated with each other. If one or both of the computational devices include multiple profiles, then the synchronization is performed relative to the associated profiles. For example, if Alice has a profile on computational device A, and both Alice and Bob have profiles stored on computational device B, then an update of Alice's profile on computational device A causes data to be synchronized to the associated profile associated with Alice on computational device B, but not to the profile associated with Bob on computational device B. The two profiles may be stored in the same storage unit, or in two different secure storage units. Each profile may correspond to one or more records, which may be stored in different storage units. In some embodiments, at least one portion is stored in a secure storage. In one embodiment and for some devices, all storage may be considered secure; this assessment can be based on what types of processes are allowed to execute on the device. For example, if only trusted processes are allowed to run on the device, all storage may be considered trusted, based on a security evaluation being performed to confirm that only trusted processes are present. In some embodiments, this security evaluation involves performing remote attestation. Once two devices have established a secure channel, the secure channel can be reused for such synchronization, whether the encrypted synchronization data is sent directly from device A to device B (e.g., using a direct wireless connection) or whether it uses one or more intermediaries, such as a communication network involving a cloud storage entity as one party to the communication, or a communication network such as the telephony network or the Internet. One example approach, for example, is for one computational device to advertise the existence of synchronization data to one or more other computational devices, using a notification system that may involve an untrusted third party that simply is in charge of conveying notifications; a device receiving such a notification can respond to it, whether to request the synchronization to take place or not, and then, if a synchronization was requested, to receive the synchronization data over a secure channel. Here, the secure channel provides encryption of the contents, as well as a conditional authentication of the contents. As one example, the encryption is performed using a first key and an algorithm such as AES, and the authentication performed using a second key and an algorithm such as SHA-MAC, which is an example of a keyed hash function. The first and the second key are derived from a shared key that has previously been established between the devices. Alternatively, the devices have stored

each other's public key and perform key transport for a master key from which the two keys used for encryption and authentication of the synchronization data is performed. Example contents on the synchronization data include, but are not limited to, new policies, new credentials such as keys used to interact with service providers, new keys to be distributed to address revocation of previously delivered keys, new biometric data, new user information associated with profiles, and more.

[0080] Another example of performing synchronization involves the transmission of a certificate signed by one of the computational devices involved in the synchronization data to be transmitted, where, in some embodiments, the certificate associates a capability or right with a public key associated with a user profile, or with a user profile associated with a specified computational device on which the user profile is stored. In some embodiments, a certificate also describes the security context of the receiving device, or requirements relating to this. In some embodiments, certificates are exchanged in one or both directions of the exchange corresponding to the synchronization, where the certificate from the originator of the vault is associated with stated requirements on the receiving device while the certificate transmitted by the receiving device is associated with the security context of the receiving device. The receiving computational device associates a received certificate and associated policies with the indicated profile after verifying that they are valid (e.g., by verifying the digital signature of the certificate). To later authenticate on behalf of the user, the receiving computational device sends a digital signature associated with the certified public key, and where the digital signature is generated on an input message that relates to a description of the requested action, along with the received certificate. This enables the recipient of the associated request, which for example is a service provider, to verify the validity of the request relative to the signer, where in some embodiments, the signer is a computational device or a component thereof, and relative to the computational device that originated the synchronization data including the certificate. It provides additional granularity relative to a system in which the same key is used on multiple devices, which in turn enables device-specific revocation, should a device be suspected of having been compromised. An alternative to this approach is the automated generation of a new key by a computational device whose capabilities are not being revoked, where this new key is signed using the old key, thereby invalidating the old key, no matter what device uses it, in favor of the new key. In some embodiments, this also requires the synchronization of the new key to each

computational device whose capabilities are not being revoked relative to the now-replaced key. Here, signing using a key is an action performed using the secret key of a secret key - public key pair that is newly created, and that the data that is signed includes the public key to be revoked, where revoking this means that the associated secret key of the revoked public key no longer can be used to sign messages. Other techniques of synchronizing authentication data, whether to add or replace policies, keys and other data, or to perform revocation, may be used instead, as appropriate.

[0081] In some embodiments. secure storage can only be accessed using a restricted interface. One example of such a restricted interface is a dedicated physical connection from a processor permitted to access the secure storage. For example, this may be a bus; alternatively, the secure storage may be integrated with the processor allowed to access it (e.g., the storage includes non-volatile registers of the processor, or an alternative type of memory that can be accessed from the permitted processor). The secure storage and the processor permitted to access it may also be integrated on a SoC (System on a Chip). Alternatively, the restricted interface may be an API (Application Programming Interface) that is only accessible from a secure mode of operation of a processor. In one embodiment, access to the API is only granted from selected processes or applications; in another embodiment, the API is only accessible using a secure operating mode of the processor.

[0082] The processing device, in some embodiments, includes a hardware-based cryptographic accelerator, such as a special-purpose processor with hardware support for cryptographic operations. Alternatively, a processor of the processing device may have micro-instructions dedicated to cryptographic operations, such as computing cryptographic hash functions, computing or verifying digital signatures, encrypting or decrypting data, or computing other one-way functions efficiently. An example cryptographic hash function is SHA-256. Example algorithms for encryption and decryption are AES, RSA and ElGamal. Example digital signature algorithms are RSA and DSA, which also include or use the computation of a cryptographic hash function. Digital signatures can also be generated using Merkle signatures or Lamport signatures, both of which are based on a one-way function. SHA-256 is a believed one-way function. In some embodiments, a processing device has both hardware support for cryptographic operations and dedicated micro-instructions for cryptographic operations.

[0083] In some embodiments, a policy associated with a vault determines whether a vault may be backed up. In some embodiments, the policy depends on externally available information, such as the contents of a registry maintained by a trusted third party, the contents of the registry indicating how many backups have been made of the vault; how many of these backups are known to still exist; and whether there is a need to revoke the rights of any computational devices holding backups of the vault, resulting in the vault being erased from such computational devices. In some embodiments, this policy is also used to determine whether contents of a vault need to be revoked (e.g., by placing a public key associated with the vault on a revocation list); whether the contents of a vault need to be updated (e.g., by replacing one key with another). Policies can also be associated with devices, or with all vaults on a device. Such a policy may state that vaults can only be backed up to computational devices of the same brand, or to computational devices that satisfy software requirements associated with the policy, such as having anti-virus software or using an operating system that is the most recent version or the version before that, but not older. Policies may be associated with individual vaults, or with selected contents of a vault, such as a key that is used for a purpose identified in the policy. In some embodiments, authentication information such as biometric data is not included in the data that is synchronized during a backup, whereas in other embodiments biometric data is included unless a policy associated with the vault prohibits it.

[0084] In one embodiment, as vaults are backed up, they are not copied verbatim to the backup device. Instead, some of the contents are modified as a backup is performed, whether of the copy of the vault that is transmitted to the other device or to the copy of the vault that is kept. For example, the system may update policies associated with a vault (e.g., to indicate whether a vault contains a master key or a derived key), where the derived key may be associated with lesser capabilities. As another example, the original copy of a vault includes a first secret key and associated first public key, but the derived copy of the vault includes a second secret key and associated second public key, along with a digital signature on the second public key using the first secret key, where this digital signature is verified using the first public key. Such an approach simplifies revocation, as selected keys can be revoked. In addition, this allows revocation of any key that was digitally signed using an already revoked key, which may be performed, for example, if there is a breach. In some embodiments, a backup is split into two parts, each part which is backed up to a separate device, and where both parts are required to be

synchronized to one and the same device, which can be yet another device, in order for the backup data to be accessible. In some embodiments, a backup is split up into three or more parts, and in a manner that requires a quorum of backup components to be combined for the data to be reconstituted. In some embodiments, public key secret sharing techniques are used to facilitate such functionality. Techniques based on symmetric key technology may also be used.

[0085] Figure 10 is a flow diagram illustrating an embodiment of a process of a user registering as a second user on a computational device. In some embodiments, process 1000 is executed by a computational device. The process begins at 1001, when the registration process is initiated, for example, by the main user of the computational device making a request to add a new user as a second user. At 1002, a new profile is created for the second user. As one example, the profile has at least one database record, to which one or more profiles may be added, whether by the new user or during the synchronization of one or more vaults, such as described in the example of Figure 9, where policies may be associated with the one or more vaults. Additional policies may be obtained from third parties, such as an employer. A user may indicate the source of such policies during the registration at 1001, or the source may be indicated by vault data transferred to the device, such as at step 905 of Figure 9. Alternatively, in some embodiments, the source is communicated along with policies, which may be received, for example, as part of the pairing process 902 described in conjunction with Figure 9. At 1003, the computational device receives authentication information, such as cryptographic keys, passwords or other credentials. These are added to the profile as part of one or more vaults associated with the profile. At least portions of the profile are stored securely at 1004; examples of such secure storing include storing the profile in a secure storage such as a storage that can only be accessed by a dedicated processor; and encrypted and authenticated and stored in an insecure storage, while storing the keys to decrypt and verify such data in a secure storage that can only be accessed by the dedicated processor. Another example of such secure storage includes storing the profile in a storage that can only be accessed using a restricted API. In some embodiments, this restricted API is only accessible by some processes or from some processing environments. In yet another example, the profile is encrypted and authenticated using one or more keys that are only accessible using a restricted API from a whitelisted process or from a selected processing environment; and where the encrypted and authenticated profile can be stored in another type of storage, including a storage that is not secure. Multiple users may be

added as second users on a device. In some embodiments, for each one of these multiple users, a separate profile is generated and stored. In some instances, multiple users may share access to a resource. In these instances, their authentication information may be stored in one and the same profile (i.e., the same profile for all the multiple users with access to the resource); they may also be stored in independent profiles, where each profile indicates the resource to which an associated user has access. The access information may include multiple resources. This information may be stored in the profile or in one or more associated records. The access information, in one embodiment, is stored securely (e.g., on a storage unit that can only be accessed by a dedicated processor, only be accessed using a restricted API, or only accessed from a computational environment that has been determined to be safe).

[0086] Figure 11 is a flow diagram illustrating an embodiment of a process of an authentication attempt on a computational device. In some embodiments, process 1100 is executed by a computational device. The process begins at 1101, when the computational device receives a user input, such as a fingerprint, iris biometric information, face biometric information, or another input with the capability to authenticate the user, including other biometric information and/or a password, PIN or knowledge-based authentication string. Such user input is referred to herein as authentication input. At 1102, the computational device accesses one or more stored profiles to determine whether any one of these matches the authentication input. If a profile is securely stored in an insecure storage (e.g., authenticated and encrypted, making the insecure storage a secure storage with respect to the encrypted and authenticated element), then it is loaded into secure storage, decrypted, and verified with respect to its authenticity. If a profile is already stored in secure storage, such as a storage only accessible from a dedicated processor or only accessible using a restricted API, then this may not be necessary, but is still performed in some embodiments as additional assurance. For example, in some embodiments, this is required for a computational device to be certified to high security levels. A match is performed by comparing the one or more templates associated with the profile, and determining whether the match is sufficiently good (e.g., by determining that a matching score exceeds a threshold value, such as a value 0.82 – this is but one example of a threshold value, and other threshold values maybe used). Another biometric template may have a higher threshold value associated with it (e.g., a value 0.92). In this example, this corresponds to a better quality match. In some embodiments, policies associated with vaults specify the

threshold at which a match needs to be performed for an action to be permitted, where different types of actions may be associated with different thresholds. As a match is found, the associated profile is accessed, as shown at 1103. In this example, when the profile is accessed, the computational device extracts or loads the associated vault, or portions thereof. In some cases, the vault may already have been loaded, as part of the loading of the profile, or it may be loaded in response to the match being made. In some embodiments, as a vault is loaded, it is decrypted and, in some embodiments, its authentication value verified. An example authentication value is a message authentication code generated at the time the vault was generated or stored on the computational device. Another example of an authentication value is a digital signature. As one example, the decryption key is the same decryption key as described in 906, or it is a new key that is generated after the decryption key is received in 906 and the vault is decrypted using this key. If a new key is used, in some embodiments, this is performed using a high-quality random generator, such as a physical randomness generator or a cryptographically secure pseudo-random generator. In some embodiments, sensors on the computational device are used to generate true random values, whether for use as a physical randomness generator or to seed a pseudo-random generator. Examples of such sensors include biometric readers, which collect a large amount of high-entropy data. After the matched profile is accessed at1103, and at least one vault associated with the profile is loaded and accessed, an action is initiated at 1104. An example action is to use a cryptographic key stored in the accessed vault to compute a cryptographic value, such as a digital signature or other authentication value, and send the cryptographic value to an external resource. Alternatively, the action at 1104 is to access an internal resource relative to the computational device, where such an internal data may be an application, data accessible from an application, or similar. In this example case, the key extracted from the vault may be used to decrypt information, such as the data to be accessed, where the encrypted data may be stored on insecure storage. In some embodiments, such data is also authenticated, for example, using a message authentication code (MAC), using a key also stored in the vault. Thus, vaults can store many keys, where each such key may be specific to a particulate usage, and associated with a tag or other descriptor that identifies what it can be used for. This may also be controlled by one or more policies, as described above.

[0087] Figure 12 illustrates an embodiment of a computational device. In this example, computational device 1201 includes a user input element 1202 such as a dedicated biometric

sensor, a touchscreen, a camera or another input element capable to receive data usable to authenticate a user. As shown in this example, computational device 1201 further includes one or more secure processors 1203, as well as optional one or more application processors 1204. The computational device 1201 further includes a user-facing output element 1204, such as a screen, an LED, a speaker, a haptic element, etc. While a user-facing output element is shown in this example of a computational device, the computational device need not have a user-facing output element, and the techniques described herein may be variously adapted to accommodate computational devices without user-facing output elements. Examples of communication element 1206 include a Bluetooth-enabled radio, a WiFi-enabled radio, a USB port, a speaker, etc. In this example, secure storage 1207 is accessible only from secure processor 1203, or requires the use of an application programming interface (API) only accessible to secure processor 1203. Thus, in this example, application processor 1204 cannot access secure storage 1207. In this example, insecure storage 1208 can be accessed both by secure processor 1203 and application processor 1204. Computational device 1201 further includes a power source 1209, such as a battery. In some embodiments, power source 1209 is an interface from which power can be obtained from an external device. One example of such an interface used to power a computational device is a USB connector, which receives power to a computational device from a computer it is connected to, or another power source.

[0088] Figure 13 illustrates an embodiment of a computational device. In this example, computational device 1301 includes a user input element 1302 such as a dedicated biometric sensor, a touchscreen, a camera or another input element capable to receive data usable to authenticate a user. In this example, computational device 1301 further includes one or more processors 1303 that can be run in secure mode 1304a, or non-secure mode 1304b. Computational device 1301 further includes (but need not include) a user-facing output element 1304, such as a screen, an LED, a speaker, a haptic element, etc. In various embodiments, communication element 1306 is a Bluetooth-enabled radio, a WiFi-enabled radio, a USB port, a speaker, etc. In this example, secure storage 1307 is accessible only from processor 1303 in secure mode 1304a, using a restricted interface. Thus, in this example, processor 1303 in non-secure mode 1304b cannot access secure storage 1307. In this example, insecure storage 1308 is accessible by processor 1303 both in secure mode 1304a and non-secure mode 1304b. As shown in this example, the computational device 1301 further includes a power source 1309, such as a

APPL-1002
APPLE INC. / Page 411 of 419

battery. In some embodiments, power source 1309 is an interface from which power can be obtained from an external device. One example of such an interface used to power a computational device is a USB connector, which receives power to a computational device from a computer it is connected to, or another power source.

[0089] Figure 14 is a flow diagram illustrating an embodiment of a backup process between two computational devices. In some embodiments, process 1400 illustrates an aspect of the backup process between two computational devices. In some embodiments, process 1400 is executed by one or more computational devices. The process begins at 1401, when a pairing request is transmitted between a first computational device and a second computational device. In this example, suppose a computational device A has a vault requested to be backed up to a computational device B. At 1402, device A receives compliance data related to computational device B. In some embodiments, the compliance data includes a description of the system of computational device B, which includes, for example a serial number, a hardware version specification, data describing the software configuration and its versions, a description detailing hardware attachments, software plugins, etc. In some embodiments, at least part of the compliance data is digitally signed by a trusted third party, such as a manufacturer, anti-virus vendor, an employer of the user, a financial institution, insurance company, etc. In some embodiments, aspects or portions of the compliance data are digitally signed by a first trusted party while other aspects of the compliance data are signed by a second trusted party. In some embodiments, the compliance data also includes digital certificates and other data usable to assess risk, such as usage logs associated with computational device B. In some embodiments, the compliance data is transmitted over a secure channel. In some embodiments, at least some of the compliance data is sent from a third party repository or service provider while at least some of the compliance data is sent from computational device B. At 1403, computational device A or a party associated with it evaluates the compliance data and determines whether computational device B is in compliance (e.g., matches the requirements specified by one or more policies associated with at least one of the requested vault and computational device A). For example, computational device B is determined to be compliant if it is associated with a whitelisted hardware configuration and satisfies a minimum requirement for software configuration, such as having a sufficiently recent operating system installed. At 1404, new policies addressing what the vault can be used for are generated. For example, if the compliance verification in step 1403

determines that computational device B is in partial compliance but not in full compliance, a policy restricting the use of the vault may be generated and associated with the copy of the vault to be transmitted to computational device B. At 1405, the two computational devices engage in a synchronization of data in which at least part of the requested vault information is transmitted to computational device B. In some embodiments, if there are future changes to the vault information, a notification is transmitted from the computational device where the modification was performed or observed to other entities, such as other computational devices and cloud storage repositories and service providers assisting in synchronization processes. An analogous process can be used if the requested vault is requested from computational device B from a cloud storage unit.

[0090] Figure 15 is a flow diagram illustrating an embodiment of a pairing process. In some embodiments, process 1500 illustrates an aspect of an example pairing process. In some embodiments, process 1500 is executed by a computational device. The process begins at 1501, when a first computational device receives a biometric input, such as a fingerprint, face biometric data, voice data, typing behavior, etc. This may be received from a built-in sensor, such as a fingerprint sensor, or it may be received from a device the first computational device is in communication with, such as a connected keyboard. At 1502, the first computational device receives a pairing signal, such as data related to a distance-bounding protocol, a code input by a user, accelerometer data indicating a time series of movement data, etc. At 1503, a code is generated. In some embodiments, the code is generated from the biometric data. The code may also be generated from the pairing signal data. In some embodiments, the code is generated in a manner that is robust to minor errors. As one example, the code is generated at least in part from a key generated from the biometric data. For example, an approach that is robust to minor modifications of the input data may be used, where robust entropy is extracted from biometric data of various types. Alternatively, key data is extracted from biometric data. In some embodiments, the code is set as the combination of a key derived using such an approach, and a function of at least some of the pairing signal. If a fuzzy pairing signal such as accelerometer data is used, a similar process of extracting a robust key from the pairing signal may be used. If non-fuzzy pairing data is used, in some embodiments such data is appended to the key extracted from fuzzy data, such as biometric data and accelerometer data. The result is, for example, a code. In some embodiments, another code is computed by a second computational device in an

analogous manner. At 1504, the code computed by the first computational device is compared to the code computed by the second computational device. In some embodiments, this is done by communication of the code from one of these devices to the other, or by a user entering the code from one device into the other device, or a user input unit associated with the other device. In some embodiments, it is performed using a socialist millionaires' protocol. In response to the comparison, the first computational device makes a pairing determination at 1505, where this determination reflects whether the codes compared matched or not. If the codes match, the pairing is determined to have succeeded, otherwise not.

[0091] Although the foregoing embodiments have been described in some detail for purposes of clarity of understanding, the invention is not limited to the details provided. There are many alternative ways of implementing the invention. The disclosed embodiments are illustrative and not restrictive.

[0092] WHAT IS CLAIMED IS:

CLAIMS

1. A system, comprising:

one or more processors configured to:

receive, at a first device, a request to access a resource external to the first device, wherein the resource external to the first device is associated with a user;

access at least one record stored on the first device, the at least one record including authentication information associated with the user and credential information associated with the external resource to which the user has requested access, wherein the credential information comprises a cryptographic key;

receive authentication input from the user;

determine that the authentication input from the user matches the authentication information associated with the user included in the at least one record stored on the first device;

retrieve at least a portion of the credential information from the at least one record stored on the first device;

facilitate access of the user to the external resource at least in part by transmitting, on behalf of the user, from the first device, output based at least in part on the at least portion of the credential information retrieved from the at least one record, wherein the user of the first device is granted access to the external resource based at least in part on the output transmitted from the first device on behalf of the user; and

initiate a backup, to a second device, of at least a portion of the at least one record; and

a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.

2. The system of claim 1, wherein the second device is used to authenticate the user to one or more external resources.

3. The system of claim 1, wherein the backup is completed after the first device has performed a verification that the second device conforms to a policy associated with the at least one record stored on the first device.

4. The system of claim 1, wherein the backup is completed after a secure channel is established by at least one of the first device and the second device.

5. The system of claim 1, wherein the first device and the second device are configured to complete a pairing process.

6. The system of claim 5, wherein the pairing process comprises a comparison of data generated from one or more authentication inputs.

7. The system of claim 1, wherein subsequent to completion of the backup, the second device comprises a first profile associated with the user of the first device, and a second profile associated with a second user different from the user of the first device.

8. The system of claim 1, wherein the one or more processors are further configured to:

determine that the authentication input from the user does not match authentication information of a first profile; and

subsequent to determining that the authentication input from the user does not match the authentication information of the first profile, determine that the authentication input from the user matches authentication information of a second profile, wherein the first profile is associated with a different user than the second profile.

9. The system of claim 1, wherein the at least one record stored on the first device is stored in a secure storage, and where the one or more processors are configured to access the record stored on the secure storage using a restricted interface.

10. The system of claim 9, wherein the restricted interface comprises a dedicated physical connection.

11. The system of claim 9, wherein the restricted interface comprises an application programming interface.

12. The system of claim 1, wherein the backup causes a certificate to be transmitted to the second device.

13. The system of claim 12, wherein the certificate is generated at least in part by the first device.

14. The system of claim 1, wherein the authentication input from the user is received using a biometric user input element.

15. The system of claim 1, wherein the backup comprises copying a modified version of a vault to the second device.

16. The system of claim 1, wherein the backup is performed in response to a determination that the first device is of a same brand as the second device.

17. A method, comprising:

receiving, at a first device, a request to access a resource external to the first device, wherein the resource external to the first device is associated with a user;

accessing at least one record stored on the first device, the at least one record including authentication information associated with the user and credential information associated with the external resource to which the user has requested access, wherein the credential information comprises a cryptographic key;

receiving authentication input from the user;

determining that the authentication input from the user matches the authentication information associated with the user included in the at least one record stored on the first device;

retrieving at least a portion of the credential information from the at least one record stored on the first device;

facilitating access of the user to the external resource at least in part by transmitting, on behalf of the user, from the first device, output based at least in part on the at least portion of the credential information retrieved from the at least one record, wherein the user of the first device is granted access to the external resource based at least in part on the output transmitted from the first device on behalf of the user; and

initiating a backup, to a second device, of at least a portion of the at least one record.

18. A computer program product embodied in a non-transitory computer readable storage medium and comprising computing instructions for:

receiving, at a first device, a request to access a resource external to the first device, wherein the resource external to the first device is associated with a user;

accessing at least one record stored on the first device, the at least one record including authentication information associated with the user and credential information associated with the external resource to which the user has requested access, wherein the credential information comprises a cryptographic key;

receiving authentication input from the user;

determining that the authentication input from the user matches the authentication information associated with the user included in the at least one record stored on the first device;

retrieving at least a portion of the credential information from the at least one record stored on the first device;

facilitating access of the user to the external resource at least in part by transmitting, on behalf of the user, from the first device, output based at least in part on the at least portion of the credential information retrieved from the at least one record, wherein the user of the first device is granted access to the external resource based at least in part on the output transmitted from the first device on behalf of the user; and

initiating a backup, to a second device, of at least a portion of the at least one record.

ABSTRACT OF THE DISCLOSURE

Authentication translation is disclosed. A request to access a resource is received at an authentication translator, as is an authentication input. The authentication input corresponds to at least one stored record. The stored record is associated at least with the resource. In response to the receiving, a previously stored credential associated with the resource is accessed. The credential is provided to the resource.

APPL-1002
APPLE INC. / Page 419 of 419