

AO 120 (Rev. 08/10)

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

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

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

DOCKET NO. 1:23-cv-607	DATE FILED 5/30/2023	U.S. DISTRICT COURT for the Western District of Texas Austin Division
PLAINTIFF PACID TECHNOLOGIES, LLC		DEFENDANT BANK OF AMERICA CORPORATION and BANK OF AMERICA, N.A.
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 9,577,993	2/21/2017	PACid Technologies, LLC
2 9,876,771	1/23/2018	PACid Technologies, LLC
3 10,044,689	8/7/2018	PACid Technologies, LLC
4 10,171,433	1/1/2019	PACid Technologies, LLC
5 10,484,344	11/19/2019	PACid Technologies, LLC

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

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

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

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
-------	-------------------	------

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

AO 120 (Rev. 08/10)

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

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

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

DOCKET NO. 1:23-cv-607	DATE FILED 5/30/2023	U.S. DISTRICT COURT for the Western District of Texas Austin Division
PLAINTIFF PACID TECHNOLOGIES, LLC		DEFENDANT BANK OF AMERICA CORPORATION and BANK OF AMERICA, N.A.
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 11,070,530	7/20/2021	PACid Technologies, LLC
2		
3		
4		
5		

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

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

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

DECISION/JUDGEMENT		
CLERK	(BY) DEPUTY CLERK	DATE

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

AO 120 (Rev. 08/10)

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

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

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

DOCKET NO. 1:23-cv-251	DATE FILED 3/7/2023	U.S. DISTRICT COURT for the Western District of Texas Austin Division
PLAINTIFF PACID TECHNOLOGIES, LLC		DEFENDANT BANK OF AMERICA CORPORATION and BANK OF AMERICA, N.A.
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 9,577,993	2/21/2017	PACid Technologies, LLC
2 9,876,771	1/23/2018	PACid Technologies, LLC
3 10,044,689	8/7/2018	PACid Technologies, LLC
4 10,171,433	1/1/2019	PACid Technologies, LLC
5 10,484,344	11/19/2019	PACid Technologies, LLC

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

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

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

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
-------	-------------------	------

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

AO 120 (Rev. 08/10)

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

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

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

DOCKET NO. 1:23-cv-251	DATE FILED 3/7/2023	U.S. DISTRICT COURT for the Western District of Texas Austin Division
PLAINTIFF PACID TECHNOLOGIES, LLC		DEFENDANT BANK OF AMERICA CORPORATION and BANK OF AMERICA, N.A.
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 11,070,530	7/20/2021	PACid Technologies, LLC
2		
3		
4		
5		

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

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

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

DECISION/JUDGEMENT		
See attached Order Approving Notice of Voluntary Dismissal entered 06/12/2023		
CLERK Philip J. Devlin	(BY) DEPUTY CLERK <i>Jay Cicha</i>	DATE 06/12/2023

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

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

PACID TECHNOLOGIES, LLC,	§	No. 1:23-cv-00251
	§	
<i>Plaintiff,</i>	§	
	§	
vs.	§	
	§	
BANK OF AMERICA CORPORATION and	§	
BANK OF AMERICA, N.A.,	§	
	§	
<i>Defendants.</i>	§	
	§	
	§	
	§	

ORDER APPROVING NOTICE OF VOLUNTARY DISMISSAL

Before the Court is a Notice of Voluntary Dismissal filed by counsel for Plaintiff PACid Technologies, LLC. (Dkt. # 16.) Finding that the notice was filed before Defendants served an answer or a motion for summary judgment, the Court finds that the notice complies with Federal Rule of Civil Procedure 41(a)(1)(A)(i). Accordingly, all claims in the instant suit against Defendants are hereby **DISMISSED WITHOUT PREJUDICE**. The Clerk is **INSTRUCTED TO CLOSE THE CASE**.

IT IS SO ORDERED.

DATED: Austin, Texas, June 12, 2023.



David Alan Ezra
Senior United States District Judge

AO 120 (Rev. 08/10)

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

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

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

DOCKET NO. 1:23-cv-607	DATE FILED 5/30/2023	U.S. DISTRICT COURT for the Western District of Texas Austin Division
PLAINTIFF PACID TECHNOLOGIES, LLC		DEFENDANT BANK OF AMERICA CORPORATION and BANK OF AMERICA, N.A.
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 9,577,993	2/21/2017	PACid Technologies, LLC
2 9,876,771	1/23/2018	PACid Technologies, LLC
3 10,044,689	8/7/2018	PACid Technologies, LLC
4 10,171,433	1/1/2019	PACid Technologies, LLC
5 10,484,344	11/19/2019	PACid Technologies, LLC

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

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

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

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
-------	-------------------	------

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

AO 120 (Rev. 08/10)

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

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

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

DOCKET NO. 1:23-cv-607	DATE FILED 5/30/2023	U.S. DISTRICT COURT for the Western District of Texas Austin Division
PLAINTIFF PACID TECHNOLOGIES, LLC		DEFENDANT BANK OF AMERICA CORPORATION and BANK OF AMERICA, N.A.
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 11,070,530	7/20/2021	PACid Technologies, LLC
2		
3		
4		
5		

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

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

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

DECISION/JUDGEMENT

CLERK Philip J. Devlin	(BY) DEPUTY CLERK <i>Christina Cordero</i>	DATE 05/31/2023
----------------------------------	---	--------------------

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

AO 120 (Rev. 08/10)

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

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

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

DOCKET NO. 2:18-cv-00133	DATE FILED 4/6/2018	U.S. DISTRICT COURT Eastern District of Texas - Marshall Division
PLAINTIFF PACID TECHNOLOGIES, LLC		DEPENDANT SAMSUNG ELECTRONICS CO., LTD. and SAMSUNG ELECTRONICS AMERICA, INC.
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 9,577,993	2/21/2017	PACid Technologies, LLC
2 9,876,771	1/23/2018	PACid Technologies, LLC
3		
4		
5		

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

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

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

DECISION/JUDGEMENT Defendants Samsung Electronics America, Inc. and Samsung Electronics Co., Ltd. are hereby dismissed with prejudice

CLERK <i>David A. O'Toole</i>	(BY) DEPUTY CLERK CH	DATE 11/21/18
----------------------------------	-------------------------	------------------

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



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	REQUEST ID
15/195,606	06/28/2016	PACID TECHNOLOGIES, LLC	5101-0005-C3	85432

Acknowledgement of Loss of Entitlement to Entity Status Discount

The entity status change request below filed through Private PAIR on 04/10/2019 has been accepted.

CERTIFICATIONS:

Change of Entity Status:

☒ Applicant changing to regular undiscounted fee status.

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

This portion must be completed by the signatory or signatories making the entity status change in accordance with 37 CFR 1.4(d)(4).

Signature:	/Tarek N. Fahmi/
Name:	Tarek N. Fahmi
Registration Number:	41402

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

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

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

DOCKET NO. 6:19cv154	DATE FILED 2/14/2019	U.S. DISTRICT COURT Western District of Texas - Waco Division
PLAINTIFF PACID TECHNOLOGIES, LLC		DEFENDANT GEMALTO, INC.,
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 ~~SEE ATTACHED~~		
2 9577993		
3 9876771		
4 10044689		
5 10171433		

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

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

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

DECISION/JUDGEMENT

CLERK Jeannette J. Clack	(BY) DEPUTY CLERK <i>L Diaz</i>	DATE 2/15/2019
-----------------------------	------------------------------------	-------------------

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

AO 120 (Rev. 08/10)

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

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

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

DOCKET NO. 2:18-cv-00133	DATE FILED 4/6/2018	U.S. DISTRICT COURT Eastern District of Texas - Marshall Division
PLAINTIFF PACID TECHNOLOGIES, LLC		DEPENDANT SAMSUNG ELECTRONICS CO., LTD. and SAMSUNG ELECTRONICS AMERICA, INC.
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 9,577,993	2/21/2017	PACid Technologies, LLC
2 9,876,771	1/23/2018	PACid Technologies, LLC
3		
4		
5		

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

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

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

DECISION/JUDGEMENT		
CLERK	(BY) DEPUTY CLERK	DATE

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

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 9,577,993 B2
APPLICATION NO. : 15/195606
DATED : February 21, 2017
INVENTOR(S) : Guy Fielder

Page 1 of 1

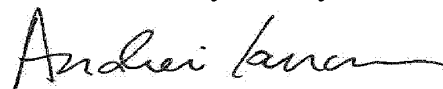
It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In the Claims

In Column 28, Line 31 (Claim 13, Line 11) replace "a" with --the--.

In Column 29, Line 14 (Claim 22, Line 10) replace "a" with --the--.

Signed and Sealed this
Fifteenth Day of May, 2018



Andrei Iancu
Director of the United States Patent and Trademark Office

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Inventor: Guy Fielder

Application No.: 15/195,606
Filed: June 28, 2016

Patent No.: 9,577,993
Issued: February 21, 2017

Examiner: Shaw, Brian F.
Art Unit: 2491

Docket No.: 5101-0005-C3

Confirmation No.: 8706

**PETITION TO REQUEST EXPEDITED HANDLING OF REQUEST FOR
CERTIFICATE OF CORRECTION**

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

Dear Sir:

Petitioner-Patent Owner hereby petitions for expedited handling of a Request for a Certificate of Correction pursuant to 37 C.F.R. § 1.323 to correct mistakes in the above-identified patent. Said Request is submitted concurrently herewith.

U.S Patent 9,577,993 is believed to be infringed and Patent Owner seeks to abate the infringement. Certificates of Correction are generally understood to have prospective application only. See, e.g., *Southwest Software, Inc. v. Harlequin Inc.*, 226 F.3d 1280, 1294 (Fed. Cir. 2000). Therefore, until the requested Certificate is issued, Patent Owner is disadvantaged insofar as seeking to abate the on-going infringement. Accordingly,

expedited handling of the Request is respectfully requested.

The required fee under 37 C.F.R. 1.17(f) is included herewith, however, should any additional fees be required, please deduct them from Deposit Account No. 50-5798.

Respectfully submitted,

Date: April 16, 2018

By: /Tarek N. Fahmi/
Tarek N. Fahmi
Reg. No. 41,402

Ascenda Law Group, PC
333 W. San Carlos, St., Suite 200
San Jose, CA 95110
866-877-4883

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Inventor: Guy Fielder

Application No.: 15/195,606

Filed: June 28, 2016

Patent No.: 9,577,993

Issued: February 21, 2017

Examiner: Shaw, Brian F.

Art Unit: 2491

Docket No.: 5101-0005-C3

Confirmation No.: 8706

REQUEST FOR CERTIFICATE OF CORRECTION

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

Dear Sir:

This is a Request for a Certificate of Correction pursuant to 37 C.F.R. § 1.323 to correct mistakes in the above-identified patent.

All of the errors shown in the accompanying Form PTO/SB/44 are of a clerical nature, a typographical error, and/or a minor character and occurred in good faith.

Correction of these mistakes does not involve any changes which would constitute new matter or require reexamination.

Claim 13 is corrected as follows:

13. A token for use in connection with secure communications, comprising:

a processor and a memory communicatively coupled to the processor the memory storing a security application for execution by the processor, said security application, when executed by said processor, causing said processor to perform steps, including:

generating, according to a unique user input, a secret, and storing said secret with an identifier and in a directory which the processor configures in the memory such that said secret is retrievable when [[a]] the unique user input is received by the token;

responsive to receiving the identifier associated with the secret, prompting, via a user interface, entry of the unique user input; and

upon receipt of the unique user input, verifying said unique user input, and using said secret to encode a first communication with a remote computer-based station.

Claim 22 is corrected as follows:

22. A mobile phone, comprising:

a processor and a memory communicatively coupled to the processor the memory storing a security application for execution by the processor, said security application, when executed by said processor, causing said processor to perform steps, including:

generating, according to a unique user input, a secret, and storing said secret with an identifier and in a directory which the processor configures in the memory such that said secret is retrievable when [[a]] the unique user input is received via a user interface of the mobile phone;

responsive to receiving the identifier associated with the secret, prompting, via the user interface of the mobile phone, entry of the unique user input; and

upon receipt of the unique user input, verifying said unique user input, and using said secret to encode a first communication with a remote computer-based station,

wherein the unique user input comprises user credentials, and said security application, when executed by said processor, further causes said processor to receive, via the user interface of the mobile phone, the user credentials prior to generating the secret.

The foregoing corrections do not introduce any new matter or require reexamination because the same subject matter as reflected in the above, corrected claims was already presented, examined, and issued in claim 1:

1. A method for authenticating a user, comprising:

generating, by an application running on a computing device and according to *a unique user input*, a secret, said secret stored at the computing device with an identifier and in a directory so as to be retrievable when *the unique user input* is applied to the computing device;

receiving at the computing device from a remote computer-based station a first communication, said first communication including the identifier associated with the secret;

responsive to said receiving, prompting a user for the user input via a user interface of the computing device and, upon verifying said unique user input to the computing device, transmitting from the computing device to the remote computer-based station a second communication encoded using the secret.

In claim 1, as originally presented and issued, the same *unique user input* is referenced in each instance in the claim. The corrections to claims 13 and 22 conform to this requirement. These errors are of a clerical nature, a typographical error, and/or a minor character and occurred in good faith. Hence, a certificate of correction is respectfully requested.

The required fee under 37 C.F.R. 1.20(a) is included herewith, however, should any additional fees be required, please deduct them from Deposit Account No. 50-5798.

Respectfully submitted,

Date: April 16, 2018

By: /Tarek N. Fahmi/
Tarek N. Fahmi
Reg. No. 41,402

Ascenda Law Group, PC
333 W. San Carlos, St., Suite 200
San Jose, CA 95110
866-877-4883

UNITED STATES PATENT AND TRADEMARK OFFICE CERTIFICATE OF CORRECTION

Page 1 of 1

PATENT NO. : 9,577,993

APPLICATION NO.: 15/195,606

ISSUE DATE : 02/21/2017

INVENTOR(S) : Guy Fielder

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In column 28, line 31 (claim 13, line 11) replace "a" with --the--.

In column 29, line 14 (claim 22, line 10) replace "a" with --the--.

MAILING ADDRESS OF SENDER (Please do not use Customer Number below):

Ascenda Law Group, PC
333 W San Carlos St., Suite 200
San Jose, CA 95110

This collection of information is required by 37 CFR 1.322, 1.323, and 1.324. 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 1.0 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: Attention Certificate of Corrections Branch, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Privacy Act Statement

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

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

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

Electronic Patent Application Fee Transmittal				
Application Number:		15195606		
Filing Date:		28-Jun-2016		
Title of Invention:		SYSTEM AND METHOD FOR AUTHENTICATING USERS		
First Named Inventor/Applicant Name:		Guy Fielder		
Filer:		Tarek N. Fahmi/Sarah Zizzo		
Attorney Docket Number:		5101-0005-C3		
Filed as Small Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
CERTIFICATE OF CORRECTION	2811	1	150	150

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				150

Electronic Acknowledgement Receipt	
EFS ID:	32354065
Application Number:	15195606
International Application Number:	
Confirmation Number:	8706
Title of Invention:	SYSTEM AND METHOD FOR AUTHENTICATING USERS
First Named Inventor/Applicant Name:	Guy Fielder
Customer Number:	27571
Filer:	Tarek N. Fahmi/Sarah Zizzo
Filer Authorized By:	Tarek N. Fahmi
Attorney Docket Number:	5101-0005-C3
Receipt Date:	16-APR-2018
Filing Date:	28-JUN-2016
Time Stamp:	19:15:38
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	\$150
RAM confirmation Number	041718INTEFSW19163500
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Petition for review by the Office of Petitions	2018-04-16_CoC_Petition.pdf	69569	no	2
			770574125e37be483fd7495aaba0e7a81c902a4		
Warnings:					
Information:					
2	Request for Certificate of Correction	2018-04-16_CoC_Transmittal_Letter.pdf	73576	no	4
			872aea43d606438527eb8547e37b3ec09c105495		
Warnings:					
Information:					
3	Request for Certificate of Correction	2018-04-16_Cert_of_Correct_form.pdf	168427	no	2
			20dc66028cb927259018d555260f8dd45cf8a876		
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	30056	no	2
			9aee2b365249727e4040695434973bea440a2b27		
Warnings:					
Information:					
Total Files Size (in bytes):			341628		

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.

Electronic Patent Application Fee Transmittal				
Application Number:		15195606		
Filing Date:		28-Jun-2016		
Title of Invention:		SYSTEM AND METHOD FOR AUTHENTICATING USERS		
First Named Inventor/Applicant Name:		Guy Fielder		
Filer:		Tarek N. Fahmi/Sarah Zizzo		
Attorney Docket Number:		5101-0005-C3		
Filed as Small Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
PETITION FEE - 37 CFR 1.17(F)(GROUP I)	2462	1	200	200
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				200

Electronic Acknowledgement Receipt	
EFS ID:	32354143
Application Number:	15195606
International Application Number:	
Confirmation Number:	8706
Title of Invention:	SYSTEM AND METHOD FOR AUTHENTICATING USERS
First Named Inventor/Applicant Name:	Guy Fielder
Customer Number:	27571
Filer:	Tarek N. Fahmi/Sarah Zizzo
Filer Authorized By:	Tarek N. Fahmi
Attorney Docket Number:	5101-0005-C3
Receipt Date:	16-APR-2018
Filing Date:	28-JUN-2016
Time Stamp:	19:24:26
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	\$200
RAM confirmation Number	041718INTEFSW19251900
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Fee Worksheet (SB06)	fee-info.pdf	30435	no	2
			cc46b755ef491d1c15754ba76921f5794cfb05eb		
Warnings:					
Information:					
Total Files Size (in bytes):			30435		
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/195,606	02/21/2017	9577993	5101-0005-C3	8706

27571 7590 02/01/2017
Ascenda Law Group, PC
333 W San Carlos St.
Suite 200
San Jose, CA 95110

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

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

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

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

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

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

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

PACID TECHNOLOGIES, LLC, Austin, TX;
Guy Fielder, Austin, TX;

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

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.

Substitute for form 1449/PTO		Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)		Application Number	
		Filing Date	
		First Named Inventor	Guy Fielder
		Art Unit	
		Examiner Name	
Sheet	3	of	9
Attorney Docket No: 5101-0005-C3			

		20050039030	02/17/2005	RODGERS; et al.	
		20050063352	03/24/2005	AMARA; et al.	
		20050076061	04/07/2005	COX	
		20060112418	05/25/2006	BANTZ; et al.	
		20060174349	08/03/2006	CRONCE; et al.	
		20060210082	09/21/2006	DEVADAS; et al.	
		20060271697	11/30/2006	KRUSE	
		20070130463	06/07/2007	LAW; et al.	
		20070150742	06/28/2007	CUKIER; et al.	
		20070255941	11/01/2007	ELLIS	
		20070258584	11/08/2007	BROWN; et al.	
		20080065880	~~08/13/2008~~	MARTIN; et al.	03/2008
		20080098464	04/24/2008	MIZRAH	
		20080244078	10/02/2008	VILJOEN; et al.	
		20080270791	10/30/2008	NYSTROM; et al.	
		20090094520	04/09/2009	KULAS	
		20100070778	03/18/2010	MURRAY; et al.	

Change(s) applied
to document
/M.H.E./
10/17/2016

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T 6
		Country Code ³⁻ Number ⁴ Kind Code ⁵ (if known)				
		EP 1304848 A2	04/23/2003	MICROSOFT CORP		
		EP 1478156 A2	11/17/2004	SAMSUNG ELECTRONICS CO., LTD.		
		EP 1906587 A2	04/02/2008	THOMSON LICENSING INC		

EXAMINER SIGNATURE

DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached. 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 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, 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 (1-800-786-9199) and select option 2.

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

Document Description: Issue Fee Payment (PTO-85B)

Issue Fee Transmittal Form

Application Number	Filing Date	First Named Inventor	Atty. Docket No.	Confirmation No.
15195606	28-Jun-2016	Guy Fielder	5101-0005-C3	8706

TITLE OF INVENTION :

SYSTEM AND METHOD FOR AUTHENTICATING USERS

Entity Status	Application Type	Art Unit	Class - Subclass	EXAMINER
Small	Utility under 35 USC 111(a)	2491	181000	BRIAN SHAW
Issue Fee Due	Publication Due	Total Fee(s) Due	Date Due	Prev. Paid Fee
\$480	\$0	\$480	06-Jan-2017	\$0

1.Change of Correspondence Address and/or Indication Of Fee Address (37 CFR 1.33 & 1.363)

Current Correspondence Address:	Current Indicated Fee Address :
27571 Ascenda Law Group, PC 333 W San Carlos St. Suite 200 San Jose CA 95110 UNITED STATES 408-799-0612 ~~patents@ascendlaw.com~~	
☐ Change of correspondence address requested, system generated AIA/122-EFS form attached	☐ Fee Address indication requested, system generated SB/47-EFS form attached

2.Entity Status**Change in Entity Status**

Applicant certifying micro entity status; system generated Micro Entity certification form attached. See 37 CFR 1.29.

Note: Absent a valid certification of micro entity status, issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment. If this box is checked, you will be prompted to choose a micro entity status on the gross income basis (37 CFR 1.29(a)) or the institution of higher education basis (37 CFR 1.29(d)), and make the applicable certification online.



Applicant asserting small entity status. See 37 CFR 1.27.

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



Applicant changing to regular undiscounted fee status.

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



Document Description: Issue Fee Payment (PTO-85B)

3.The Following Fee(s) Are Submitted:☒ Issue Fee☐ I authorize USPTO to apply my previously paid issue fee to the current fees due☐ Publication Fee☐ The Director is hereby authorized to apply my previously paid issue fee to the current fee due and to charge deficient fees to Deposit Account Number _____☐ Advance Order - # of copies _____

If **in addition to** the payment of the issue fee amount submitted with this form, there are any discrepancies in any amount(s) due, the Director is authorized to charge any deficiency, or credit any overpayment, to Deposit Account Number 505798.

☒ The **issue fee must be submitted** with this form. **If payment of the issue fee does not accompany this form, checking this box and providing a deposit account number will NOT be effective to satisfy full payment of the fee(s) due.**

4.Firm and/or Attorney Names To Be Printed**NOTE: If no name is listed, no name will be printed**

For printing on the patent front page, list to be displayed as entered

1. Ascenda Law Group, PC

2.

3.

5.Assignee Name(s) and Residence Data To Be Printed

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

Name	City	State	Country	Category
PACID TECHNOLOGIES, LLC	Austin	TEXAS	united states	other

6.Signature

I certify, in accordance with 37 CFR 1.4(d)(4) that I am an attorney or agent registered to practice before the Patent and Trademark Office who has filed and has been granted power of attorney in this application. I also certify that this Fee(s) Transmittal form is being transmitted to the USPTO via EFS-WEB on the date indicated below.

Signature	/Tarek N. Fahmi/	Date	01-06-2017
Name	Tarek N. Fahmi	Registration Number	41402

Electronic Patent Application Fee Transmittal				
Application Number:		15195606		
Filing Date:		28-Jun-2016		
Title of Invention:		SYSTEM AND METHOD FOR AUTHENTICATING USERS		
First Named Inventor/Applicant Name:		Guy Fielder		
Filer:		Tarek N. Fahmi/Sarah Zizzo		
Attorney Docket Number:		5101-0005-C3		
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 APPL ISSUE FEE	2501	1	480	480
PUBL. FEE- EARLY, VOLUNTARY, OR NORMAL	1504	1	0	0
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				480

Electronic Acknowledgement Receipt	
EFS ID:	27992192
Application Number:	15195606
International Application Number:	
Confirmation Number:	8706
Title of Invention:	SYSTEM AND METHOD FOR AUTHENTICATING USERS
First Named Inventor/Applicant Name:	Guy Fielder
Customer Number:	27571
Filer:	Tarek N. Fahmi/Sarah Zizzo
Filer Authorized By:	Tarek N. Fahmi
Attorney Docket Number:	5101-0005-C3
Receipt Date:	06-JAN-2017
Filing Date:	28-JUN-2016
Time Stamp:	13:20:49
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	\$480
RAM confirmation Number	010617INTEFSW13204600
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	Web85b.pdf	46028	no	2
			80b460e14d253f1cf81f320cd71a8221c7c48af		
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	32141	no	2
			17774c3282d964416d7ff07572634dbd2d89987a		
Warnings:					
Information:					
Total Files Size (in bytes):			78169		
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
15/195,606	06/28/2016	Guy Fielder	5101-0005-C3

CONFIRMATION NO. 8706

POA ACCEPTANCE LETTER



27571
Ascenda Law Group, PC
333 W San Carlos St.
Suite 200
San Jose, CA 95110

Date Mailed: 12/27/2016

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 12/21/2016.

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.

/nhorne/

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/AIA/82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	15/195,606
Filing Date	06-28-2016
First Named Inventor	Guy Fielder
Title	SYSTEM AND METHOD FOR AUTHENTICATING USERS
Art Unit	2491
Examiner Name	Shaw, Brian F
Attorney Docket Number	5101-0005-C3

SIGNATURE of Applicant or Patent Practitioner

Signature	/Tarek N. Fahmi/	Date (Optional)	2016-12-21
Name	Tarek N. Fahmi	Registration Number	41402
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 _____ 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.

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:
- 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):

PACid Technologies, 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	Guy L. Fielder		
Title	Chief Executive Officer/Founder, PACid Technologies, LLC		

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 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.

Electronic Acknowledgement Receipt	
EFS ID:	27867622
Application Number:	15195606
International Application Number:	
Confirmation Number:	8706
Title of Invention:	SYSTEM AND METHOD FOR AUTHENTICATING USERS
First Named Inventor/Applicant Name:	Guy Fielder
Customer Number:	27571
Filer:	Tarek N. Fahmi/Sarah Zizzo
Filer Authorized By:	Tarek N. Fahmi
Attorney Docket Number:	5101-0005-C3
Receipt Date:	21-DEC-2016
Filing Date:	28-JUN-2016
Time Stamp:	16:08:30
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	Assignee showing of ownership per 37 CFR 3.73	5101-0005-C3_Statement_3-73c.pdf	96009	no	3
			a7a706fcd5e9948f9ea0c39bc362bdf5c109d6c		

Warnings:

Information:					
2	Power of Attorney	2016-12-21_5101-0005-C3_POA.pdf	358533	no	2
			d6ef2041f39275a46896fb6fd6fd6f485b4dc15de8		
Warnings:					
Information:					
Total Files Size (in bytes):			454542		
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.					

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: PACID TECHNOLOGIES, LLC

Application No./Patent No.: 15/195,606 Filed/Issue Date: 06-28-2016

Titled: SYSTEM AND METHOD FOR AUTHENTICATING USERS

PACID TECHNOLOGIES, LLC, a company

(Name of Assignee)

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

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

1. ☒ The assignee of the entire right, title, and interest.
2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):
- ☐ The extent (by percentage) of its ownership interest is ____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.
- ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

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

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

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

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

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

- A. ☒ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel 024869, Frame 0590, or for which a copy thereof is attached.
- B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

2. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

[Page 1 of 2]

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

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

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

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

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

/Tarek N. Fahmi/

2016-12-21

Signature

Date

Tarek N. Fahmi

41402

Printed or Typed Name

Title or Registration Number

Privacy Act Statement

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

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

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



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
15/195,606	06/28/2016	Guy Fielder	5101-0005-C3

CONFIRMATION NO. 8706

27571
Ascenda Law Group, PC
333 W San Carlos St.
Suite 200
San Jose, CA 95110

PUBLICATION NOTICE



Title:SYSTEM AND METHOD FOR AUTHENTICATING USERS

Publication No.US-2016-0308844-A1

Publication Date:10/20/2016

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 Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, 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 <http://pair.uspto.gov/>. 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 Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101



UNITED STATES PATENT AND TRADEMARK OFFICE

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

27571 7590 10/06/2016
Ascenda Law Group, PC
333 W San Carlos St.
Suite 200
San Jose, CA 95110

EXAMINER

SHAW, BRIAN F

ART UNIT

PAPER NUMBER

2491

DATE MAILED: 10/06/2016

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/195,606	06/28/2016	Guy Fielder	5101-0005-C3	8706

TITLE OF INVENTION: SYSTEM AND METHOD FOR AUTHENTICATING USERS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$480	\$0	\$0	\$480	01/06/2017

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

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

HOW TO REPLY TO THIS NOTICE:

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

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

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

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

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

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

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

PART B - FEE(S) TRANSMITTAL

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

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

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

27571 7590 10/06/2016
Ascenda Law Group, PC
333 W San Carlos St.
Suite 200
San Jose, CA 95110

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

Certificate of Mailing or Transmission

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

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/195,606	06/28/2016	Guy Fielder	5101-0005-C3	8706

TITLE OF INVENTION: SYSTEM AND METHOD FOR AUTHENTICATING USERS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$480	\$0	\$0	\$480	01/06/2017

EXAMINER	ART UNIT	CLASS-SUBCLASS
SHAW, BRIAN F	2491	713-181000

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

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

2. For printing on the patent front page, list

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

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

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

(A) NAME OF ASSIGNEE

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

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

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

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

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

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

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.
15/195,606	06/28/2016	Guy Fielder	5101-0005-C3	8706
27571 7590 10/06/2016 Ascenda Law Group, PC 333 W San Carlos St. Suite 200 San Jose, CA 95110			EXAMINER SHAW, BRIAN F	
			ART UNIT 2491	PAPER NUMBER

DATE MAILED: 10/06/2016

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

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

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

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

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

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

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

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. 15/195,606	Applicant(s) FIELDER, GUY	
	Examiner BRIAN SHAW	Art Unit 2491	AIA (First Inventor to File) 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 06/28/2016.
☐ 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 1-22. 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) | 5. ☐ Examiner's Amendment/Comment |
| 2. ☒ Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____ | 6. ☒ Examiner's Statement of Reasons for Allowance |
| 3. ☐ Examiner's Comment Regarding Requirement for Deposit
of Biological Material | 7. ☐ Other _____. |
| 4. ☐ Interview Summary (PTO-413),
Paper No./Mail Date _____. | |

/BRIAN SHAW/
Primary Examiner, Art Unit 2491

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

DETAILED ACTION

Reasons For Allowance

1. Claims 1 – 22 are allowed.
2. The following is an examiner's statement of reasons for allowance:

Claims 1 – 22 are allowable over the prior art since the prior art references taken individually or in combination fail to particularly disclose, fairly suggest, or render obvious Applicant's independent claim language.

The Examiner asserts the prior art of record does not suggest Applicant's novel aspect and claim language of transmitting a secret encoded communication responsive to receiving a prompted for and verified user input responsive to receiving an identifier associated with the secret, wherein the secret is generated based on the verified user input, and stored with the identifier in a directory.

Fielder_6049612 (US Patent No. 6049612 A1) is relied upon to teach the secret is generated and stored with the identifier in a directory (reads on the constant value is stored in the encrypted information file, see Fielder_6049612 Figure 5); however, Fielder_6049612 does not teach Applicant's novel claim language.

Fielder_5995624 (US Patent No. 5995624 A1) is relied upon to teach transmitting a secret encoded communication (reads on encrypting all exchanges between the systems, see

Fielder_5995624 col. 10 lines 13 – 34); however Fielder_5995624 does not remedy the deficiencies of the prior art of record.

Cox (US Pub. No. 2005/0076061) is relied upon to teach extracting a secrets file name (reads on file names for the licensed digital content files are randomly generated in a manner such that the licensed digital content files cannot be distinguished from the dummy files, see Cox para 0010 and 0026) from the first message digest (The Examiner construes this to be an obvious limitation of the disclosure of Cox because Cox teaches the file names comprise randomly generated characters and Cox does not limit or preclude any particular method of generating those randomly generated characters. As a result of one of ordinary skill in the art also being one of ordinary creativity, using a message digest as a source for random characters, would have been obvious because a message digest is reasonably scoped as an output of a random generator that produces a series of randomly generated characters and one of ordinary skill in the art would reasonably look to use any source of random characters that met the needs of the business in order to generate the disclosed randomly generated file names, see Cox para 0010 and 0026); however, integrating the teachings of Cox do not remedy the deficiencies of the previous references.

Matyas (US Patent No. 5953420) is relied upon to teach generating, by an application running on a computing device and according to a unique user input, a secret (see Matyas Figure 2); however, integrating the teachings of Matyas do not remedy the deficiencies of the previous references.

Accordingly, the prior art does not suggest Applicant's independent claim language.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brian Shaw whose telephone number is (571) 270-5191. The examiner can normally be reached on Mon-Thurs. from Monday through Thursday 6:30 A.M. to 2:30 P.M..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ashok Patel can be reached on (571) 272-3972. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRIAN SHAW/

Primary Examiner, Art Unit 2491

EAST Search History**EAST Search History (Prior Art)**

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	9094	(generat\$5 OR creat\$5 OR calculat\$5) SAME (directory) SAME (secret OR key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/09/28 15:46
L2	3527	((generat\$5 OR creat\$5 OR calculat\$5) NEAR5(secret OR key)) SAME (directory)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/09/28 15:47
L3	6284	(secret OR key) NEAR4 (directory)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/09/28 15:48
L4	2586	1 AND 3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/09/28 15:48
L5	276775	((generat\$5 OR creat\$5 OR calculat\$5) NEAR5(secret OR key))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/09/28 15:48
L6	2957	5 AND 3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/09/28 15:49
L7	1075	6 AND ((H04L63/08,0428,20,10 OR H04L9/0861,14,0894 OR G06F21/6209,62 OR h04I2209/24 OR G06F2221/2107).CPC. OR (713/168,193,181,165 OR 726/1,26,17,21,4 OR 380/44,278 OR 709/231).CCLS.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/09/28 15:49
L8	1039	(store OR storing OR stored) NEAR4	US-PGPUB;	OR	ON	2016/09/28

		((secret OR key) NEAR4 (directory))	USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			15:54
L9	697	5 AND 8	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/09/28 15:54
L10	284	9 AND ((H04L63/08,0428,20,10 OR H04L9/0861,14,0894 OR G06F21/6209,62 OR h04I2209/24 OR G06F2221/2107).CPC. OR (713/168,193,181,165 OR 726/1,26,17,21,4 OR 380/44,278 OR 709/231).CCLS.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/09/28 15:54
L11	265	5 SAME 8	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/09/28 15:55
L12	120	11 AND ((H04L63/08,0428,20,10 OR H04L9/0861,14,0894 OR G06F21/6209,62 OR h04I2209/24 OR G06F2221/2107).CPC. OR (713/168,193,181,165 OR 726/1,26,17,21,4 OR 380/44,278 OR 709/231).CCLS.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/09/28 15:55
L13	60	12 AND @RLAD<="20090325"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/09/28 16:08
L14	54	12 AND @RLAD<="20090324"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/09/28 16:56
L16	45745	((generat\$5 OR creat\$5 OR calculat\$5) NEAR5(secret OR key)).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/09/28 17:10

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L15	91311	(((H04L63/08,0428,20,10 OR	US-	OR	ON	2016/09/28

		H04L9/0861,14,0894 OR G06F21/6209,62 OR h04l2209/24 OR G06F2221/2107).CPC. OR (713/168,193,181,165 OR 726/1,26,17,21,4 OR 380/44,278 OR 709/231).CCLS.)	PGPUB; USPAT			17:10
L17	45745	((generat\$5 OR creat\$5 OR calculat\$5) NEAR5(secret OR key)).clm.	US-PGPUB; USPAT	OR	ON	2016/09/28 17:10
L18	124	((store OR storing OR stored) NEAR4 ((secret OR key) NEAR4 (directory))).clm.	US-PGPUB; USPAT	OR	ON	2016/09/28 17:11
L21	24	I17 SAME I18	US-PGPUB; USPAT	OR	ON	2016/09/28 17:11
L22	12	I15 AND I21	US-PGPUB; USPAT	OR	ON	2016/09/28 17:12

9/ 28/ 2016 5:20:47 PM

C:\ Users\ bshaw\ Documents\ EAST\ Workspaces\ 15195606.wsp

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.

Substitute for form 1449/PTO		<i>Complete if Known</i>	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)		Application Number	
		Filing Date	
		First Named Inventor	Guy Fielder
		Art Unit	
		Examiner Name	
Sheet	1	of	9
Attorney Docket No: 5101-0005-C3			

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number-Kind Code ² (if known)			
		4613901	09/23/1986	GILHOUSEN; et al.	
		4649233	03/10/1987	BASS; et al.	
		4720860	01/19/1988	WEISS	
		4864615	09/05/1989	BENNETT; et al.	
		4924515	05/08/1990	MATYAS; et al.	
		4937866	06/26/1990	CROWTHER; et al.	
		5020105	05/28/1991	ROSEN; et al.	
		5060263	10/22/1991	BOSEN; et al.	
		5065429	11/12/1991	LANG	
		5068894	11/26/1991	HOPPE	
		5153919	10/06/1992	REEDS, III; et al.	
		5233655	08/03/1993	SHAPIRO	
		5237610	08/17/1993	GAMMIE; et al.	
		5241598	08/31/1993	RAITH	
		5309516	05/03/1994	TAKARAGI; et al.	
		5355413	10/11/1994	OHNO	
		5361062	11/01/1994	WEISS; et al.	
		5367572	11/22/1994	WEISS	
		5475758	12/12/1995	KIKUCHI	
		5475826	12/12/1995	FISCHER	
		5481611	01/02/1996	OWENS; et al.	
		5495533	02/27/1996	LINEHAN; et al.	
		5638448	06/10/1997	NGUYEN	

EXAMINER SIGNATURE**DATE CONSIDERED**

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached. 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 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, 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 (1-800-786-9199) and select option 2.

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

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.

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	
				Filing Date	
				First Named Inventor Guy Fielder	
				Art Unit	
				Examiner Name	
(Use as many sheets as necessary)					
Sheet	2	of	9	Attorney Docket No: 5101-0005-C3	

	5757924	05/26/1998	FRIEDMAN; et al.	
	5796830	08/18/1998	JOHNSON; et al.	
	5953420	09/14/1999	MATYAS, JR.; et al.	
	5963646	10/05/1999	FIELDER; et al.	
	5963696	10/05/1999	YOSHIDA; et al.	
	5966441	10/12/1999	CALAMERA	
	5974550	10/26/1999	MALISZEWSKI	
	5995623	11/30/1999	KAWANO; et al.	
	5995624	11/30/1999	FIELDER; et al.	
	6049612	04/11/2000	FIELDER; et al.	
	6105133	08/15/2000	FIELDER; et al.	
	6345101	02/05/2002	SHUKLA	
	6490353	12/03/2002	TAN	
	6587563	07/01/2003	CRANDALL	
	6636968	10/21/2003	ROSNER; et al.	
	6769060	07/27/2004	DENT; et al.	
	6947556	09/20/2005	MATYAS, JR.; et al.	
	6987853	01/17/2006	UNER	
	7032240	04/18/2006	CRONCE; et al.	
	7095855	08/22/2006	COLLINS	
	7178025	02/13/2007	SCHEIDT; et al.	
	7890769	02/15/2011	CHEN; et al.	
	20020143872	10/03/2002	WEISS; et al.	
	20020191796	12/19/2002	MUSCHENBORN	
	20040025028	02/05/2004	TAKEUCHI	
	20040179684	09/16/2004	APPENZELLER; et al.	
	20040230800	11/18/2004	FUTA; et al.	

EXAMINER SIGNATURE**DATE CONSIDERED**

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached. 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 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, 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 (1-800-786-9199) and select option 2.

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

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.

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)				Application Number	
				Filing Date	
				First Named Inventor	Guy Fielder
				Art Unit	
				Examiner Name	
Sheet	3	of	9	Attorney Docket No: 5101-0005-C3	

		20050039030	02/17/2005	RODGERS; et al.	
		20050063352	03/24/2005	AMARA; et al.	
		20050076061	04/07/2005	COX	
		20060112418	05/25/2006	BANTZ; et al.	
		20060174349	08/03/2006	CRONCE; et al.	
		20060210082	09/21/2006	DEVADAS; et al.	
		20060271697	11/30/2006	KRUSE	
		20070130463	06/07/2007	LAW; et al.	
		20070150742	06/28/2007	CUKIER; et al.	
		20070255941	11/01/2007	ELLIS	
		20070258584	11/08/2007	BROWN; et al.	
		20080065880	08/13/2008	MARTIN; et al.	
		20080098464	04/24/2008	MIZRAH	
		20080244078	10/02/2008	VILJOEN; et al.	
		20080270791	10/30/2008	NYSTROM; et al.	
		20090094520	04/09/2009	KULAS	
		20100070778	03/18/2010	MURRAY; et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶
		Country Code ³⁻ Number ⁴ Kind Code ⁵ (if known)				
		EP 1304848 A2	04/23/2003	MICROSOFT CORP		
		EP 1478156 A2	11/17/2004	SAMSUNG ELECTRONICS CO., LTD.		
		EP 1906587 A2	04/02/2008	THOMSON LICENSING INC		

EXAMINER SIGNATURE

DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached. 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 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, 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 (1-800-786-9199) and select option 2.

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

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.

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Application Number	
				Filing Date	
				First Named Inventor	Guy Fielder
				Art Unit	
				Examiner Name	
Sheet	4	of	9	Attorney Docket No: 5101-0005-C3	

		GB 2421407 A	06/21/2006	HEWLETT PACKARD DEVELOPMENT CO		
		GB 2478147 A	08/31/2011	KINDBERG TIMOTHY PAUL JAMES GERARD; et al.		
		WO 2005107287 A1	11/10/2005	STORCARD, INC.; et al.		
		WO 2005119397 A1	12/15/2005	AXALTO SA; et al.		
		WO 2009074056 A1	06/18/2009	FIRE FLIGHT (PTY) LTD		
		WO 2010103345 A1	09/16/2010	NOKIA CORPORATION; et al.		
		WO 2010149407 A1	12/29/2010	GEMALTO SA; et al.		
		WO 2011068719 A1	06/09/2011	ALCATEL LUCENT; et al.		
		WO 2011089143 A1	07/28/2011	INTRINSIC ID B.V.; et al.		
		WO 03/077469 A1	09/18/2003	CERTICOM CORP; et al.		
		WO 2004/092864 A2	10/28/2004	MATSUSHITA ELECTRIC IND CO LTD; et al.		
		WO 2007/005909 A2	01/11/2007	COVELY		
		WO 2008/061848 A2	05/29/2008	THOMSON LICENSING; et al.		
		WO 98/47258 A2	10/22/1998	FIELDER; et al.		

NON PATENT LITERATURE DOCUMENTS					
Examiner Initials*	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume- issue number(s), publisher, city and/or country where published.			T2
		Barrett, Daniel and Sliverman, Richard, "SSH, The Secure Shell: The Definitive Guide, 2nd Edition", O'Reilly Media, Section 2.4, Section 3.3, Section 3.4, Section 6.1-6.7, May 1, 2005.			
		Bellare, Mihir Rogaway, Phillip, "Entity Authentication and Key Distribution," Advances in Crypto 1993 Proceedings, Springer-verlag (August 1993).			

EXAMINER SIGNATURE

DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached. 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 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, 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 (1-800-786-9199) and select option 2.

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

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.

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)				Application Number	
				Filing Date	
				First Named Inventor Guy Fielder	
				Art Unit	
				Examiner Name	
Sheet	5	of	9	Attorney Docket No: 5101-0005-C3	

		Berson, Thomas A., "Differential Cryptanalysis Mod 232 with Applications to MD5". EUROCRYPT (1992), 658-71-80.	
		Bert den Boer, Antoon Bosselaers (1993). Collisions for the Compression Function of MD5. Berlin; London: Springer. ISBN 3-540-57600-2.	
		Bird, R. et al, "The KryptoKnight Family of Light-Weight Protocols for Authentication and Key Distribution," IEEE/ACM Transactions on Networking, Vol. 3, No.1, pages 31-41, IEEE Press, Piscataway, NJ, Feb. 1995.	
		Brenno de Winter (Fischer v. Mollard); "Gnu Privacy Guard (GnuPG) Mini Howto"; retrieved from the Internet: http://www.gnupg.org/documentation/howtos.en.html , version 0.1.4; August 10, 2004 (14 pages)	
		Carl Meyer and S.M. Matyas, CRYPTOGRAPHY: A NEW DIMENSION IN COMPUTER DATA SECURITY (1982).	
		Cheng, P. et al., Modular Key Management Protocol (MKMP). November 28, 1994.	
		Damgard; "A Design Principle for Hash Functions"; Advances in Cryptology: Proceedings of CRYPTO '89, vol. 433 of Lecture Notes in Computer Science, pp. 416-427; Springer-Verlag, New York (12 pages).	
		Decker et al.; "The SumoDacs-project: Secure Mobile Data Access with a Tamperproof Hardware Token"; eChallenges e-2010 Conference Proceedings, IIMC; 2010 (8 pages).	
		Ehrtam, W.F. et al., A Cryptographic Key Management Scheme for Implementing the Data Encryption Standard, IBM Sys. J., Vol. 17 No.2, 1978.	
		Freier, A. et al., "SSL Version 3.0," Netscape Communications Corporation, December 1995.	
		Gong, L., "Using One-Way Functions for Authentication," ACM Sigcom Computer Communication Review, Vol. 19, Issue 5, pages 8-11, New York, 1989.	
		Gunson et al.; "User Perceptions of Security and Usability of Single-Factor and Two-Factor Authentication in Automated Telephone Banking"; Computers & Security (2011) vol. 30, no. 4; pp. 208-220 (13 pages).	
		Hans Dobbertin, "The Status of MD5 After a Recent Attack", RSA Laboratories; CryptoBytes, 1996.	
		Hans Dobbertin, Cryptanalysis of MD5 Compress, May 2, 1996.	

EXAMINER SIGNATURE

DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached. 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 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, 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 (1-800-786-9199) and select option 2.

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

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.

Substitute for form 1449/PTO				<i>Complete if Known</i>	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)				Application Number	
				Filing Date	
				First Named Inventor	Guy Fielder
				Art Unit	
				Examiner Name	
Sheet	6	of	9	Attorney Docket No: 5101-0005-C3	

		International Preliminary Report on Patentability and The Written Opinion issued in PCT/US2010/028562; Dated: October 6, 2011; (22 pages).	
		International Preliminary Report on Patentability and The Written Opinion issued in PCT/US2010/028565 Dated: October 6, 2011; (23 pages).	
		International Preliminary Report on Patentability and The Written Opinion issued in PCT/US2010/028566; Dated: October 6, 2011; (14 pages).	
		International Preliminary Report on Patentability and The Written Opinion issued in PCT/US2010/028582; Dated: October 6, 2011 (8 pages).	
		International Preliminary Report on Patentability and The Written Opinion issued in PCT/US2010/028583; Dated: October 6, 2011; (9 pages).	
		International Search Report and The Written Opinion issued in PCT/US2010/028562; Dated: September 29, 2010; (31 pages).	
		International Search Report and The Written Opinion issued in PCT/US2010/028565; Dated: October 6, 2010; (31 pages).	
		International Search Report and The Written Opinion issued in PCT/US2010/028566; Dated: December 30, 2010; (17 pages).	
		International Search Report and The Written Opinion issued in PCT/US2010/028582; Dated: July 30, 2010; (21 pages).	
		International Search Report and The Written Opinion issued in PCT/US2010/028583; Dated: July 6, 2010; (21 pages).	
		Javinen et al.; "Embedded SFE: Offloading Server and Network Using Hardware Tokens"; Financial Cryptography and Data Security Proceeding, 14th International Conference, FC 2010; Tenerife, Canary Islands, January 25-28, 2010 (15 pages).	
		Kaya (2003). Secure multicast groups on ad hoc networks. SASN '03 Proceedings of the 1st ACM Workshop on Security of ad hoc and sensor networks, pages 94-102.	
		Kelsey, John et al., "Passphrase FAQ," alt.security.pgp, October 1993.	
		Krawczyk, H., "SKEME: A Versatile Secure Key Exchange Mechanism for Internet," Proceedings of the 1996 Symposium on Network and Distributed System Security (SNDSS) '96, pages 114-127, IEEE Computer Society, Washington, DC (1996).	

EXAMINER SIGNATURE**DATE CONSIDERED**

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached. 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 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, 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 (1-800-786-9199) and select option 2.

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

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.

Substitute for form 1449/PTO				<i>Complete if Known</i>	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)				Application Number	
				Filing Date	
				First Named Inventor Guy Fielder	
				Art Unit	
				Examiner Name	
Sheet	7	of	9	Attorney Docket No: 5101-0005-C3	

		Leighton, T., "Secret Key Agreement without Public-Key Cryptography," Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology, Santa Barbara, CA, pages 456-479, Springer-Verlag, New York, 1998.	
		Lin et al.; "A Practical Electronic Payment System for Message Delivery Service in the Mobile Environment"; Wireless Personal Communications, vol. 42, no. 2; pp. 247-261; July 2007 (15 pages).	
		Matyas, S.M. & Meyer, C.H., "Generation, Distribution, and Installation of Cryptographic Keys," 17 IBM Sys. J. 2 (1978).	
		Menezes, Alfred J. et al. HANDBOOK OF APPLIED CRYPTOGRAPHY. CRC Press, October 16, 1996.	
		Merkle, R., "One Way Hash functions and DES," In In G. Brassard, editor, Advances in Cryptology: Proceedings of CRYPTO'89, vol. 435 of Lecture Notes in Computer Science, pages 428-446, Springer-Verlag, New York, 1990.	
		Molva, Reflik et al., "KryptoKnight Authentication and Key Distribution System," Computer Security-ESORICS 92 (Nov. 23-25, 1992).	
		Preneel, B., "MDx-MAC and Building Fast MAGs from Hash Functions," Lecture Notes in Computer Science, Vol. 963, Proceedings of the 15th Annual International Cryptology Conference on Advances in Cryptology, pages 1-14, Springer-Verlag, London, UK (1995).	
		Rivest, R. "The MD5 Message-Digest Algorithm." IETF RFC 1321. April 1992.	
		RSA Laboratories, "PKCS #5: Password-Based Encryption Standard," version 1.5, November 1993.	
		RSA Laboratories, PKCS #5 v2.0: Password-Based Cryptography Standard, March 25, 1999.	
		Schneider, B., "Security Pitfalls in Cryptography", Counterpane Systems, www.counterpane.com/publish.html, 1998, (11 pages).	
		Schneier, B., "Cryptographic Design Vulnerabilities", Counterpane Systems, www.counterpane.com/publish.html, September 1998, (5 pages).	
		Schneier, Bruce, APPLIED CRYPTOGRAPHY, Katherine Schowalter, 1996 (and first edition (1994) of same).	

EXAMINER SIGNATURE**DATE CONSIDERED**

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached. 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 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, 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 (1-800-786-9199) and select option 2.

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

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.

Substitute for form 1449/PTO				<i>Complete if Known</i>	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)				Application Number	
				Filing Date	
				First Named Inventor Guy Fielder	
				Art Unit	
				Examiner Name	
Sheet	8	of	9	Attorney Docket No: 5101-0005-C3	

		Schneier. B . "Why Cryptography is Harder Than it Looks". Counterpane Systems, www.counterpane.com/publish. html, 1997, (8 pages).	
		Sun et al.; "A New Design of Wearable Token System for Mobile Device Security"; IEEE Transactions on Consumer Electronics, vol. 54, no. 4; pp. 1784-1789; November 2008 (6 pages).	
		U.S. Department of Commerce, National Institute of Standards and Technology, "Secure Hash Standard", FIPS PUB 180-1, April 17, 1995. (24 pages).	
		Windows '95 Vulnerabilities, US Department of Energy, Computer Incident Advisory Committee, available at http://ftp.cerias.purdue.edu/pub/lists/academic-firewalls/academic-firewalls.951224 (1995).	
		Yuill, J., Denning, D., Feer, F.; "Using Deception to Hide Things from Hackers: Processes, Principles, and Techniques", Journal of Information Warfare, (16 pages).	

EXAMINER SIGNATURE

/Brian Shaw/

DATE CONSIDERED 10/03/2016

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached. 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 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, 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 (1-800-786-9199) and select option 2.

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

[Web](#)
[Images](#)
[More...](#)

[Sign In](#)

[Scholar](#)
About 20,200 results (0.06 sec)

Articles

Case law

My library

Any time

Since 2016

Since 2015

Since 2012

Custom range...

Sort by relevance

Sort by date

☐ include patents

☐ include citations

Create alert

Technique for synchronizing security credentials from a master **directory, platform, or registry**

RC Leah, JR McGarvey - US Patent 6,986,038, 2006 - Google Patents

... unless the **directory** software is identical) and thus would be unable to **generate** a hash ... at the master registry, and the user knows the password used to **create** those credentials ... there (perhaps because the user has forgotten the password value used in **creating** those credentials ...

Cited by 32 Related articles All 2 versions Cite Save

Linking security association to entries in a contact **directory of a wireless device**

S Moloney, J Teinila, N Asokan ... - US Patent App. 10/ ..., 2004 - Google Patents

... particular embodiments of such a communication device, the processing arrangement is configured to **create** the authorization **identifier**, such as, for example, **creating** the authorization ... specification v1.2. At block 520, the link key is used to **generate** an encryption ...

Cited by 108 Related articles All 2 versions Cite Save

Health information identification and de-identification toolkit. [PDF] nih.

IS Kohane, H Dong, P Szolovits - Proceedings of the AMIA ..., 1998 - ncbi.nlm.nih.gov

... Each principal can **create** and share with others local name spaces with which she can refer to ... These bioinformatics databases have begun to **generate** a lot of confidentiality concerns ... The **identifier** for the central database is **generated** by encrypting the Source ID with the public ...

Cited by 22 Related articles All 5 versions Cite Save

Bilateral authentication and encryption system

GL Fielder, PN Alito - US Patent 6,105,133, 2000 - Google Patents

... and **generating** therefrom a pseudo-random message digest is repeated n times to **create** a message ... 2 could be made to **generate** a message digest with encryption key components of ... US8234638 *, Dec 27, 2005, Jul 31, 2012, Hercules Software, Llc, **Creating** a relatively unique ...

Cited by 82 Related articles All 2 versions Cite Save

Method and system for **creating and utilizing managed roles in a **directory** system**

D Boreham, P Rowley, MC Smith - US Patent 6,785,686, 2004 - Google Patents

... Additionally, roles allow for support of **generated** attribute values, and **directory** server-performed membership verification for ... As an example, suppose one wants to **create** a role to be assigned to all marketing ... After **creating** a role in a similar manner to that of a managed role, a ...

Cited by 62 Related articles All 4 versions Cite Save

Removable media for password based authentication in a distributed system

AD Eldridge, CW Kaufman - US Patent 6,061,799, 2000 - Google Patents

... 3B, to **generate** a key **identifier**. ... data may occur in a successive, iterative manner until a match occurs or all keys for all of the password data contained on medium 620 have been **generated** and compared to ... Method of **creating** password list for remote authentication to services. ...

Cited by 144 Related articles All 2 versions Cite Save

Tahoe: the least-authority filesystem [PDF] res

Z Wilcox-O'Hearn, B Warner - Proceedings of the 4th ACM international ..., 2008 - dl.acm.org

... This is because the initial creator of the immutable file could **generate** some erasure code shares ... caps and write-caps we **create** small (16-byte) **secrets** cryptographically linked to the RSA keys ... **Creating** a new DSA key is as easy as choosing an unguessable **secret** x (and a ...

Cited by 207 Related articles All 15 versions Cite Save

Technique for synchronizing security credentials using a trusted authenticating domain

RC Leah, JR McGarvey - US Patent 6,986,039, 2006 - Google Patents

... unless the **directory** software is identical) and thus would be unable to **generate** a hash ... Several means of **creating** such a secure connection, with both data protection and authentication of ... at the master registry, and the user knows the password used to **create** those credentials. ...

Cited by 32 Related articles All 2 versions Cite Save

Security token

H Gregory - US Patent App. 12/002,705, 2007 - Google Patents

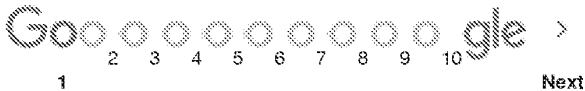
... [0013]. Conventional password generators that **create** unique passwords ... If there is no special

format requirement, a step 414 uses a default format to **generate** an authentication ... Once authentication code for user is **generated**, step 520 sends it out with the user name to server. ...
Cited by 10 Related articles All 2 versions Cite Save

Secure computer data storage method and device

J Debiez · US Patent App. 10/548,459, 2004 · Google Patents
... of the equipment whilst publishing its existence, possibly before authentication, by **generating** randomly by ... Writing new data, new files or **creating** new **directories** is possible, the storage ... unique **secret** identification element 7 **generated** and **stored** imperatively internally of the ...
Cited by 25 Related articles All 2 versions Cite Save

 Create alert



[About Google Scholar](#) [Privacy](#) [Terms](#) [Provide feedback](#)

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S2440	53	pacid.as. AND fielder.in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/09/04 21:05
S2441	374	(file OR directory) SAME unique SAME identifier SAME secret	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/09/04 21:06
S2442	22	S2440 AND S2441	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/09/04 21:06
S2443	185337	((H04L63/08 OR H04L63/0428 OR H04L63/20 OR H04L9/0861 OR H04L63/10 OR G06F21/6209 OR G06F2221/2107 OR G06F21/62).CPC. OR (713/168 OR 713/193 OR 713/181 OR 713/165 OR 726/1 OR 726/26 OR 726/17 OR 726/21 OR 726/4 OR 380/44 OR 380/278 OR 709/231).CCLS.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/09/04 21:21
S2444	192946	((H04L63/08,0428,20,10 OR H04L9/0861,14,0894 OR G06F21/6209,62 OR h04l2209/24 OR G06F2221/2107).CPC. OR (713/168,193,181,165 OR 726/1,26,17,21,4 OR 380/44,278 OR 709/231).CCLS.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/09/04 21:26
S2445	310	"6049612" "5995624" "20050076061" "5953420"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/09/04 21:27
S2446	179	((transmit\$5 OR send\$6 OR communicat\$6) SAME identifier) AND (secret SAME directory SAME identifier)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/09/04 21:33

EAST Search History

S2447	68	S2444 AND S2446	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM TDB	OR	ON	2016/09/04 21:33
-------	----	-----------------	--	----	----	---------------------

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S2448	3111	(file OR directory) SAME unique SAME identifier.clm.	US-PGPUB; USPAT	OR	ON	2016/09/04 20:59
S2449	30	(file OR directory) SAME unique SAME identifier SAME secret.clm.	US-PGPUB; USPAT	OR	ON	2016/09/04 20:59
S2450	10	(file OR directory) SAME unique SAME identifier SAME secret SAME (message OR communication).clm.	US-PGPUB; USPAT	OR	ON	2016/09/04 20:59
S2451	90455	((H04L63/08,0428,20,10 OR H04L9/0861,14,0894 OR G06F21/6209,62 OR h04I2209/24 OR G06F2221/2107).CPC. OR (713/168,193,181,165 OR 726/1,26,17,21,4 OR 380/44,278 OR 709/231).OCLS.)	US-PGPUB; USPAT	OR	ON	2016/09/04 21:36
S2452	15	S2449 AND S2451	US-PGPUB; USPAT	OR	ON	2016/09/04 21:37

9/ 28/ 2016 1:05:49 PM

C:\Users\bshaw\Documents\EAST\Workspaces\15195606.wsp

Search Notes 	Application/Control No. 15195606	Applicant(s)/Patent Under Reexamination FIELDER, GUY
	Examiner BRIAN SHAW	Art Unit 2491

CPC- SEARCHED		
Symbol	Date	Examiner
H04L63/08,0428,20,10	09/28/16	BS
H04L9/0861,14,0894	09/28/16	BS
G06F21/6209,62	09/28/16	BS
h04I2209/24	09/28/16	BS
G06F2221/2107	09/28/16	BS

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
713	168,193,181,165	09/28/16	BS
726	1,26,17,21,4	09/28/16	BS
380	44,278	09/28/16	BS
709	231	09/28/16	BS
SEE	SEARCH NOTES	09/28/16	BS

SEARCH NOTES		
Search Notes	Date	Examiner
East (USPAT, USPGPUB, EPO, USOCR, FERS, JPO, DERWENT, IBM_TDB) - see Search Notes	09/28/16	BS
Inventor/Assignee Search - PALM	09/28/16	BS
NPL Search	09/28/16	BS

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

--	--

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
H04L63/08,042 8,20,10		09/28/16	BS
H04L9/0861,14 ,0894		09/28/16	BS
G06F21/6209,6 2		09/28/16	BS
h04l2209/24		09/28/16	BS
G06F2221/210 7		09/28/16	BS
713	168,193,181,165	09/28/16	BS
726	1,26,17,21,4	09/28/16	BS
380	44,278	09/28/16	BS
709	231	09/28/16	BS
SEE	SEARCH NOTES	09/28/16	BS

--	--

Issue Classification 	Application/Control No. 15195606	Applicant(s)/Patent Under Reexamination FIELDER, GUY	
	Examiner BRIAN SHAW	Art Unit 2491	

CPC						
Symbol					Type	Version
H04L		63		0428	F	2013-01-01
H04L		9		14	I	2013-01-01
H04L		9		0894	I	2013-01-01
H04L		2209		24	A	2013-01-01

CPC Combination Sets						
Symbol			Type	Set	Ranking	Version

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	22	
/BRIAN SHAW/ Primary Examiner.Art Unit 2491	08/20/2016	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

Issue Classification 	Application/Control No. 15195606	Applicant(s)/Patent Under Reexamination FIELDER, GUY
	Examiner BRIAN SHAW	Art Unit 2491

US ORIGINAL CLASSIFICATION						INTERNATIONAL CLASSIFICATION													
CLASS			SUBCLASS			CLAIMED					NON-CLAIMED								
713			181			H	0	4	L	9 / 32 (2006.01.01)									
CROSS REFERENCE(S)																			
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)																		

NONE		Total Claims Allowed:	
		22	
(Assistant Examiner)	(Date)		
/BRIAN SHAW/ Primary Examiner.Art Unit 2491	08/20/2016	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

<i>Index of Claims</i> 	Application/Control No. 15195606	Applicant(s)/Patent Under Reexamination FIELDER, GUY
	Examiner BRIAN SHAW	Art Unit 2491

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

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

CLAIM		DATE								
Final	Original	08/20/2016								
	1	=								
	2	=								
	3	=								
	4	=								
	5	=								
	6	=								
	7	=								
	8	=								
	9	=								
	10	=								
	11	=								
	12	=								
	13	=								
	14	=								
	15	=								
	16	=								
	17	=								
	18	=								
	19	=								
	20	=								
	21	=								
	22	=								



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. 8706

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.		
15/195,606	06/28/2016	713	2491	5101-0005-C3		
APPLICANTS PACID TECHNOLOGIES, LLC, Austin, TX; INVENTORS Guy Fielder, Austin, TX; ** CONTINUING DATA ***** This application is a CON of 14/861,630 09/22/2015 PAT 9411972 which is a CON of 14/228,463 03/28/2014 PAT 9165153 which is a CON of 13/203,327 08/25/2011 PAT 8726032 which is a 371 of PCT/US10/28562 03/25/2010 which claims benefit of 61/163,406 03/25/2009 ** FOREIGN APPLICATIONS ***** ** IF REQUIRED, FOREIGN FILING LICENSE GRANTED *** SMALL ENTITY ** 07/11/2016						
Foreign Priority claimed ☐ Yes ☒ No 35 USC 119(a-d) conditions met ☐ Yes ☒ No Verified and /BRIAN F SHAW/ Acknowledged Examiner's Signature		☐ Met after Allowance Initials	STATE OR COUNTRY TX	SHEETS DRAWINGS 14	TOTAL CLAIMS 22	INDEPENDENT CLAIMS 3
ADDRESS Ascenda Law Group, PC 333 W San Carlos St. Suite 200 San Jose, CA 95110 UNITED STATES						
TITLE SYSTEM AND METHOD FOR AUTHENTICATING USERS						
FILING FEE RECEIVED 810	FEES: Authority has been given in Paper 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		

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 15/195,606				
APPLICATION AS FILED - PART I										
(Column 1)		(Column 2)		SMALL ENTITY		OTHER THAN SMALL ENTITY				
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)			
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	70		N/A				
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A	300		N/A				
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A				
TOTAL CLAIMS (37 CFR 1.16(j))	22	minus 20 = *	2	x 40 = 80	OR					
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3	minus 3 = *		x 210 = 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						
				TOTAL		TOTAL				
				810						
* If the difference in column 1 is less than zero, enter "0" in column 2.										
APPLICATION AS AMENDED - PART II										
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OTHER THAN SMALL ENTITY		
AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=	OR	x	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=	OR	x	=
	Application Size Fee (37 CFR 1.16(s))							OR		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	
AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=	OR	x	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=	OR	x	=
	Application Size Fee (37 CFR 1.16(s))							OR		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.										



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
15/195,606	06/28/2016		810	5101-0005-C3	22	3

CONFIRMATION NO. 8706

FILING RECEIPT



000000084280535

27571

Ascenda Law Group, PC
333 W San Carlos St.
Suite 200
San Jose, CA 95110

Date Mailed: 07/13/2016

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Guy Fielder, Austin, TX;

Applicant(s)

PACID TECHNOLOGIES, LLC, Austin, TX;

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 14/861,630 09/22/2015
which is a CON of 14/228,463 03/28/2014 PAT 9165153
which is a CON of 13/203,327 08/25/2011 PAT 8726032
which is a 371 of PCT/US10/28562 03/25/2010
which claims benefit of 61/163,406 03/25/2009

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: 07/11/2016

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 15/195,606**

Projected Publication Date: 10/20/2016

Non-Publication Request: No

Early Publication Request: No

**** SMALL ENTITY ****

Title

SYSTEM AND METHOD FOR AUTHENTICATING USERS

Preliminary Class

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER
Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

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.

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.

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Complete if Known</i>	
				Application Number	
				Filing Date	
				First Named Inventor Guy Fielder	
				Art Unit	
				Examiner Name	
Sheet	1	of	9	Attorney Docket No: 5101-0005-C3	

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number-Kind Code ² (if known)			
		4613901	09/23/1986	GILHOUSEN; et al.	
		4649233	03/10/1987	BASS; et al.	
		4720860	01/19/1988	WEISS	
		4864615	09/05/1989	BENNETT; et al.	
		4924515	05/08/1990	MATYAS; et al.	
		4937866	06/26/1990	CROWTHER; et al.	
		5020105	05/28/1991	ROSEN; et al.	
		5060263	10/22/1991	BOSEN; et al.	
		5065429	11/12/1991	LANG	
		5068894	11/26/1991	HOPPE	
		5153919	10/06/1992	REEDS, III; et al.	
		5233655	08/03/1993	SHAPIRO	
		5237610	08/17/1993	GAMMIE; et al.	
		5241598	08/31/1993	RAITH	
		5309516	05/03/1994	TAKARAGI; et al.	
		5355413	10/11/1994	OHNO	
		5361062	11/01/1994	WEISS; et al.	
		5367572	11/22/1994	WEISS	
		5475758	12/12/1995	KIKUCHI	
		5475826	12/12/1995	FISCHER	
		5481611	01/02/1996	OWENS; et al.	
		5495533	02/27/1996	LINEHAN; et al.	
		5638448	06/10/1997	NGUYEN	

EXAMINER SIGNATURE**DATE CONSIDERED**

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached. 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 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, 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 (1-800-786-9199) and select option 2.

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

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Complete if Known</i>	
				Application Number	
				Filing Date	
				First Named Inventor Guy Fielder	
				Art Unit	
				Examiner Name	
Sheet	2	of	9	Attorney Docket No: 5101-0005-C3	

		5757924	05/26/1998	FRIEDMAN; et al.	
		5796830	08/18/1998	JOHNSON; et al.	
		5953420	09/14/1999	MATYAS, JR.; et al.	
		5963646	10/05/1999	FIELDER; et al.	
		5963696	10/05/1999	YOSHIDA; et al.	
		5966441	10/12/1999	CALAMERA	
		5974550	10/26/1999	MALISZEWSKI	
		5995623	11/30/1999	KAWANO; et al.	
		5995624	11/30/1999	FIELDER; et al.	
		6049612	04/11/2000	FIELDER; et al.	
		6105133	08/15/2000	FIELDER; et al.	
		6345101	02/05/2002	SHUKLA	
		6490353	12/03/2002	TAN	
		6587563	07/01/2003	CRANDALL	
		6636968	10/21/2003	ROSNER; et al.	
		6769060	07/27/2004	DENT; et al.	
		6947556	09/20/2005	MATYAS, JR.; et al.	
		6987853	01/17/2006	UNER	
		7032240	04/18/2006	CRONCE; et al.	
		7095855	08/22/2006	COLLINS	
		7178025	02/13/2007	SCHEIDT; et al.	
		7890769	02/15/2011	CHEN; et al.	
		20020143872	10/03/2002	WEISS; et al.	
		20020191796	12/19/2002	MUSCHENBORN	
		20040025028	02/05/2004	TAKEUCHI	
		20040179684	09/16/2004	APPENZELLER; et al.	
		20040230800	11/18/2004	FUTA; et al.	

EXAMINER SIGNATURE**DATE CONSIDERED**

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached. 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 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, 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 (1-800-786-9199) and select option 2.

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

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Complete if Known</i>	
				Application Number	
				Filing Date	
				First Named Inventor Guy Fielder	
				Art Unit	
				Examiner Name	
Sheet	3	of	9	Attorney Docket No: 5101-0005-C3	

		20050039030	02/17/2005	RODGERS; et al.	
		20050063352	03/24/2005	AMARA; et al.	
		20050076061	04/07/2005	COX	
		20060112418	05/25/2006	BANTZ; et al.	
		20060174349	08/03/2006	CRONCE; et al.	
		20060210082	09/21/2006	DEVADAS; et al.	
		20060271697	11/30/2006	KRUSE	
		20070130463	06/07/2007	LAW; et al.	
		20070150742	06/28/2007	CUKIER; et al.	
		20070255941	11/01/2007	ELLIS	
		20070258584	11/08/2007	BROWN; et al.	
		20080065880	08/13/2008	MARTIN; et al.	
		20080098464	04/24/2008	MIZRAH	
		20080244078	10/02/2008	VILJOEN; et al.	
		20080270791	10/30/2008	NYSTROM; et al.	
		20090094520	04/09/2009	KULAS	
		20100070778	03/18/2010	MURRAY; et al.	

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No. ¹	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T 6
		Country Code ³⁻ Number ⁴ Kind Code ⁵ (if known)				
		EP 1304848 A2	04/23/2003	MICROSOFT CORP		
		EP 1478156 A2	11/17/2004	SAMSUNG ELECTRONICS CO., LTD.		
		EP 1906587 A2	04/02/2008	THOMSON LICENSING INC		

EXAMINER SIGNATURE

DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached. 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 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, 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 (1-800-786-9199) and select option 2.

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

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Complete if Known</i>	
				Application Number	
				Filing Date	
				First Named Inventor	Guy Fielder
				Art Unit	
				Examiner Name	
Sheet	4	of	9	Attorney Docket No: 5101-0005-C3	

		GB 2421407 A	06/21/2006	HEWLETT PACKARD DEVELOPMENT CO		
		GB 2478147 A	08/31/2011	KINDBERG TIMOTHY PAUL JAMES GERARD; et al.		
		WO 2005107287 A1	11/10/2005	STORCARD, INC.; et al.		
		WO 2005119397 A1	12/15/2005	AXALTO SA; et al.		
		WO 2009074956 A1	06/18/2009	FIRE-FLIGHT (PTY) LTD		
		WO 2010103345 A1	09/16/2010	NOKIA CORPORATION; et al.		
		WO 2010149407 A1	12/29/2010	GEMALTO SA; et al.		
		WO 2011068719 A1	06/09/2011	ALCATEL LUCENT; et al.		
		WO 2011089143 A1	07/28/2011	INTRINSIC ID B.V.; et al.		
		WO 03/077469 A1	09/18/2003	CERTICOM CORP; et al.		
		WO 2004/092864 A2	10/28/2004	MATSUSHITA ELECTRIC IND CO LTD; et al.		
		WO 2007/005909 A2	01/11/2007	COVELY		
		WO 2008/061848 A2	05/29/2008	THOMSON LICENSING; et al.		
		WO 98/47258 A2	10/22/1998	FIELDER; et al.		

NON PATENT LITERATURE DOCUMENTS				
Examiner Initials*	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.		T2
		Barrett, Daniel and Sliverman, Richard, "SSH, The Secure Shell: The Definitive Guide, 2nd Edition", O'Reilly Media, Section 2.4, Section 3.3, Section 3.4, Section 6.1-6.7. May 1, 2005.		
		Bellare, Mihir Rogaway, Phillip, "Entity Authentication and Key Distribution," Advances in Crypto 1993 Proceedings, Springer-Verlag (August 1993).		

EXAMINER SIGNATURE**DATE CONSIDERED**

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached. 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 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, 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 (1-800-786-9199) and select option 2.

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

Substitute for form 1449/PTO				<i>Complete if Known</i>	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Application Number	
				Filing Date	
				First Named Inventor	Guy Fielder
				Art Unit	
				Examiner Name	
Sheet	5	of	9	Attorney Docket No: 5101-0005-C3	

		Berson, Thomas A., "Differential Cryptanalysis Mod 232 with Applications to MD5". EUROCRYPT (1992), 658:71-80.	
		Bert den Boer, Antoon Bosselaers (1993). Collisions for the Compression Function of MD5. Berlin; London: Springer. ISBN 3-540-57600-2.	
		Bird, R. et al, "The KryptoKnight Family of Light-Weight Protocols for Authentication and Key Distribution," IEEE/ACM Transactions on Networking, Vol. 3, No.1, pages 31-41, IEEE Press, Piscataway, NJ, Feb. 1995.	
		Brenno de Winter (Fischer v. Mollard); "Gnu Privacy Guard (GnuPG) Mini Howto"; retrieved from the Internet: http://www.gnupg.org/documentation/howtos.en.html , version 0.1.4; August 10, 2004 (14 pages)	
		Carl Meyer and S.M. Matyas, CRYPTOGRAPHY: A NEW DIMENSION IN COMPUTER DATA SECURITY (1982).	
		Cheng, P. et al., Modular Key Management Protocol (MKMP), November 28, 1994.	
		Damgard; "A Design Principle for Hash Functions"; Advances in Cryptology: Proceedings of CRYPTO '89, vol. 435 of Lecture Notes in Computer Science; pp. 416-427; Springer-Verlag, New York (12 pages).	
		Decker et al.; "The SumoDacs-project: Secure Mobile Data Access with a Tamperproof Hardware Token"; eChallenges e-2010 Conference Proceedings, IIMC; 2010 (8 pages).	
		Ehrtam, W.F. et al., A Cryptographic Key Management Scheme for Implementing the Data Encryption Standard, IBM Sys. J., Vol. 17 No.2, 1978.	
		Freier, A. et al., "SSL Version 3.0," Netscape Communications Corporation, December 1995.	
		Gong, L., "Using One-Way Functions for Authentication," ACM Sigcom Computer Communication Review, Vol. 19, Issue 5, pages 8-11, New York, 1989.	
		Gunson et al.; "User Perceptions of Security and Usability of Single-Factor and Two-Factor Authentication in Automated Telephone Banking"; Computers & Security (2011), vol. 30, no. 4; pp. 208-220 (13 pages).	
		Hans Dobbertin, "The Status of MD5 After a Recent Attack", RSA Laboratories; CryptoBytes, 1996.	
		Hans Dobbertin, Cryptanalysis of MD5 Compress, May 2, 1996.	

EXAMINER SIGNATURE**DATE CONSIDERED**

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached. 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 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, 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 (1-800-786-9199) and select option 2.

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

Substitute for form 1449/PTO				<i>Complete if Known</i>	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Application Number	
				Filing Date	
				First Named Inventor Guy Fielder	
				Art Unit	
				Examiner Name	
Sheet	6	of	9	Attorney Docket No: 5101-0005-C3	

		International Preliminary Report on Patentability and The Written Opinion issued in PCT/US2010/028562; Dated: October 6, 2011; (22 pages).	
		International Preliminary Report on Patentability and The Written Opinion issued in PCT/US2010/028565 Dated: October 6, 2011; (23 pages).	
		International Preliminary Report on Patentability and The Written Opinion issued in PCT/US2010/028566; Dated: October 6, 2011; (14 pages).	
		International Preliminary Report on Patentability and The Written Opinion issued in PCT/US2010/028582; Dated: October 6, 2011 (8 pages).	
		International Preliminary Report on Patentability and The Written Opinion issued in PCT/US2010/028583; Dated: October 6, 2011; (9 pages).	
		International Search Report and The Written Opinion issued in PCT/US2010/028562; Dated: September 29, 2010; (31 pages).	
		International Search Report and The Written Opinion issued in PCT/US2010/028565; Dated: October 6, 2010; (31 pages).	
		International Search Report and The Written Opinion issued in PCT/US2010/028566; Dated: December 30, 2010; (17 pages).	
		International Search Report and The Written Opinion issued in PCT/US2010/028582; Dated: July 30, 2010; (21 pages).	
		International Search Report and The Written Opinion issued in PCT/US2010/028583; Dated: July 6, 2010; (21 pages).	
		Javinen et al.; "Embedded SFE: Offloading Server and Network Using Hardware Tokens"; Financial Cryptography and Data Security Proceeding, 14th International Conference, FC 2010; Tenerife, Canary Islands, January 25-28, 2010 (15 pages).	
		Kaya (2003). Secure multicast groups on ad hoc networks. SASN '03 Proceedings of the 1st ACM Workshop on Security of ad hoc and sensor networks, pages 94-102.	
		Kelsey, John et al., "Passphrase FAQ," alt.security.pgp, October 1993.	
		Krawczyk, H., "SKEME: A Versatile Secure Key Exchange Mechanism for Internet," Proceedings of the 1996 Symposium on Network and Distributed System Security (SNDSS) '96, pages 114-127, IEEE Computer Society, Washington, DC (1996).	

EXAMINER SIGNATURE

DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached. 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 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, 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 (1-800-786-9199) and select option 2.

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

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Complete if Known</i>	
				Application Number	
				Filing Date	
				First Named Inventor	Guy Fielder
				Art Unit	
				Examiner Name	
Sheet	7	of	9	Attorney Docket No: 5101-0005-C3	

	Leighton, T., "Secret Key Agreement without Public-Key Cryptography," Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology, Santa Barbara, CA, pages 456-479, Springer-Verlag, New York, 1998.	
	Lin et al.; "A Practical Electronic Payment System for Message Delivery Service in the Mobile Environment"; Wireless Personal Communications, vol. 42, no. 2; pp. 247-261; July 2007 (15 pages).	
	Matyas, S.M. & Meyer, C.H., "Generation, Distribution, and Installation of Cryptographic Keys," 17 IBM Sys. J. 2 (1978).	
	Menezes, Alfred J. et al., HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC Press, October 16, 1996.	
	Merkle, R., "One Way Hash functions and DES," In In G. Brassard, editor, Advances in Cryptology: Proceedings of CRYPTO'89, vol. 435 of Lecture Notes in Computer Science, pages 428-446, Springer-Verlag, New York, 1990.	
	Molva, Reflik et al., "KryptoKnight Authentication and Key Distribution System," Computer Security-ESORICS 92 (Nov. 23-25, 1992).	
	Preneel, B., "MDx-MAC and Building Fast MAGs from Hash Functions," Lecture Notes in Computer Science; Vol. 963, Proceedings of the 15th Annual International Cryptology Conference on Advances in Cryptology, pages 1-14, Springer-Verlag, London, UK (1995).	
	Rivest, R., "The MD5 Message-Digest Algorithm," IETF RFC 1321, April 1992.	
	RSA Laboratories, "PKCS #5: Password-Based Encryption Standard," version 1.5, November 1993.	
	RSA Laboratories, PKCS #5 v2.0: Password-Based Cryptography Standard, March 25, 1999.	
	Schneider, B., "Security Pitfalls in Cryptography", Counterpane Systems, www.counterpane.com/publish.html , 1998, (11 pages).	
	Schneier, B., "Cryptographic Design Vulnerabilities", Counterpane Systems, www.counterpane.com/publish.html , September 1998, (5 pages).	
	Schneier, Bruce, APPLIED CRYPTOGRAPHY, Katherine Schowalter, 1996 (and first edition (1994) of same).	

EXAMINER SIGNATURE**DATE CONSIDERED**

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached. 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 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, 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 (1-800-786-9199) and select option 2.

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

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Complete if Known</i>	
				Application Number	
				Filing Date	
				First Named Inventor Guy Fielder	
				Art Unit	
				Examiner Name	
Sheet	8	of	9	Attorney Docket No: 5101-0005-C3	

		Schneier. B . "Why Cryptography is Harder Than it Looks". Counterpane Systems, www.counterpane.com/publish.html , 1997, (8 pages).	
		Sun et al.; "A New Design of Wearable Token System for Mobile Device Security"; IEEE Transactions on Consumer Electronics, vol. 54, no. 4; pp. 1784-1789; November 2008 (6 pages).	
		U.S. Department of Commerce, National Institute of Standards and Technology, "Secure Hash Standard", FIPS PUB 180-1, April 17, 1995. (24 pages).	
		Windows '95 Vulnerabilities, US Department of Energy, Computer Incident Advisory Committee, available at http://ftp.cerias.purdue.edu/pub/lists/academic-firewalls/academic-firewalls.951224 (1995).	
		Yuill, J., Denning, D., Feer, F.; "Using Deception to Hide Things from Hackers: Processes, Principles, and Techniques", Journal of Information Warfare, (16 pages).	

EXAMINER SIGNATURE

DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached. 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 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, 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 (1-800-786-9199) and select option 2.

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th colspan="2" style="text-align: right; font-size: small;">Complete if Known</th> </tr> <tr> <td style="width: 60%;">Application Number</td> <td></td> </tr> <tr> <td>Filing Date</td> <td></td> </tr> <tr> <td>First Named Inventor</td> <td>Guy Fielder</td> </tr> <tr> <td>Art Unit</td> <td></td> </tr> <tr> <td>Examiner Name</td> <td></td> </tr> </table>	Complete if Known		Application Number		Filing Date		First Named Inventor	Guy Fielder	Art Unit		Examiner Name	
Complete if Known													
Application Number													
Filing Date													
First Named Inventor	Guy Fielder												
Art Unit													
Examiner Name													
Sheet 9 of 9	Attorney Docket No: 5101-0005-C3												

CERTIFICATION STATEMENT								
Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s): ☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1). OR ☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2). ☒ See attached certification statement. ☐ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith. ☐ None								
SIGNATURE								
A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature. <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 10px;"> <tr> <td style="width: 30%;">Signature</td> <td style="width: 30%;">/Tarek N. Fahmi/</td> <td style="width: 20%;">Date (YYYY-MM-DD)</td> <td style="width: 20%;">2016-06-28</td> </tr> <tr> <td>Name/Print</td> <td>Tarek N. Fahmi</td> <td>Registration Number</td> <td>41402</td> </tr> </table>	Signature	/Tarek N. Fahmi/	Date (YYYY-MM-DD)	2016-06-28	Name/Print	Tarek N. Fahmi	Registration Number	41402
Signature	/Tarek N. Fahmi/	Date (YYYY-MM-DD)	2016-06-28					
Name/Print	Tarek N. Fahmi	Registration Number	41402					
This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.								

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Inventor: Guy Fielder

Application No.: Not yet assigned

Filed: Herewith

Examiner: Not Yet Assigned

Art Unit: Not Yet Assigned

Docket No.: 5101-0005-C3

Customer No.: 27571

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

INFORMATION DISCLOSURE STATEMENT UNDER 37 C.F.R. §1.97

In accordance with the duty of disclosure, enclosed is a copy of IDS Citation Form PTO/SB/08, together with copies of the documents cited on that form, except for copies not required to be submitted (e.g. copies of U.S. patents and U.S. published patent applications that need not be included and copies of Non Patent Literature documents that were previously provided in parent application Nos. 14/861,630 filed 09-22-2015 and 13/203,327 filed 08-25-2011). This IDS and IDS Citation Form are being submitted before the mailing of a First Office Action. It is respectfully requested that the cited references be considered and that the enclosed copy of PTO/SB/08 be initialed by the Examiner to indicate such consideration and a copy thereof returned to applicant(s).

The submission of this Information Disclosure Statement is not to be construed as a representation that a search has been made in the subject application and is not to be construed as an admission that the information cited in this statement is material to patentability.

Please charge any fees due to Deposit Account No. 50-5798.

Respectfully submitted,

Date: June 28, 2016

/Tarek N. Fahmi/
Tarek N. Fahmi
Reg. No. 41,402

ASCENDA LAW GROUP, PC
333 W. San Carlos St., Suite 200
San Jose, CA 95110-2730
(866) 877-4883

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

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	SYSTEM AND METHOD FOR PROTECTING SECRETS FILE
---------------------------	---

As the below named inventor, I hereby declare that:

This declaration ☒ The attached application, or
is directed to: ☐ United States application or PCT international application number _____
filed on _____

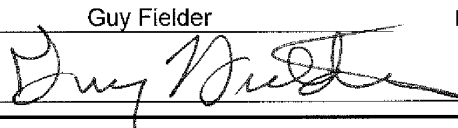
The above-identified application was made or authorized to be made by me.

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

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR	
Inventor: _____	Guy Fielder
Date (Optional): <u>Mar 26, 2014</u>	
Signature: _____	

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

22511

PATENT TRADEMARK OFFICE

Electronic Patent Application Fee Transmittal				
Application Number:				
Filing Date:				
Title of Invention:		SYSTEM AND METHOD FOR AUTHENTICATING USERS		
First Named Inventor/Applicant Name:		Guy Fielder		
Filer:		Tarek N. Fahmi/Sarah Zizzo		
Attorney Docket Number:		5101-0005-C3		
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	70	70
Utility Search Fee	2111	1	300	300
Utility Examination Fee	2311	1	360	360
Pages:				
Claims:				
Claims in excess of 20	2202	2	40	80
Miscellaneous-Filing:				
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				810

Electronic Acknowledgement Receipt	
EFS ID:	26201428
Application Number:	15195606
International Application Number:	
Confirmation Number:	8706
Title of Invention:	SYSTEM AND METHOD FOR AUTHENTICATING USERS
First Named Inventor/Applicant Name:	Guy Fielder
Customer Number:	27571
Filer:	Tarek N. Fahmi/Sarah Zizzo
Filer Authorized By:	Tarek N. Fahmi
Attorney Docket Number:	5101-0005-C3
Receipt Date:	28-JUN-2016
Filing Date:	
Time Stamp:	17:29:45
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$810
RAM confirmation Number	4750
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	5101-0005-C3_ADS.pdf	1823498	no	9
			9048a36fa10ac290acc463c4b7e0a1dd4cb9c7f8		
Warnings:					
Information:					
2		5101-0005-C3_Specification.pdf	319781	yes	53
			a120e22015e2a3d332771aae0458653477014192		
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Specification		1	48	
	Claims		49	52	
	Abstract		53	53	
Warnings:					
Information:					
3	Drawings-only black and white line drawings	5101-0005-C3_Figures.pdf	389846	no	14
			f2de5c6a34bc1ff514fdbd448ed162abfc8b3858		
Warnings:					
Information:					
4	Information Disclosure Statement (IDS) Form (SB08)	5101-0005-C3_IDS.pdf	291150	no	9
			bc1307ceed65632a3ad26bffa89988304fc2972f		
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					

5	Transmittal Letter	5101-0005-C3_IDS_Statement.pdf	73843	no	2
			545f960483c4daebe5b09eca6738deca64a8824a		
Warnings:					
Information:					
6	Oath or Declaration filed	5101-0005-C3_Declaration.pdf	51819	no	1
			35dfc789539947343b0052b6e3589acc44ffbcf		
Warnings:					
Information:					
7	Fee Worksheet (SB06)	fee-info.pdf	36797	no	2
			a293e104cbbc6925b790807198ff9150b0143627		
Warnings:					
Information:					
Total Files Size (in bytes):			2986734		
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.					

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	5101-0005-C3
		Application Number	
Title of Invention	SYSTEM AND METHOD FOR AUTHENTICATING USERS		
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	
	Guy		Fielder		
Residence Information (Select One) • US Residency Non US Residency Active US Military Service					
City	Austin	State/Province	TX	Country of Residence	US
Mailing Address of Inventor:					
Address 1	2616 Maria Anna Rd., Suite 500				
Address 2					
City	Austin	State/Province	TX		
Postal Code	78703-1656	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	27571		
Email Address	patents@ascendallaw.com	Add Email	Remove Email

Application Information:

Title of the Invention	SYSTEM AND METHOD FOR AUTHENTICATING USERS		
Attorney Docket Number	5101-0005-C3	Small Entity Status Claimed	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	14	Suggested Figure for Publication (if any)	

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	5101-0005-C3
		Application Number	
Title of Invention	SYSTEM AND METHOD FOR AUTHENTICATING USERS		

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	27571		

Domestic Benefit/National Stage Information:

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

When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status	Pending	Remove	
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Continuation of	14861630	2015-09-22

Application Data Sheet 37 CFR 1.76		Attorney Docket Number		5101-0005-C3	
		Application Number			
Title of Invention	SYSTEM AND METHOD FOR AUTHENTICATING USERS				

Prior Application Status		Patented		Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14861630	Continuation of	14228463	2014-03-28	9165153	2015-10-20
Prior Application Status		Patented		Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14228463	Continuation of	13203327	2011-08-25	8726032	2014-05-13
Prior Application Status		Expired		Remove	
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)		
13203327	a 371 of international	PCT/US10/28562	2010-03-25		
Prior Application Status		Expired		Remove	
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)		
PCT/US10/28562	Claims benefit of provisional	61163406	2009-03-25		
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the Add button.					

Foreign Priority Information:

This section allows for the applicant to claim 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).

			Remove
Application Number	Country ⁱ	Filing Date (YYYY-MM-DD)	Access Code ⁱ (if applicable)
Additional Foreign Priority Data may be generated within this form by selecting the Add button.			

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

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	5101-0005-C3
		Application Number	
Title of Invention	SYSTEM AND METHOD FOR AUTHENTICATING USERS		

☐ 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.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	5101-0005-C3
		Application Number	
Title of Invention	SYSTEM AND METHOD FOR AUTHENTICATING USERS		

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.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	5101-0005-C3
		Application Number	
Title of Invention	SYSTEM AND METHOD FOR AUTHENTICATING USERS		

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	PACID TECHNOLOGIES, LLC		
Mailing Address Information For Applicant:			
Address 1	2616 Maria Anna Rd.		
Address 2	Suite 500		
City	Austin	State/Province	TX
Country	US	Postal Code	78703-1656
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.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	5101-0005-C3
		Application Number	
Title of Invention	SYSTEM AND METHOD FOR AUTHENTICATING USERS		

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

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	/Tarek N. Fahmi/		Date (YYYY-MM-DD)	2016-06-28
First Name	Tarek	Last Name	Fahmi	Registration Number
				41402
Additional Signature may be generated within this form by selecting the Add button.				Add

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

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	5101-0005-C3
		Application Number	
Title of Invention	SYSTEM AND METHOD FOR AUTHENTICATING USERS		

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

Privacy Act Statement

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

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

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

SYSTEM AND METHOD FOR AUTHENTICATING USERS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This is a CONTINUATION of and claims priority to U.S. Patent Application No. 14/861,630, filed September 22, 2015, which is a CONTINUATION of U.S. Patent Application No. 14/228,463, filed March 28, 2014, which is a CONTINUATION of U.S. Patent Application No. 13/203,327, filed August 25, 2011, which is a 371 national stage filing of International Application PCT/US10/28562, filed March 25, 2010, which claims priority to U.S. Provisional Application No. 61/163,406, filed March 25, 2009, each of which is incorporated herein by reference.

BACKGROUND

[0002] The computer system assists in managing (*e.g.*, storing, organizing, and communicating) a large amount of information. Some of the information managed by a computer system is confidential. In other words, access to such information is intended to be limited. Traditional protection schemes attempt to prevent unauthorized users from accessing the confidential information by requiring that a user provide authentication credential(s), for example a username and password, at a predefined entry point, to access an account that includes the confidential information. Protecting only the predefined entry points, however, fails to account for nefarious individuals creating other entry points by exploiting computer system vulnerabilities. For example, knowledge of a user's hardware and software system, system configuration, types of network connections, etc. may be used to create an entry point and gain access to the confidential information.

[0003] In order to prevent unauthorized access to the confidential information, the confidential information may be encrypted. Encryption is a process of transforming the clear text confidential information into an encrypted format that is unreadable by anyone or anything that does not possess a corresponding decryption key. An encryption algorithm and an encryption key are used to

perform the transformation. Encryption technology is classified into two primary technology types: symmetric encryption technology and asymmetric encryption technology. Symmetric encryption technology uses the same encryption key to both encrypt and decrypt confidential information. Asymmetric encryption technology uses a pair of corresponding encryption keys: this key pair share a relationship such that data encrypted using one encryption key can only be decrypted using the other encryption key of the pair.

BRIEF DESCRIPTION OF DRAWINGS

- [0004]** Fig. 1 shows a schematic diagram of a system in accordance with one or more embodiments of the invention.
- [0005]** Figs. 2A-5B show flowcharts in accordance with one or more embodiments of the invention.
- [0006]** Figs. 6A-7E show examples in accordance with one or more embodiments of the invention.
- [0007]** Fig. 8 shows a computing device in accordance with one or more embodiments of the invention.

DETAILED DESCRIPTION

- [0008]** In general, in one aspect, the invention relates to a method for protecting a first secrets file. The method includes an n-bit generator generating a secrets file name for the secrets file and generating a decoy file names for decoy files. The secrets file includes a secret. Each of the decoy files includes decoy file contents, are a same size as the secrets file, and is associated with a modification time within a range of modification times. The modification time of the secrets file is within the range of modification times. The secrets file and decoy files are stored in a secrets directory.

[0009] In general, in one aspect, the invention relates to a method for encrypting communication. The method includes receiving a request to communicate with a group, obtaining a group agreed connect name corresponding to the group, obtaining a username and password of a user of a member connecting to the group, and generating a first message digest using the group agreed connect name, the username, the password, and an n-bit generator. The method further includes extracting a secrets file name from the first message digest, obtaining an encrypted secrets file from a secrets directory, decrypting the encrypted secrets file to obtain a secrets file using a secrets file encryption key obtained from the first message digest, generating a second message digest using the n-bit generator and a first secret and a second secret from the secrets file, and encrypting communication between the member and the group using an encryption key obtained, at least in part, from the second message digest.

[0010] In general, in one aspect, the invention relates to a computing device for protecting a secrets file that includes a processor, a memory, and software instructions stored in memory. The software instructions cause the computing device to generate a secrets file name for the secrets file and generating a decoy file names for decoy files. The secrets file includes a secret. Each of the decoy files includes decoy file contents, are a same size as the secrets file, and is associated with a modification time within a range of modification times. The modification time of the secrets file is within the range of modification times. The secrets file and decoy files are stored in a secrets directory.

[0011] In general, in one aspect, the invention relates to a computing device for protecting a secrets file that includes a processor, a memory, and software instructions stored in memory. The software instructions cause the computing device to receive a request to communicate with a group, obtain a group agreed connect name corresponding to the group, obtain a username and password of a user of a member connecting to the group, and generate a first message digest using the group agreed connect name, the username, the password, and an n-bit

generator. The software instructions further cause the computing device to extract a secrets file name from the first message digest, obtain an encrypted secrets file from a secrets directory, decrypt the encrypted secrets file to obtain a secrets file using a secrets file encryption key obtained from the first message digest, generate a second message digest using the n-bit generator and a first secret and a second secret from the secrets file, and encrypt communication between the member and the group using an encryption key obtained, at least in part, from the second message digest.

[0012] In general, in one aspect, the invention relates to a computer readable medium comprising computer readable program code embodied therein for causing a computer system to perform a method for protecting a first secrets file. The method includes an n-bit generator generating a secrets file name for the secrets file and generating a decoy file names for decoy files. The secrets file includes a secret. Each of the decoy files includes decoy file contents, are a same size as the secrets file, and is associated with a modification time within a range of modification times. The modification time of the secrets file is within the range of modification times. The secrets file and decoy files are stored in a secrets directory.

[0013] In general, in one aspect, the invention relates to a computer readable medium comprising computer readable program code embodied therein for causing a computer system to perform a method for protecting a first secrets file. The method includes receiving a request to communicate with a group, obtaining a group agreed connect name corresponding to the group, obtaining a username and password of a user of a member connecting to the group, and generating a first message digest using the group agreed connect name, the username, the password, and an n-bit generator. The method further includes extracting a secrets file name from the first message digest, obtaining an encrypted secrets file from a secrets directory, decrypting the encrypted secrets file to obtain a secrets file using a secrets file encryption key obtained from the first message digest, generating a second message digest using the n-bit

generator and a first secret and a second secret from the secrets file, and encrypting communication between the member and the group using an encryption key obtained, at least in part, from the second message digest.

[0014] Specific embodiments of the invention will now be described in detail with reference to the accompanying figures. Like elements in the various figures are denoted by like reference numerals for consistency.

[0015] In the following detailed description of embodiments of the invention, numerous specific details are set forth in order to provide a more thorough understanding of the invention. However, it will be apparent to one of ordinary skill in the art that the invention may be practiced without these specific details. In other instances, well-known features have not been described in detail to avoid unnecessarily complicating the description.

[0016] In general, embodiments of the invention relate to securing communication between members of a group, where each member is a computing device. In one or more embodiments of the invention, the group is two or more members that share (or intend to share) confidential information. The confidential information may be transmitted as communication (or portion thereof). Examples of communications include, but are not limited to, short messaging service (SMS) messages, electronic mail (e-mail), chat messages, audio messages, graphics, audio-visual messages (*e.g.*, video file, streaming video, etc.). As used herein, a communication is encrypted when at least a portion of the communication is encrypted.

[0017] In one embodiment of the invention, a computing device is any physical or virtual device that may be used to perform embodiments of the invention. The physical device may correspond to any physical system with functionality to implement one or more embodiments of the invention. For example, the physical device may be implemented on a general purpose computing device (*i.e.*, a device with a processor(s) and an operating system) such as, but not

limited to, a desktop computer, a laptop computer, a gaming console, a mobile device (*e.g.*, smart phone, a personal digital assistant, gaming device).

[0018] Alternatively, the physical device may be a special purpose computing device that includes an application-specific processor(s)/hardware configured to only execute embodiments of the invention. In such cases, the physical device may implement embodiments of the invention in hardware as a family of circuits and limited functionality to receive input and generate output in accordance with various embodiments of the invention. In addition, such computing devices may use a state-machine to implement various embodiments of the invention.

[0019] In another embodiment of the invention, the physical device may correspond to a computing device that include both a general purposes processor(s) and an application-specific processor(s)/hardware. In such cases, one or more portions of the invention may be implemented using the operating system and general purpose processor(s) and one or more portions of the invention may be implemented using the application-specific processor(s)/hardware.

[0020] The virtual device may correspond to a virtual machine. Broadly speaking, the virtual machines are distinct operating environments configured to inherit underlying functionality of the host operating system (and access to the underlying host hardware) via an abstraction layer. In one or more embodiments of the invention, a virtual machine includes a separate instance of an operating system, which is distinct from the host operating system. For example, one or more embodiments of the invention may be implemented on VMware® architectures involving: (i) one or more virtual machines executing on a host computer system such that each virtual machine serves as host to an instance of a guest operating system; and (ii) a hypervisor layer serving to facilitate intra-host communication between the one or more virtual machines and host computer system hardware. Alternatively, one or more embodiments of the invention may be implemented on Xen® architectures involving: (i) a

control host operating system (*e.g.*, Dom 0) including a hypervisor; and (ii) one or more VMs (*e.g.*, Dom U) executing guest operating system instances. The invention is not limited to the aforementioned exemplary architectures. VMware® is a registered trademark of VMware, Inc. Xen® is a trademark overseen by the Xen Project Advisory Board.

[0021] Each of the members may be used by, for example, an individual, a business entity, a family, any other entity, or any combination thereof. For example, a group may have members John Smith's computing device and Jane Doe's computing device. As another example, a group may have members John Smith's smart phone, John Smith's personal computer, and John Smith's gaming console. As another example, a group may have members John Smith's computing device, Jane Smith's computing device, and the servers of the Smith's financial advisors. Other possible groups may exist without departing from the scope of the invention.

[0022] In one or more embodiments of the invention, each member creates a secrets file that has secret(s). The name of the secrets file and the secret is generated by an n-bit generator. The secret(s) is used to secure communications between the members of the group. The n-bit generator also generates decoy file names and decoy file contents for decoy files. The decoy files and the secrets file are stored together in the same secrets directory. Thus, the secrets file is indistinguishable from the decoy files. Whenever the secrets file is updated, each of the decoy files are also updated such that the secrets file remains indistinguishable from the decoy files.

[0023] Fig. 1 shows a schematic diagram of a system in accordance with one or more embodiments of the invention. As shown in Fig. 1, the system includes a security application (102) and a security directory (104). Both of these components are discussed below.

[0024] In one or more embodiments of the invention, each member includes a security application (102). The security application (102) on each member may

be instances of the same application, different versions of the same application, or different applications. Further, the security application may correspond to a complete program product or a programming module of another application. For example, the security application may be a part of and provide security for banking and/or commerce applications. In one or more embodiments of the invention, the security application (102) includes an n-bit generator (106), an encryption module (108), and a user interface (110). Each of the components of the security application (102) may be implemented in hardware, software, firmware, or a combination thereof. The components of the security application are discussed below.

[0025] In one or more embodiments of the invention, an n-bit generator (106) includes functionality to receive and process one or more inputs to generate a message digest. A message digest is a string of characters, which may be represented as a bit-string, in accordance with one or more embodiments of the invention. In one or more embodiments of the invention, the message digest is a bit string. Further, the n-bit generator includes functionality to generate a deterministic and repeatable message digest, which appears pseudo-random or random, in accordance with one or more embodiments of the invention. A pseudo-random output (*e.g.*, message digest) is output that is repeatable and predictable but appears random. Specifically, in one or more embodiments of the invention, although the message digest is repeatable and calculable when the inputs and the operations performed by the n-bit generator (106) are known, the message digest appears random. The apparent randomness may be with respect to someone who knows or does not know the inputs in accordance with one or more embodiments of the invention. Alternatively, or additionally, the apparent randomness may be with respect to someone who does not know the operations performed by the n-bit generator in accordance with one or more embodiments of the invention. In one or more embodiments of the invention, the message digest is deterministic in that a single output exists for a given set of inputs. Moreover, the message digest may be a fixed length. In other

words, regardless of the input length, the same n-bit generator (106) may produce a message digest with a fixed length.

[0026] The number of bits in the input to the n-bit generator may be different or the same as the number of bits in the output produced by the n-bit generator. For example, if the n-bit generator accepts n number of bits for input and produces m number of bits for output, m may be less than, equal to, or greater than n. Multiple iterations of the n-bit generator may be performed to construct an ever-increasing m-bit result that includes multiple message digests.

[0027] Further, the n-bit generator (106) includes functionality to generate a deterministic message digest. Specifically, the n-bit generator (106) has the following two properties. First, the n-bit generator (106) generates the same message digest when provided with the same input(s). Second, the n-bit generator generates, with a high probability, a different message digest when provided with different input(s). For example, a single bit change in the input may result in a significant change of the bits in the resulting message digest. In the example, the change may be fifty percent of the bits depending on the type of n-bit generator used. However, a greater percentage or less percentage of bits may change without departing from the scope of the invention.

[0028] The n-bit generator (106) may include multiple sub-routines, such as a bit shuffler (not shown) and a hash function (not shown). In one or more embodiments of the invention, the bit shuffler includes functionality to combine multiple inputs into a single output. Specifically, the bit shuffler applies a function to the bit level representation of inputs to generate a resulting set of output bits. The output of the bit shuffler may appear as a shuffling of bits in each of inputs and may or may not have the same ratio of 1's to 0's as the input. In one or more embodiments of the invention, the bit shuffling by the bit shuffler has a commutative property. In other words, the order that inputs are provided to the bit shuffler does not affect the output. For example, consider the scenario in which the inputs are input X, input Y, and input Z. Bit

shuffling on input X, input Y, and input Z produces the same output as bit shuffling on input Y, input Z, and input X.

[0029] In one embodiment of the invention, the bit shuffler may correspond to any function or series of functions for combining inputs. For example, the bit shuffler may correspond to the XOR function, the multiplication function, an addition function, or another function that may be used to combine inputs. As another example, the security application with the bit shuffler may correspond to a function that orders the inputs and then uses a non-commutative function to generate an output. The bit shuffler may correspond to other mechanisms for combining multiple inputs without departing from the scope of the invention.

[0030] In one or more embodiments of the invention, a hash function is a function that includes functionality to receive an input and produce a pseudo-random output. In one or more embodiments of the invention, the hash function may include functionality to convert a variable length input into a fixed length output. For example, the hash function may correspond to GOST, HAVAL, MD2, MD4, MD5, PANAMA, SNEERU, a member of the RIPEMD family of hash functions, a member of the SHA family of hash functions, Tiger, Whirlpool, S-Box, P-Box, any other hash function, or combination thereof.

[0031] Although the above description discusses the use of the bit shuffler prior to the hash function, in one or more embodiments of the invention, the hash function operations may be performed prior to the bit shuffler operations. For example, the hash function may be performed separately on each of the inputs to create hashed inputs. The hashed inputs may then be combined by the bit shuffler. Alternatively, the bit shuffler may be first performed on the inputs to create a single intermediate result before the intermediate result is provided to the hash function. The intermediate result may be stored to be used later to create subsequent message digests.

[0032] Further, in one or more embodiments of the invention, the n-bit generator includes a random character generator, such as a random number generator. The random character generator includes functionality to generate a random string of characters of a specified length. The n-bit generator may use the random character generator, for example, to generate the decoy file names (*e.g.*, 134A, 134X) and/or the decoy data (*e.g.*, 132A, 132X).

[0033] The n-bit generator (106) is operatively connected to an encryption module (108) in accordance with one or more embodiments of the invention. An encryption module (108) includes functionality to manage the encryption and decryption of information for the computing device. Specifically, the encryption module (108) includes functionality to request generation of a secrets file (112) (discussed below) and decoy files (*e.g.*, 114A, 114X) (discussed below). The encryption module (108) may further include functionality to update files in the security directory (104) (discussed below) so that all files in the secrets directory (104) appear indistinguishable from each other.

[0034] For example, the encryption module may include functionality to receive information, request one or more message digests from the n-bit generator (106), extract an encryption key from the one or more message digests, and/or encrypt the information using the encryption key. Alternatively, or additionally, the encryption module (108) may include functionality to receive encrypted information, request one or more message digests from the n-bit generator (106), extract an encryption key from the one or more message digests, and/or decrypt the encrypted information using the encryption key.

[0035] In one or more embodiments of the invention, the encryption module (108) is identically configured across all members of a group to request the same number of message digests. The configuration may be based, for example, on the type of communication, the encryption algorithm, and/or the type of data to be extracted from the message digest.

[0036] The encryption module (108) implements one or more encryption algorithms. In one or more embodiments of the invention, the encryption algorithm includes functionality to transform information in a clear text format into an encrypted format that is unreadable by anyone or anything that does not possess a corresponding encryption key. For example, the encryption algorithm may correspond to Data Encryption Algorithm (DEA) specified in the Data Encryption Standard (DES), Triple DES, Advanced Encryption Standard (AES), FEAL, SKIPJACK, any other encryption algorithm, or any combination thereof. In one or more embodiments of the invention, the encryption module implements only symmetric encryption algorithm(s).

[0037] Although not shown in Fig. 1, the encryption module (108) may also include or be operatively connected to an algorithm selector table (not shown). An algorithm selector table is a logical association between encryption algorithms and an algorithm identifier. The algorithm identifier may be, for example, a numeric, binary, or another such value. In one or more embodiments of the invention, all algorithm identifiers in a range are present. For example, the algorithm identifier may be a range of integers (e.g., 0...15), a sequence of binary values (e.g., 000, 001, 010,...111). Further, the same encryption algorithm may be associated with multiple algorithm identifiers in the table. For example, "0" may correspond to AES, "1" may correspond to Triple DES, "2" may correspond FEAL, and "3" may correspond to Triple DES. The use of the term, "table", is only to denote a logical representation, various data structures may be used to implement the algorithm selector table without departing from the scope of the invention.

[0038] Further, in one or more embodiments of the invention, the association between the encryption algorithm identifiers and the encryption algorithms is not based on a pre-defined ordering of encryption algorithms. Specifically, the association may be randomly defined.

[0039] The use of the term, "table", is only to denote a logical representation, various implementations of the algorithm selector table may be used without

departing from the scope of the invention. For example, the algorithm selector table may be implemented in computer instructions using a series of conditional statements. Specifically, when a conditional statement is satisfied, the code corresponding to the implementation of the encryption algorithm is executed. By way of another example, the algorithm selector table may be implemented as a data structure that associates the consecutive encryption algorithm identifiers with identifiers used by the security application for each of the encryption algorithms. The above are only a few examples of possible implementations for the algorithm selector table and not intended to limit the scope of the invention.

[0040] Further, all members associate the same encryption algorithm identifiers with the same corresponding encryption algorithms. For example, if one member associates “0” with AES, “1” with Triple DES, “2” with FEAL, and “3” with Triple DES, then the remaining members associates “0” with AES, “1” with Triple DES, “2” with FEAL, and “3” with Triple DES. Further, all members may or may not use the same implementation of the algorithm selector table.

[0041] In one or more embodiments of the invention, the algorithm selector table includes separate entries for each encryption algorithm and key length pair. In one or more embodiments of the invention, the encryption module may identify the encryption algorithm from the algorithm selector table and use the key length associated with the encryption algorithm to extract the appropriate number of bits for the encryption key. For example, an entry may exist for Blowfish with an encryption key length 256 bits and a separate entry may exist for Blowfish with an encryption key length of 384 bits. In the example, if the first entry is specified in the algorithm selector bits of the message digest (discussed below), then 256 bits are extracted from the message digest(s) for the encryption key. Alternatively, in the example, if the second entry is specified, then 384 bits are extracted from the message digest for the encryption key.

[0042] Further, each entry in the algorithm selector table may include a starting bit value. The starting bit value may be used to identify a first secret to use in the secrets repository or a starting bit for the encryption key in the message digest.

[0043] Alternatively, although not shown in Fig. 1, the system may include a key length table. The key length table may specify an identifier with a corresponding encryption key length. Similar to the algorithm selector table, multiple different possible implementations of the key length table may be used without departing from the scope of the invention. Further, all members of the group have the associations between key length identifiers and key lengths, but may not have the same implementation of key length table. For example, “1” may be associated with “256 bits”, 2 may be associated with “128 bits”, etc.

[0044] In one or more embodiment of the invention, when a key length table is used, the algorithm selector table may be used to specify the encryption algorithm, and the key length table may be used to specify the number of bits in the encryption key. Specifically, a key length field (discussed below) in the message digest may index the corresponding entry in the key length table. In one or more embodiments of the invention, if the specified encryption algorithm does not allow for variable key length, then the key length field in the message digest is ignored.

[0045] Continuing with the security application (102), in one or more embodiments of the invention, the user interface (110) includes functionality to communicate with a user of the computing device. For example, the user interface (110) may include functionality to guide a user through configuring the security application to communicate with one or more groups of which the computing device is a member. Further, the user interface (110) may include functionality to inform a user when another member of a group is requesting communication and provide the user with the option of allowing the communication with the user’s computing device. The user interface (110) may include hardware and/or software components, such as information boxes,

menu buttons, drop down boxes, input boxes, hardware lights, hardware buttons, and/or other user interface components.

[0046] Although not shown in Fig. 1, the security application may include an application programming interface (API). The security application may be configured to communicate with other applications executing on the same or different computing devices using the API. Thus, for example, the API of member A may include functionality to communicate via the network with member B's security application. As another example, the API may include functionality to receive an encrypted format of a file and provide a clear text format of the file to another application executing on member A. Conversely, the API may include functionality to receive, from another application on member A, a clear text format of a file and provide an encrypted format of the file to another application executing on member A on member B.

[0047] In one or more embodiments of the invention, the security application (102) includes functionality to access and use a security directory (104). A security directory (104) is located within a file system for storage of the secrets file (112) and the decoy files (*e.g.*, 114A, 114X). Alternatively, the file system merely includes an access point for the security directory, which is stored on an external physical storage medium that is accessible via the file system (*e.g.*, the external physical storage medium is mounted to the file system). In one or more embodiments of the invention, the security directory (104) does not include any partitioning (*e.g.*, in the form of subdirectories or subfolders) of the secrets file (112) and the decoy files (*e.g.*, 114A, 114X). Further, in one or more embodiments of the invention, secrets files (112) and decoy files (*e.g.*, 114A, 114X) generated for different groups of users are not partitioned in the security directory (104). Alternatively, the security directory (104) may include a partitioning of files for each group of which the user is a member.

[0048] In one embodiment of the invention, the secrets directory (104) (or portions thereof) is located on an external device that is accessible to the security application. Examples of external devices include, but are not limited

to, a mobile phone, a smart phone, a personal digital assistant, a portable gaming device, a memory device (*e.g.*, any device with non-volatile memory) with a contactless interface (*e.g.*, a BlueTooth Interface), a memory device (*e.g.*, any device with non-volatile memory) with a contact interface (*e.g.*, a Universal Serial Bus (USB) interface), etc.

[0049] Although Fig. 1 shows the security directory (104) as only including the secrets file (112) and the decoy files (*e.g.*, 114A, 114X), the security directory (104) may include other files without departing from the scope of the invention. For example, the security directory (104) may include general files for the member, general files for a computer system (not shown) connected to the member, configuration files for the security application (102), and/or any other files. Further, the other files may or may not be in the same partition in the security directory as the secrets file (112) and the decoy files (*e.g.*, 114A, 114X).

[0050] The secrets file (112) is a file for storing secrets (118). Secrets in the secrets file (112) are shared secrets. Shared secrets (118) correspond to data known only to the members of the group. Specifically, the security application (102) of each member of the group independently generates the secrets (118) using an n-bit generator (106) and the same group agreed seed as inputs to the n-bit generator (106). The group agreed seed may be any password, passphrase, or series of characters agreed upon by members of the group or their corresponding users. For example, the group agreed seed may be “the cow jumped over the moon,” “#8\$#DsaVA(@12w@,” or any other collection of characters (*e.g.*, symbols and/or alphanumeric characters).

[0051] In one or more embodiments of the invention, because each secret is generated by the n-bit generator (106), each secret is pseudo-random. For example, when interpreted in textual-based format, each secret appears as random string of characters (*e.g.*, ASCII symbols or any other character set used to represent characters).

[0052] In one or more embodiments of the invention, each security application generates the same set of secrets (118). Each secret (118) in the secrets file may be associated with a unique secret identifier. The unique secret identifier may be a consecutive integer specifying when the secret was generated. For example, the first generated secret may be associated with the number one, while the second generated may be associated with the number two, etc. The consecutive integer may be explicitly or implicitly associated with the secret. For example, the number one may be stored in the secrets file (112) with the first generated secret. Alternatively, the first generated secret may be in the first position in the secrets file to indirectly associate the first generated secret with the first integer.

[0053] Secrets (118) in the secrets file (112) are each associated with a given group and may be further organized according to type of communication in accordance with one or more embodiments of the invention. For example, secrets used for encryption in a chat session may be different than secrets used for encryption in an email communication. Alternatively or additionally, the secrets may be organized based on the clear text file format of a file to be encrypted. For example, secrets used to encrypt portable document formatted (PDF) files may be different than secrets used to encrypt extensible markup language (XML) files.

[0054] In one or more embodiments of the invention, each shared secret may include a static secret, a dynamic secret, or both a static secret and a dynamic secret. The static secret may remain unchanged throughout the lifetime of the group in accordance with one or more embodiments of the invention. For example, the static secret may be used to recover secure communications by providing a new set of secrets when the members of the group lose synchronization with regards to the dynamic secrets. In contrast, the dynamic secret may periodically change, such as at the end of each communication session or prior to beginning a communication session.

[0055] In one or more embodiments of the invention, a communication session may be a set of related communications (*e.g.*, related short messaging service messages (SMS), related emails, chat messages, or other related communications). Alternatively, or additionally, a communication session may correspond to a set of communications starting at a first time and having a duration of a pre-defined amount of time. The pre-defined amount of time may be defined, for example, according to the amount of time after the last communication is sent and/or received.

[0056] In one or more embodiments of the invention, secrets (118) are protected in the secrets file. The protection of the secrets (118) may be performed by encrypting the file. Specifically, the secrets file (112) may have an encryption key (not shown) associated with the secrets file (112), such that only the encryption module (108) can decrypt the file. Protection may further include making the secrets (118) inaccessible to the member having the secrets directory (104). Specifically, the member (or user of the member) may be unable to identify the secrets (118) or even the secrets file (112). By hiding the secrets (118) even from the member (and the user of the member) having the security application (102) and the security directory (104), the secrets (118) are highly unlikely to be compromised by the member (or the user of the member).

[0057] In addition to secrets (118), the secrets file (112) also include secrets file metadata (116). The secrets file metadata (116) includes information about the secrets file (112). As shown in Fig. 1, the secrets file metadata (116) may include a file name (120), a created timestamp (122), an accessed timestamp (124), a modified timestamp (126), and a file size (128).

[0058] The file name (120) is the unique identifier of the file within the security directory (104). In one or more embodiments of the invention, the file name appears randomly generated. Specifically, the file name (120) is a pseudo-random string of characters (*e.g.*, symbols and/or alphanumeric characters) of a pre-defined length. The file name may be generated by the n-bit generator and may be converted to textual based format.

[0059] The created timestamp (122) specifies when the secrets file (112) was created. If the secrets file (112) is a copy of an original secrets file (112), then the created timestamp specifies when the copy was created. Similarly, the accessed timestamp specifies when the secrets file (112) was last accessed by the user or the program. For example, the accessed timestamp may correspond to the last time in which the secrets file (112) was opened. The modified timestamp (126) specifies when the secrets file (112) was last modified. Specifically, the modified timestamp (126) specifies when a change was saved to the secrets file (112). The file size (128) provides the size of the secrets file (112). Specifically, the file size (128) may specify, for example, the amount of physical storage space required to store the secrets file.

[0060] In addition to the secrets file (112), the security directory (104) also includes decoy files (*e.g.*, 114A, 114X) in accordance with one or more embodiments of the invention. In one or more embodiments of the invention, the decoy files (*e.g.*, 114A, 114X) are indistinguishable from the secrets file (112). Specifically, like the secrets file (112), the decoy files include metadata (*e.g.*, 130A, 130X) [130X was omitted from Fig 1] and data (*e.g.*, 132A, 132X). The decoy file metadata (*e.g.*, 130A, 130X) may include a file name (*e.g.*, 134A, 134X), a created timestamp (*e.g.*, 136A, 136X), accessed timestamp (*e.g.*, 138A, 138X), modified timestamp (*e.g.*, 140A, 140X), and file size (*e.g.*, 142A, 142X).

[0061] In one or more embodiments of the invention, the file name (*e.g.*, 134A, 134X) of the decoy files (*e.g.*, 114A, 114X) are similar to the file name (120) of the secrets file (112). Specifically, like the secrets file name (120), the decoy file name (*e.g.*, 134A, 134X) is a pseudo-random string of characters. Further, the decoy file name (*e.g.*, 134A, 134X) includes only characters that may be present in the secrets file name (120). For example, if the secrets file name (120) includes only alphanumeric characters, then the decoy file names (*e.g.*, 134A, 134X) also only include alphanumeric characters. Thus, the secrets

file name (120) appears indistinguishable from the decoy file name (*e.g.*, 114A, 114X).

[0062] Further, in one or more embodiments of the invention, the created timestamp (*e.g.*, 136A, 136X), the accessed timestamp (*e.g.*, 138A, 138X), the modified timestamp (*e.g.*, 140A, 140X), and the file size (*e.g.*, 142A, 142X) of the decoy files (*e.g.*, 114A, 114X) are identical to created timestamp (122), accessed timestamp (124), modified timestamp (126), and the file size (128) of the secrets file (112). Rather than being completely identical, the aforementioned components may be substantially identical (*e.g.*, have only a difference of a few seconds or millisecond). Moreover, the values of the aforementioned components of the secrets file (112) are within the range of values of the aforementioned components of the various decoy files (*e.g.*, 114A, 114X). For example, if the modified timestamp of the secrets file is 10:21:45 AM on August 1, 2010, the modified timestamp of the decoy files may range from 10:21:36 AM on August 1, 2010 to 10:21:59 AM on August 1, 2010. A broader range of timestamps may exist without departing from the scope of the invention.

[0063] Similar to the file name (*e.g.*, 134A, 134X) of the decoy files (*e.g.*, 114A, 114X) and the file name (120) of the secrets file (112), the decoy data (*e.g.*, 132A, 132X) appear indistinguishable to the secrets (118). In particular, the decoy data (*e.g.*, 132A, 132X) has the same apparent randomization of characters as the secrets. Further, if the secrets file is partitioned into secrets (*e.g.*, static and dynamic secrets), then the decoy data is also partitioned into strings of the same number of characters as the secrets. Similarly, if the secrets file includes identifiers, then the decoy data also includes similar identifiers. Thus, the decoy data (*e.g.*, 132A, 132X) includes the same amount, same identifier, same file structure and the same apparent randomization of characters as the secrets (118) in accordance with one or more embodiments of the invention. The decoy data (*e.g.*, 132A, 132X) may be encrypted, for example, using the same encryption algorithm to encrypt the secrets (118).

[0064] Although Fig. 1 shows the secrets file (112) as the first file, the secrets file (112) may be intermingled between the decoy files (*e.g.*, 114A, 114X). For example, the ordering of the files within the secrets directory does not account for fact that the secrets file is a secrets file. Thus, the secrets file (112) is not in a pre-defined position within the secrets directory.

[0065] Further, a portion of the security application (102) may be remote from the computing device. For example, a portion of the security application may be stored on an external storage device. As another example, an external device that is connected to the computing device may be configured to process and display a user interface for the security application (102) executing on the computing device.

[0066] Further, the metadata shown in Fig. 1 may be only a portion of the metadata (*e.g.*, 116, 130A, 130X) that is manipulated to be identical or substantially identical for the secrets file (112) and the decoy files (*e.g.*, 114A, 114X). Specifically, the secrets file (112) and the decoy files (*e.g.*, 114A, 114X) may include additional metadata without departing from the scope of the invention. Further, the additional metadata may or may not be updated to be identical or substantially identical without departing from the scope of the invention. For example, if the metadata includes the file creator, then the secrets file and decoy files are forced to have the same file creator in accordance with one or more embodiments of the invention. In the example, the file creator may be the user or a pre-specified name.

[0067] Figs. 2A-5B show flowcharts in accordance with one or more embodiments of the invention. While the various steps in these flowcharts are presented and described sequentially, one of ordinary skill will appreciate that some or all of the steps may be executed in different orders, may be combined or omitted, and some or all of the steps may be executed in parallel. Further, in the following flowcharts, a member of the group is deemed to perform the actions when the security application of the member performs the actions on behalf of the member.

[0068] Figs. 2A-2B show a flowchart for configuring the security application in accordance with one or more embodiments of the invention. As shown in Fig. 2A, in Step 201, execution of a configuration utility in the security application is started. In one or more embodiments of the invention, the first time that a user starts the security application, the configuration utility is started. Further, in one or more embodiments of the invention, the user may use the configuration utility after the first configuration, such as to add additional groups. As discussed below, the configuration utility may guide the user through configuring the security application to communicate with the groups of which the user's computing device is a member. Those skilled in the art will appreciate that a process executing on the computing device may initiate the configuration of the security instead of the user.

[0069] Continuing with Fig. 2A, in Step 203, the security application receives new user credentials. In one or more embodiments of the invention, the new user credentials may include, for example, a username and password. Other forms of user credentials may be used without departing from the scope of the invention. After the user provides the new user credentials, the user may be required later to use the provided credentials to use the security application.

[0070] Alternatively, rather than the user providing new user credentials in Step 203, the security application may be pre-configured with user credentials. For example, consider the scenario in which the security application is provided to the user by a business entity that pre-associates the security application with user credentials. In such a scenario, the user in Step 203 may be requested to provide the pre-associated credentials in order to configure the security application.

[0071] Continuing with Fig. 2A, in Step 205, a configuration of a new group is initiated. For example, a user may select a menu option or software button to indicate that the user would like to add a new group. Alternatively or additionally, the configuration may be based on the user receiving an invite via the security application. The user may be invited by other members to the

group. For example, consider the scenario in which the user is an employee of a company. An administrator of the company may trigger the administrator's security application to send, to the employee's work computer, an invitation to join the group. Based on the invite, the security application on the employees work computer starts the configuration of the new group.

[0072] In Step 207, the name of the group is received. In one or more embodiments of the invention, the user provides a nickname for the group. The user may provide a name that the user is capable of remembering. For example, the name may be the names of the users who have computing devices that are members of the group. For example, if John's computing device, Angie's computing device, and Joe's computing device are members, then the group name may be John-Angie-Joe. Further, in one or more embodiments of the invention, the names are alphabetically ordered. For example, the group name may be Angie-Joe-John. Rather than using names associated with the members of the group, the group name may be a description of the group (*e.g.*, "financial management team," "work group," "lawsuit strategy team," etc.).

[0073] In Step 209, a group agreed connect name for the new group is received. In one or more embodiments of the invention, a group agreed connect name is an identifier of the group used by all of the members. Specifically, each member of the group associates the same group agreed connect name with the group. Thus, whereas the name of the group in Step 207 may be a name used by a single member, the group agreed connect name is an identifier shared by all members. Further, the group agreed connect name may be an alphanumeric value which would be very difficult to memorize. Because all members associate the same group with the same group agreed connect name, the group agreed connect name may be used by a member of the group when triggering the start of a communication session with other members of the group. For example, consider the scenario in which group A includes Angie's computing device, Joe's computing device, and John's computing device, and has a connect name of 32. Group B includes only Joe's computing device and

Angie's computing device, and has connect name 43. In the scenario, Joe's computing device may start communication with the Group A by using connect name 32. Thus, Angie's computing device uses the correct set of secrets for Group A.

[0074] The group may agree on a group agreed connect name by using a negotiation protocol. For example, one or more members may broadcast a proposed connect name, which is either accepted or rejected by the other group members. If all members agree, then the agreed proposed connect name may be a group agreed connect name. Alternatively, the group agreed connect name may be assigned. For example, an administrator of the group, who may or may not be a member, may assign the group agreed connect name to the group. As another example, users of the members may communicate the group agreed connect name in person, over the phone, via postal mail, or using any other alternative communication channel.

[0075] In Step 211, a first message digest is generated using the group agreed connect name and the user credentials as inputs into the n-bit generator. Specifically, the encryption module calls the n-bit generator using the group agreed connect name and the user credentials as the input values. The n-bit generator generates the first message digest by applying the operations of the n-bit generator (discussed above) to the input values.

[0076] In Step 213, a secrets file name and a secrets file encryption key is extracted from the first message digest. Specifically, the encryption module identifies each portion of the message digest corresponding to a secrets file name and a secrets file encryption key. For example, in a 512-bit message digest, bits in bit positions 0-255 may correspond to the secrets file name, bits in bit positions corresponding to 256-383 may correspond to the secrets file encryption key, and the final 128 bits may correspond to discard bits that remain unused. In the example, the security application extracts the secrets file name by obtaining 0-255 bits and extracts the secrets file encryption key by obtaining the next 128 bits. In one or more embodiments of the invention,

because the user credentials are part of the input in Step 211, with a high probability, a different message digest is generated by each member of the group. Thus, the secrets file name and the secrets file encryption key are different for each member of the group. Thus, a nefarious individual or computer system cannot correlate file names on different members to identify the secrets file or decrypt an encrypted secrets file using a secrets file encryption key generated by another member.

[0077] In Step 215, a determination is made whether a file naming conflict exists in the security directory. Specifically, a determination is made whether the file name matches an existing file name in the security directory. If a file naming conflict exists, the naming conflict is corrected in Step 217. Different techniques may be used to correct the naming conflict. For example, the member having the naming conflict may request that a new group agreed connect name is used. The new group agreed connect name may be generated by incrementing or appending a value on the previous group agreed connect name or repeating Step 209. Other methods to correct the naming conflict may be used without departing from the scope of the invention.

[0078] Continuing with Fig. 2B, in Step 219, regardless of whether a naming conflict exists, a group agreed seed is received for the secrets file. Specifically, the members of the group and/or their corresponding users communicate and agree on a group agreed seed. If the users communicate and agree on the group agreed seed, then the user may submit the group agreed seed to the security application. In such embodiments, the security application obtains the group agreed seed from the member. If the members communicate with the other members regarding the group agreed seed, then the member obtains the group agreed seed as the one agreed upon. The group agreed seed may be any password, passphrase, or series of characters. For example, the group agreed seed may be “the cow jumped over the moon,” “#8\$#DsaVA(@12w@,” or any other collection of characters (*e.g.*, symbols and/or alphanumeric characters). Users of the members may communicate the group agreed seed in person, over

the phone, via postal mail, or using any other alternative communication channel. Each member may independently submit the group agreed seed to the security application. When prompted, the user of each member may enter the group agreed seed in a field of the user interface of the security application.

[0079] In Step 221, a second message digest is generated using the group agreed seed as input into the n-bit generator. Specifically, the encryption module calls the n-bit generator using the group agreed seed as the input value. The n-bit generators of each of the members performs the same one or more functions for all of the members of the group. Thus, the same message digest (*i.e.*, the second message digest) is generated by all members of the group.

[0080] In Step 223, secrets are obtained from the second message digest. Specifically, the encryption module identifies each portion of the second message digest relating to a secret. The following examples are not intended to limit the scope of the invention. Turning to an example, in a 512-bit message digest, bits in bit positions 0-127 may correspond to the static secret, bits in bit position corresponding to 128-383 may correspond to the dynamic secret and the final 128 bits may correspond to discard bits that remain unused or to a change (increment) value to be included as an input to an iterative pass of the n-bit generator. In the example, the security application extracts the static secret by obtaining the first 128 bits of the message digest and extracts the dynamic secret by obtaining the next 256 bits. As discussed, the above is only an example. For example, the ordering of the static secrets, dynamic secret, and discard bits may be different from the previous example, the discard bits may be omitted, the static secret or a portion thereof may be in different message digests, the dynamic secret or a portion thereof may be in different message digests, or one of the secrets may be omitted. In one or more embodiments of the invention, each security application extracts the same bits for each of the secrets. Thus, each member of the group generates the same set of secrets.

[0081] As another example for extracting secrets, bits in the message digest may indicate the starting position of each of the secrets. For example, the first four bits low order or least significant of the message digest may be used as shift bits defining the start of a secret. In such an example, the first bit of a secret may start following the shift value. By way of an example, if the shift bits in the message digest is “0001” (or one in base 10), then the secret starts at bit position two. As another example, if the shift bits is “1000” (or eight in base 10), the secret starts a bit 9.

[0082] Additional secrets may be generated for the group by repeating Steps 221 and 223 using the second message digest (or a portion thereof) and subsequent message digests (or a portion thereof) as an input to the n-bit generator. Alternatively, or additionally, Steps 221 and 223 may be repeated multiple times to generate a succession of new secrets. For example, each subsequent time may use, as input, the message digest from the previously time. Alternatively or additionally, additional secrets may be generated by repeating Steps 203-205 in which new group agreed seeds are used.

[0083] In Step 225, the secrets are stored in the secrets file. As discussed above, each secret may be stored with the unique secret identifier and/or a secrets grouping identifier.

[0084] In Step 227, the secrets are encrypted using the secrets file encryption key (obtained in Step 213). Specifically, the encryption module applies an encryption algorithm to the secrets file using the secrets file encryption key. Thus, the secrets in the secrets file may be protected even if the secrets file is identified.

[0085] In Step 229, decoy file names and contents are generated for the decoy files. Different techniques may be used to create the decoy file names and contents. For example, the encryption module may request that the n-bit generator uses a random character generator to generate a random set of characters of an identical length as the secrets and secrets file name. As

another example, the encryption module may call the n-bit generator with pseudo-randomly generated input to create the decoy files. As another example, the encryption module may use the final generated secret (*e.g.*, secret(s) obtained in Step 223) with or without modification input as input to the n-bit generator to produce additional content.

[0086] In one or more embodiments of the invention, two or three decoy files are created each time a secrets file is created. More or fewer decoy files may be created without departing from the scope of the invention. Further, once the security directory has a threshold number of files (secrets file and decoy files), the encryption module may stop creating decoy files in one or more embodiments of the invention.

[0087] In Step 231, the decoy files are stored in the security directory with the secrets file. In one or more embodiments of the invention, the creation storage of the decoy files is the same time as the creation and storage of the encrypted secrets file. Thus, the decoy files and the secrets file have the same timestamps. Those skilled in the art will appreciate that the timestamps on the decoy files and/or the secrets file may be modified such that all timestamps are the same or within an appropriate range (as defined above).

[0088] In Step 233, identifiers of members of the group are received. Specifically, an identifier for each member of the group is received. The identifier may be a unique identifier, a nickname, or another identifier.

[0089] In Step 235, connection information to create a secure connection to each member of the group is received. Specifically, the connection information identifies how to access the member through a secure communication channel if it exists. Alternatively, the connection information may specify general contact information, such as a phone number, an internet protocol (IP) address, or other contact information. In Step 237, the connection information is stored with the identifiers for the group. The connection information and the identifiers may be stored in a separate file, such as a configuration file

associated with the security application. Further, the same connection information may be used by the member for multiple groups that have common members.

[0090] Although not shown in Figs. 2A-2B, additional groups may be added by repeating Steps 205-237 for each group. In one or more embodiments of the invention, when a new group is created, the timestamps of all existing files are updated to match the new group. The timestamps may be updated, for example, using APIs provided by the operating system to force an update of the timestamps.

[0091] Fig. 3 shows a flowchart for communicating between members of the group in one or more embodiments of the invention. In Step 231, a request for group communication is received. The request may be received from the user using the member, an application executing on the member or executing on a computer system connected to the member, another member, etc.

[0092] For example, the user may start the security application and select a group using the group name to start sending communications. The user may also select the application (*e.g.*, email application, chat application, etc.) that the user will use for the communication. In response, the security application may access the connection information for other members of the group and send an invite to the other members using the connection information. The invite may include the group agreed connect name and indicate that the member is starting a communication session for the group having the specified connect name. Additionally, or alternatively, the invite may be sent with the first communication from the member.

[0093] As a second example, the user may use an application (*e.g.*, a email application, a chat application, an internet browser) to start a communication session with another user. The security application may intercept the user's connection request, identify the members of the group corresponding to the recipient users, and invite the other members of the group to the

communication session using the group agreed connect name and the connection information for the other members.

[0094] As a third example, the request for group communication may be initiated by the security application receiving an invite to the communication session from another member of the group. In response, the security application may notify the user that a communication session is requested in accordance with one or more embodiments of the invention.

[0095] The above are only some examples of how a request for communication is received. The request for communication may be received in other manner without departing from the scope of the invention.

[0096] In Step 233, user credentials are received. In one or more embodiments of the invention, the member prompts the user to provide the user credentials. For example, the user interface of the security application may display one or more input boxes for the user to submit the user's credentials.

[0097] In Step 235, the n-bit generator generates the secrets file name and the secrets file encryption key using the user's credentials and the group agreed connect name. Specifically, the n-bit generator generates a message digest having the secrets file name and the secrets file encryption key using the aforementioned inputs. The encryption module extracts the aforementioned components from the message digest. Generating the message digest and extracting the secrets file encryption key may be performed as discussed above with reference to Steps 211 and 213 in Fig. 2.

[0098] In Step 237, a determination is made whether a matching file name is found in the security directory. If a matching file name is found, then the user's credentials are correct and the secrets file is identified. If the matching file name is not found, then the received user's credentials may be incorrect. The security application may allow the user to re-submit the credentials and/or deny access to the user.

[0099] In Step 239, if the matching file name is found, the secrets file is decrypted using the secrets file encryption key. Specifically, the encryption module applies the encryption algorithm to the encrypted secrets file (*i.e.*, the file identified in Step 237) using the secrets file encryption key to create a decrypted secrets file.

[00100] In Step 241, the secrets are obtained from the decrypted secrets file. In one or more embodiments of the invention, the secrets may be obtained based on the type of unique secret identifier and/or a secrets grouping identifier. For example, the communication request may specify an application used in the communication. Accordingly, encryption module may identify the secrets grouping identifier corresponding to the specified application. The encryption module obtains the secrets from the secrets file having the specified secrets grouping identifier.

[00101] In one or more embodiments of the invention, rather than opening the secrets file to obtain the secrets, the secrets file may be copied to a temporary memory location, such as cache memory, and the copy may be opened to obtain the secrets. Thus, if the dynamic secrets are not updated at the end of the communication session, then the metadata of the secrets file remains unchanged. When the metadata of the secrets file remains unchanged, then the metadata of the decoy files does not need to change. Further, the contents of the temporary memory location may be destroyed so as to destroy the copy of the secrets file. The destruction may include overwriting the temporary location multiple times in accordance with one or more embodiments of the invention.

[00102] As another example, the communication request may include the unique secret identifier. In the example, the encryption module may extract the secret having the unique secrets identifier from the secrets file.

[00103] By way of another example, the encryption module may randomly select secrets (*e.g.*, a static and dynamic secret) and send the unique secrets identifier of the randomly selected secrets to the other members of the group.

[00104] The above are only a few examples for obtaining secrets from the secrets file. Other methods may be used without departing from the scope of the invention.

[00105] In Step 243, the n-bit generator generates one or more message digests using the secrets. Generating one or more message digests is discussed below and in Figs. 4A and 4B.

[00106] Continuing with Fig. 3, the encryption module encrypts and decrypts communications transferred between the members of the group using an encryption key parsed from the message digest. As discussed below, from the message digest(s), an encryption key is generated. The encryption module applies the encryption key and an encryption algorithm to each communication for sending to encrypt the communication. The encrypted communication is sent to the other members of the group. Similarly, the encryption module applies the encryption key and the encryption algorithm to each received communication to decrypt the received communication.

[00107] In one or more embodiments of the invention, the encryption module intercepts the communications sent and received from the member to the group or from a computer system connected to the member to the group. The encryption module performs the encryption and decryption steps without input from and transparently to the user (or other computer system to which the security application is connected) in one or more embodiments of the invention.

[00108] In one or more embodiments of the invention, the security application may be used for communications between subgroups, in which only some of the members are present using the secrets for the group. In one or more embodiments of the invention, the sub-group may be spawned into a new group. Additionally, or alternatively, when only the subgroup is communicating, the dynamic secret is not updated for the entire group.

[00109] Figs. 4A and 4B show flowcharts for using the initial message digest to generate an encryption key. As shown in Fig. 4A, in Step 251, a shared secret(s) is obtained from the secrets file. In Step 253, a new message digest is generated using the shared secret(s) as inputs for the n-bit generator. For example, the encryption module may call the n-bit generator and pass the parameters of the shared secret(s).

[00110] In Step 255, an encryption key is extracted from the resulting message digest. Extracting the encryption key may include the encryption module identifying the bit positions corresponding to the encryption key and separately storing the series of bits in the identified bit positions as the encryption key. In addition to extracting the encryption key, algorithm selector bits, key length and other components of the message digest may be extracted. The algorithm selector bits may be used, for example, as an index to the algorithm selector table to identify an encryption algorithm to use to encrypt the communications.

[00111] Fig. 4B shows another example flowchart for using the initial message digest. Specifically, Fig. 4B shows an example for generating multiple message digests, where each message digest includes some of the components for encrypting a communication. In Step 257, the shared secret and dynamic secret are obtained from the secrets file. Obtaining the shared secret and the dynamic secret may be performed as discussed above.

[00112] In Step 259, a second message digest is generated using the shared secret and the dynamic secret as inputs for the n-bit generator. Generating the second message digest may be performed in a similar manner to that discussed above with reference to Step 253 in Fig. 4A.

[00113] In Step 261, the change value and other components are extracted from the second message digest. Extracting the components may be performed in a manner similar to the extraction of the encryption key as discussed above in Step 255 of Fig. 4A. The other components that are extracted may include, for

example, the most significant bits of the encryption key, the least significant bits of the encryption key, the algorithm selector bits, etc.

[00114] In Step 263 of Fig. 4B, the change value is combined with the dynamic secret to create an interim dynamic secret. Combining the change value with the dynamic secret may be performed, for example, by a bit shuffler. Specifically, any of the operations discussed above with respect to the bit shuffler may be performed to combine the change value with the dynamic secret. In one or more embodiments of the invention, a prime number is added to the change value or result to account for a possibility that the change value may be zero. For example, the combination may be the change value XOR'd with the dynamic secret plus one.

[00115] In Step 265, a third message digest is generated using the interim dynamic secret and the static secret as inputs to the n-bit generator. Step 265 may be performed, for example, in a manner similar to the above discussion with reference to Step 259. In one or more embodiments of the invention, rather than performing Step 263 to create an interim dynamic secret and then performing Step 265 to generate a third message digest using the interim dynamic secret, the third message digest may be generated using the change value, the dynamic secret, and the static secrets as inputs into the n-bit generator.

[00116] In Step 267, the change value and other components are extracted from the third message digest in accordance with one or more embodiments of the invention. Extracting the change value and the other components may be in a manner similar to the above discussion with reference to Step 261.

[00117] In Step 269, a determination is made whether to create another message digest. In one or more embodiments of the invention, each security application is configured to create an identical number of message digests. Additional message digests may be generated to create additional bits for an encryption key or to create additional components.

[00118] If a determination is made to create an additional message digest, then the steps repeat starting with Step 263. In Step 263, the change value extracted in Step 267 is used with the dynamic secret to create a new interim dynamic secret. Alternatively, rather than using the dynamic secret for subsequent message digests, the previously created interim dynamic secret may be used.

[00119] Alternatively, if a determination is made not to create another message digest, an encryption solution is created from the components of the message digests in Step 271. For example, the least significant bits of the encryption key may be combined with the most significant bits of the encryption key to create a single encryption key. The encryption solution may be used to encrypt and decrypt communications. Encrypting a communication may be performed for example, by accessing the algorithm selector table to identify the encryption algorithm corresponding to the algorithm selector bits in the message digest. The communication to be encrypted is encrypted by applying the identified encryption algorithm with the encryption key to the communication. The resulting encrypted communication may be sent to the members and/or stored (*e.g.*, stored on a local or remote storage device). In one or more embodiments of the invention, when an encrypted communication is stored, dynamic secrets are not used to create the encryption key used to encrypt the communication.

[00120] During or at the end of a session, the members of a group may agree to change the encryption key and/or the dynamic secret values. For example, the agreement may be based on a signal passed between the members when one of the members elects that the encryption key should change. As another example, the agreement may be based on a pre-agreed period at which a new encryption key is generated. For example, the members may agree that a new encryption key should be generated every five minutes, with every 20 communications, after 256K bits are exchanged, etc.

[00121] Fig. 5A shows a flowchart for changing an encryption key. In Step 281, a change of encryption key is initiated by the group or one of the members

thereof. As discussed above, the initiation may be based on a message, a pre-agreed period, etc.

[00122] In Step 283, intermediate results of the last performance of the n-bit generator and the last generated change value are obtained. As discussed above, the intermediate results may correspond to the output of the bit shuffler prior to performing the hash function. Further, each member may extract the change value from the last generated message digest.

[00123] In Step 285, each member generates a new message digest using the intermediate results and the last change value as inputs to the n-bit generator. In Steps 283 and 285, rather than using the intermediate results, the dynamic secret, the dynamic secret and the static secret, or the interim dynamic secret may be used in accordance with one or more embodiments of the invention.

[00124] In Step 287, a new encryption key is extracted from the new message digest. Extracting the new encryption key may be performed as discussed above with reference to Step 255 of Fig. 4A. After the new encryption key is extracted the new encryption key may be used to encrypt and decrypt communications between the members of the group. In one or more embodiments of the invention, the encryption key could be an encryption solution. The encryption solution may include, for example, the encryption key, algorithm selector bits for selecting an encryption algorithm, and/or other components used for encryption.

[00125] Fig. 5B shows an example flowchart for changing the dynamic secret values at the end of a communication session in accordance with one or more embodiments of the invention. In Step 289, a communication session is finalized with the group. For example, the group members may send a message ending the communication session. Each member may wait until the member receives confirmation from all other members of the group.

[00126] In Step 291, the initial dynamic secret and the final change value used in the communication session are obtained. For example, the initial dynamic

secret may be the secret generated in the initial message digest or a secret stored in the secrets repository. The final change value may correspond to the last generated change value. For example, the final change value may be obtained as discussed above with reference to Step 283 in Fig. 5A.

[00127] Continuing with Fig. 5B, in Step 293, a new message digest is generated using the initial dynamic secret and the change value as inputs to the n-bit generator. In Step 295, the new dynamic secret is extracted from the new message digest. The new dynamic secret may replace the initial dynamic secret in the secrets file. Specifically, in Step 297, each member of the group may store the new dynamic secret in their corresponding secrets repository. Because each member generates and stores the same new dynamic secret, the members use the same secrets in the next communication session.

[00128] Further, each member updates the secrets files and the decoy files to update the file time stamps in Step 299. Specifically, each files may be opened, modified, and closed. The modification may be changing a character into a new randomly generated character and saving the changed decoy file. As another example, the modification may be writing a character to the decoy file, saving the decoy file, and then removing the character from the decoy file and the secrets files. In one or more embodiments of the invention, the update to the secrets file is performed after some of the decoy files are updated and prior to the final decoy files are updated. By modifying the decoy files when the secrets file is modified, the timestamps of the decoy files may be automatically updated. Rather than performing the modification, the metadata of the files may be updated by manipulating the metadata directly, such as through an API of an operating system, or accessing the metadata. Thus, a nefarious user or computer system could not access the modification timestamp to identify the secrets file.

[00129] Figs. 6A-6B shows an example communication session in accordance with one or more embodiments of the invention. The following is for example purposes only. In the following example, consider the scenario in which Opal

and Andrew want to communicate via a chat application. Opal's computing device is an external token device that connects to a computer system that includes a chat application. Opal's token executes the security application and includes the secrets file. Opal's computing device is referred to below as the originating member. Similarly, Andrew's computing device is a smart phone that has a chat application and a security application. Andrew's smart phone is referred to below as the answering member.

[00130] In the example, Opal opens her chat application on her computer system and connects her token to the computer system. Opal selects Andrew as the recipient of the communication. The chat application sends a request to the token to open a communication session with Andrew. The security application executing on the token receives the request and obtains the group agreed connect name for the group having only Opal and Andrew. The security application also identifies the connection information for Andrew. The security application sends Andrew a communication request to communicate via chat.

[00131] Figs. 6A-6B shows flowcharts from the perspective of the answering member (*i.e.*, Andrew's smart phone). Starting with Fig. 6A, in Step 301, the answering member receives a communication request to communicate using a chat application. Specifically, Andrew's smart phone receives, from Opal's token, a request specifying the group agreed connect name, and an identifier of a chat session. Accordingly, in Step 303, the group agreed connect name is obtained from the communication request.

[00132] In Step 305, the answering member informs Andrew of the communication request. Specifically, the security application on the smart phone may have a notification mechanism, such as an icon, ring tone, or other notification mechanism, that informs Andrew that a communication request is received. At this stage, Andrew may decide whether to accept or reject the communication request. If Andrew rejects the communication request, then the answering member ends the communication session with Opal. (not shown)

[00133] However, if Andrew accepts the communication request, then Andrew submits his username and password. Accordingly, in Step 307, the answering system receives a username and password from Andrew.

[00134] In Step 309, the n-bit generator executing on the answering system generates a first message digest using the username, password, and the group agreed connect name as inputs. For example, the n-bit generator may XOR the username, password, and group agreed connect name to create an intermediate result. The intermediate result may be input to an MD5 hash function to create a pseudo-random string as the first message digest.

[00135] In Step 311, the answering member extracts the secrets file name and the secrets file encryption key from the first message digest. The secrets file name may be, in the example, the last 128 bits of the first message digest and the secrets file encryption key may be, in the example, the first 256 bits of the message digest. Based on the extracted secrets file name, the answering member identifies the secrets file on Andrew's smart phone. Because the first message digest is a pseudo-random bit string, the secrets file name is also pseudo random and can only be identified if the username, group agreed identifier, and password are correct. Thus, by finding the secrets file name, the security application authenticates Andrew as the user of the smart phone. Alternatively, the smart phone might verify the user name and password independent of the secure chat application.

[00136] In Step 313, the answering member decrypts the identified secrets file using the secrets file encryption key. Specifically, the answering member uses the secrets file encryption key and a symmetric encryption algorithm to decrypt the secrets file. From the decrypted secrets file, the answering member extracts the secrets corresponding to the chat application in Step 315. For example, the answering member may identify that the fifth secret is the secret corresponding to the chat application based on a pre-defined configuration parameter or an identifier stored with the fifth secret which is 384 bits and the beginning bit is bit 84.

[00137] Continuing with Fig. 6B, in Step 317, the n-bit generator on the answering system generates a second message digest using the secret. The answering system's encryption module may extract from the fifth secret, the dynamic secret and the static secret and provide the dynamic secret and the static secret as inputs to the n-bit generator. The n-bit generator combines the dynamic secret and the static secret to produce the second message digest. For example, the initial message digest may correspond to message digest (350) shown in example Fig. 6C. Referring to Fig. 6C, a message digest (350) may include an originating member's one-time password (352), discard bits (354), an encryption key most significant bits (356), and a change value (358).

[00138] The originating member's one-time password (352) is a series of bits generated by the n-bit generator for the answering member to authenticate the originating member. Specifically, because both the originating member and the answering member generate the same message digest (*e.g.*, example message digest (350)), the originating member's one-time password (352) is the same for the first member and the second member. Accordingly, if the first member's one-time password (352) that the first member sends to the second member is identical to the second member's generated first member's one time password, then the second member knows that the first member is authentic. Specifically, the first member knows that the second member received the same input and had an n-bit generator that was capable of performing the same operations. Further, in one or more embodiments, once the first member and second member passwords have been confirmed, an extremely high probability exists that the other corresponding bits of the message digest also match between systems.

[00139] In one or more embodiments of the invention, prior to sending the one-time passwords, the one-time passwords are encrypted using an encryption algorithm and an encryption key. In such embodiments, the one-time passwords are sent encrypted. The receiver may encrypt their generated one-time password and compared the encrypted generated one-time password with

the received one-time password. As an alternative, the receiver may decrypt the received one-time password and then compare the decrypted one-time password with the generated one-time password.

[00140] Discard bits (354) are bits that are ignored when creating the encryption solution. Specifically, discard bits are bits that prevent the nefarious user or computer system from understanding the message digest. By having discard bits, the nefarious user or computer system may be unable to ascertain which bits are actually used for the encryption solution.

[00141] The session encryption key most significant bits (MSB) (356) correspond to a portion of the encryption key. Specifically, the encryption key may be divided into one or more parts. A portion of the encryption key may be located in a first message digest while a second portion is located in another message digest. Because all members use the instances of the same n-bit generator to generate the message digests, the encryption key generated by each of the members is the same. Thus, the encryption key does not need to be communicated between the members. Moreover, the encryption key may be stored in the security application and not provided through any interface to any user. Thus, members (and users of the members) that leave the group remain unaware of the encryption key used to encrypt the data.

[00142] In one or more embodiments of the invention, a change value (358) provides a pseudo-random value to spawn a new message digest. For example, the change value may be used to create a new encryption key or create a new dynamic secret. Further, the stored secrets may be inputted to the n-bit generator to spawn temporary use secrets. All of the spawned secrets are used only during a session in accordance with one or more embodiments of the invention. After the session, the spawned secrets are destroyed so as to be no longer accessible or otherwise obtainable through any nefarious methods. Similar to the temporary use secrets, the change value is destroyed once combined with the appropriate dynamic secret value.

[00143] Returning to the example message digest (350), Fig. 6C is only one example of the components of a message digest. Some of the components may be removed while other components may be added.

[00144] Returning to Fig. 6B, in Step 319, the encryption module on the answering system extracts the originating member's one time password, the encryption key's most significant bits, and a change value from the second message digest. The extracted change value is combined with the original dynamic secret in Step 321 to create an interim dynamic secret in the example. The interim dynamic secret may be obtained by performing an XOR operation on the change value and the original dynamic secret plus one.

[00145] Using the interim dynamic secret, the n-bit generator generates the third message digest in Step 323. For example, the initial message digest may correspond to message digest (360) shown in example Fig. 6D. Referring to Fig. 6D, a message digest (360) may include an answering member's one-time password (362), discard bits (364), an encryption key least significant bits (366), and a change value (368). The answering member's one-time password (362), discard bits (364), an encryption key least significant bits (366), and a change value (368) are similar to the originating member's one-time password (352), discard bits (354), an encryption key most significant bits (356), and a change value (358) in Fig. 6C.

[00146] Specifically, the answering member's one-time password (362) is a series of bits generated by the n-bit generator for the originating member to authenticate the answering member. Discard bits (364) are bits that are ignored when creating the encryption solution. The session encryption key least significant bits (LSB) (366) correspond to a second portion of the encryption key. The change value (368) provides a random value to create a new message digest.

[00147] Returning to the example message digest (360), Fig. 6D is only one example of the components of a message digest. Some of the components may be removed while other components may be added.

[00148] Returning to Fig. 6B, the answering member extracts the answering member's one-time password, the encryption key's least significant bits, the change value from the third message digest.

[00149] Although not discussed above, after the originating member finds the secrets file located on the originating member, the originating member performs the same steps as the answering member. Thus, both the originating member and the answering member generate the second and third message digests. The answering member sends the answering member's one-time password to the originating member in Step 327. The originating member sends the originating member's one-time password to the answering member. Accordingly, the answering member receives the originating member's one-time password in Step 329.

[00150] Both the originating member and the answering member compare the received one-time password with the generated one-time password to determine if the received password is identical to the generated password. For example, in Step 331, the answering member determines whether the received originating member's one-time password is equal to the generated originating member's one-time password. If the two passwords are not equal, then the answering member may stop communication with the originating member. Similarly, although not shown, the originating member determines whether the received answering member's one-time password is equal to the generated answering member's one-time password. If the two passwords are not equal, then the originating member may stop communication with the answering member.

[00151] However, in Step 333, if the passwords are equal, then the encryption key's most significant bits are concatenated with the encryption key's least significant bits to create the encryption key.

[00152] At this stage, Opal and Andrew may start communicating via the chat application. The encryption modules intercept each outgoing communication and encrypt it using the encryption key in Step 335. Similarly, the encryption modules intercept each incoming communication and decrypt it using the encryption key (not shown). Further, Steps 301, 303, and 309-335 in Figs. 6A and 6B may be performed transparently to both Opal and Andrew. Thus, neither Opal nor Andrew need to be aware of the encryption. Further, in one or more embodiments of the invention, both Opal and Andrew cannot view the secrets or the encryption key. Thus, neither Opal nor Andrew can consciously or unconsciously provide a nefarious user with access to the shared secrets.

[00153] Figs. 7A-7E show an example in accordance with one or more embodiments of the invention. The following example is for example purposes only and not intended to limit the scope of the invention. Fig. 7A-7C show an example user interface for the configuration utility in accordance with one or more embodiments of the invention.

[00154] As shown in Fig. 7A, the initial configuration utility window (400) includes an input box for the user to specify the location of the security directory (402) and an input box for the user to specify a location for storing a database about users (404). Input box (402) and input box (404) may be constrained such that only a user corresponding to an administrator can change the location. Alternatively, or additionally, the input box (402) and input box (404) may be constrained so that the user can only provide locations that are on the member itself.

[00155] Additionally, in the example, the initial configuration utility window (400) includes a user manager (406). The user manager (406) allows a user to enter data specific to the user. Specifically, a user name input box (408) and

password input box (410) allows the user to enter the username and password, respectively, that the user will use each time the user uses the security application. The user may be prompted to re-enter the user password in an input box (not shown) to verify that the user entered his/her intended password.

[00156] Text box (412) provides a list of groups with whom the user may communicate. Specifically, text box (412) shows a list of the groups that the member has already added. Entries in the list may be displayed as a nickname of the group, the connect name, or other information useful to the user.

[00157] Check box (414), nick name input box (416), connect name input box (418), and connect input box (420) allows the user to submit data for a specific group. For example, if selected, check box (414) designates that the group includes more than two members. The user may submit the nick name of the group in the nick name input box (416). The user may submit the group agreed connect name of the group in the connect name input box (418). The user may submit the connection information for the group in the connect input box (420). The connect input box (420) may be used for providing the connection information for the entire group. If the check box (414) is selected, the user interface may display additional input boxes to allow a user to submit nick names and connection information for each member of the group. The additional input boxes may be displayed to provide member specific connection information.

[00158] Continuing with the example, Fig. 7B shows a user interface window (422) for submitting the group agreed seed. Specifically, the user interface window (422) may be displayed while the user is adding a new group in one or more embodiments of the invention. The user may enter the group agreed seed in input box (424) and select okay (426) to submit the group agreed seed.

[00159] In response to the user entering the group and/or the user's information, the user interface may display the window (428) shown in Fig. 7C to show that

the group has been added. Thus, the secrets file for the group may be generated.

[00160] Fig. 7D shows an example schematic diagram for generating the secrets file name and encryption key/solution. As shown in Fig. 7D, the username (430) that the user submitted in the username input box (408 in Fig. 7A), the password (432) that the user submitted in the password input box (410 in Fig. 7A), and the group agreed connect name (434) that the user submitted in connect name input box (418) are provided as inputs to the n-bit generator (436).

[00161] With the inputs, the n-bit generator (436) produces message digest (438). The message digest includes a secrets file name (440) and a secrets file encryption key (442). Accordingly, secrets created using the group agreed seed submitted in input box (424 in Fig. 7B) are stored in a secrets file, which is saved with secrets file name (440). The secrets file encryption key (442) is used to encrypt the secrets file. Accordingly, the secrets file is stored in the secrets file directory.

[00162] Fig. 7E shows an example file interface window (444) showing the secrets files directory (referred as key files in Fig. 7E) (446). As shown in the example, the contents of the secrets file directory (448) includes the secrets file and decoy files. However, because the secrets file name and the decoy file names are pseudo-random strings of characters and the secrets file and the decoy files have the same metadata, the secrets file is indistinguishable from the decoy files. For example, the security application may use the n-bit generator and similar procedures to generate the secrets as to generate the decoy files. In the example, the encryption module may call the n-bit generator four times to produce the desired number of secrets bits, and, therefore, times to produce the sufficient bits for each of ten decoy files. As another example, the encryption module may request fifty iterations of the n-bit generator to produce the decoy files and the secrets file. Because the decoy files in the example are similarly produced so as to be indistinguishable, the nefarious

computer system or user could not identify the secrets file based on the information provided in the list of files in the file interface window (444).

[00163] Embodiments of the invention may be implemented on virtually any type of computer system regardless of the platform being used. The computing device may be the computer system, execute on the computer system, be an external device of the computer system, etc. For example, as shown in Fig. 8, a computer system (500) includes one or more computing processor(s) (502), associated memory (504) (*e.g.*, random access memory (RAM), cache memory, flash memory, etc.), an internal and/or external storage device (506) (*e.g.*, a hard disk, an optical drive such as a compact disk drive or digital video disk (DVD) drive, a flash memory stick, universal serial bus (USB) drive, smart card, smart phone, etc.), and numerous other elements and functionalities typical of today's computers (not shown). The computer system (500) may also include input means, such as a keyboard (508), a touch screen (512), a mouse (510), or a microphone (not shown). Further, the computer system (500) may include output means, such as a monitor (512) (*e.g.*, a liquid crystal display (LCD), a plasma display, or cathode ray tube (CRT) monitor). The computer system (500) may be connected to a network (514) (*e.g.*, a local area network (LAN), a wide area network (WAN) such as the Internet, or any other type of network) via a network interface connection; wired or wireless (not shown). Those skilled in the art will appreciate that many different types of computer systems exist, and the aforementioned input and output means may take other forms. Generally speaking, the computer system (500) includes at least the minimal processing, input, and/or output means necessary to practice embodiments of the invention.

[00164] Computer readable program code to perform embodiments of the invention may be stored on a computer readable medium such as a compact disc (CD), a diskette, a tape, physical memory, or any other physical computer readable storage medium that includes functionality to store computer readable program code to perform embodiments of the invention. In one embodiment of

the invention the computer readable program code, when executed by a processor(s), is configured to perform embodiments of the invention.

[00165] While the invention has been described with respect to a limited number of embodiments, those skilled in the art, having benefit of this disclosure, will appreciate that other embodiments can be devised which do not depart from the scope of the invention as disclosed herein. Accordingly, the scope of the invention should be limited only by the attached claims.

CLAIMS

What is claimed is:

1. A method for authenticating a user, comprising:
 - generating, by an application running on a computing device and according to a unique user input, a secret, said secret stored at the computing device with an identifier and in a directory so as to be retrievable when the unique user input is applied to the computing device;
 - receiving at the computing device from a remote computer-based station a first communication, said first communication including the identifier associated with the secret;
 - responsive to said receiving, prompting a user for the user input via a user interface of the computing device and, upon verifying said unique user input to the computing device, transmitting from the computing device to the remote computer-based station a second communication encoded using the secret.
2. The method of claim 1, wherein the computing device is a mobile communication device.
3. The method of claim 1, wherein the secret is stored in the directory along with other secrets and the identifier is used to distinguish the secret from the other secrets.
4. The method of claim 1, wherein the secret comprises an encryption key, the encryption key is stored in the directory along with other encryption keys, and the identifier is used to distinguish the encryption key from the other encryption keys.
5. The method of claim 1, wherein the secret comprises an encryption key, the encryption key is stored in the directory along with decoy encryption keys, and the identifier is used to distinguish the encryption key from the decoy encryption keys.
6. The method of claim 1, wherein the first communication comprises an encrypted communication.
7. The method of claim 1, wherein the first communication comprises a request for user credentials of the user of the computing device.

8. The method of claim 1, further comprising encrypting said secret prior to storing said secret in said directory.
9. The method of claim 1, wherein the unique user input comprises user credentials, and further comprising receiving, via the user interface of the computing device, the user credentials prior to generating the secret.
10. The method of claim 9, further comprising receiving at the computing device an invitation to create the secret prior to generating the secret.
11. The method of claim 10, wherein the invitation to create the secret is received from the remote computer-based station.
12. The method of claim 1, wherein the first and second communications comprise two related communications of a communication session.
13. A token for use in connection with secure communications, comprising:
 - a processor and a memory communicatively coupled to the processor the memory storing a security application for execution by the processor, said security application, when executed by said processor, causing said processor to perform steps, including:
 - generating, according to a unique user input, a secret, and storing said secret with an identifier and in a directory which the processor configures in the memory such that said secret is retrievable when a unique user input is received by the token;
 - responsive to receiving the identifier associated with the secret, prompting, via a user interface, entry of the unique user input; and
 - upon receipt of the unique user input, verifying said unique user input, and using said secret to encode a first communication with a remote computer-based station.
14. The token of claim 13, wherein the secret is stored in the directory along with other secrets and the processor uses the identifier to distinguish the secret from the other secrets.
15. The token of claim 13, wherein the secret comprises an encryption key, the encryption key is stored in the directory along with other encryption keys, and the processor uses the identifier to distinguish the encryption key from the other encryption keys.

16. The token of claim 13, wherein the secret comprises an encryption key, the encryption key is stored in the directory along with decoy encryption keys, and the processor uses the identifier to distinguish the encryption key from the decoy encryption keys.
17. The token of claim 13, wherein the identifier is received in a second communication with the remote computer-based station.
18. The token of claim 15, wherein the second communication comprises a request for user credentials.
19. The token of claim 13, wherein said security application, when executed by said processor, further causes said processor to encrypt said secret prior to storing said secret in said directory.
20. The token of claim 13, wherein the unique user input comprises user credentials, and said security application, when executed by said processor, further causes said processor to receive, via the user interface of the mobile communication device, the user credentials prior to generating the secret.
21. The token of claim 20, wherein said security application, when executed by said processor, further causes said processor to generate said secret responsive to an invitation to create the secret received prior to generating the secret.
22. A mobile phone, comprising:
 - a processor and a memory communicatively coupled to the processor the memory storing a security application for execution by the processor, said security application, when executed by said processor, causing said processor to perform steps, including:
 - generating, according to a unique user input, a secret, and storing said secret with an identifier and in a directory which the processor configures in the memory such that said secret is retrievable when a unique user input is received via a user interface of the mobile phone;
 - responsive to receiving the identifier associated with the secret, prompting, via the user interface of the mobile phone, entry of the unique user input; and
 - upon receipt of the unique user input, verifying said unique user input, and using said secret to encode a first communication with a remote computer-based station,

wherein the unique user input comprises user credentials, and said security application, when executed by said processor, further causes said processor to receive, via the user interface of the mobile phone, the user credentials prior to generating the secret.

ABSTRACT

A security application for a computing device, e.g., a mobile phone, allows generation of a secret according to a unique user input (e.g., user credentials). The secret is stored in a directory such that it is retrievable when the unique user input is received via a user interface of a device on which the security application executes or is coupled with. Responsive to receiving an identifier associated with the secret, the security application prompts, e.g., via a user interface of the mobile phone, entry of the unique user input; and, subsequently, verifies the unique user input. Following such verification, the security application provides the secret for use in encoding a communication with a remote computer-based station. Entry of the user credentials may be required prior to the security application generating the secret, and may be responsive to receipt of an invitation (e.g., from the remote computer-based station) to generate it.

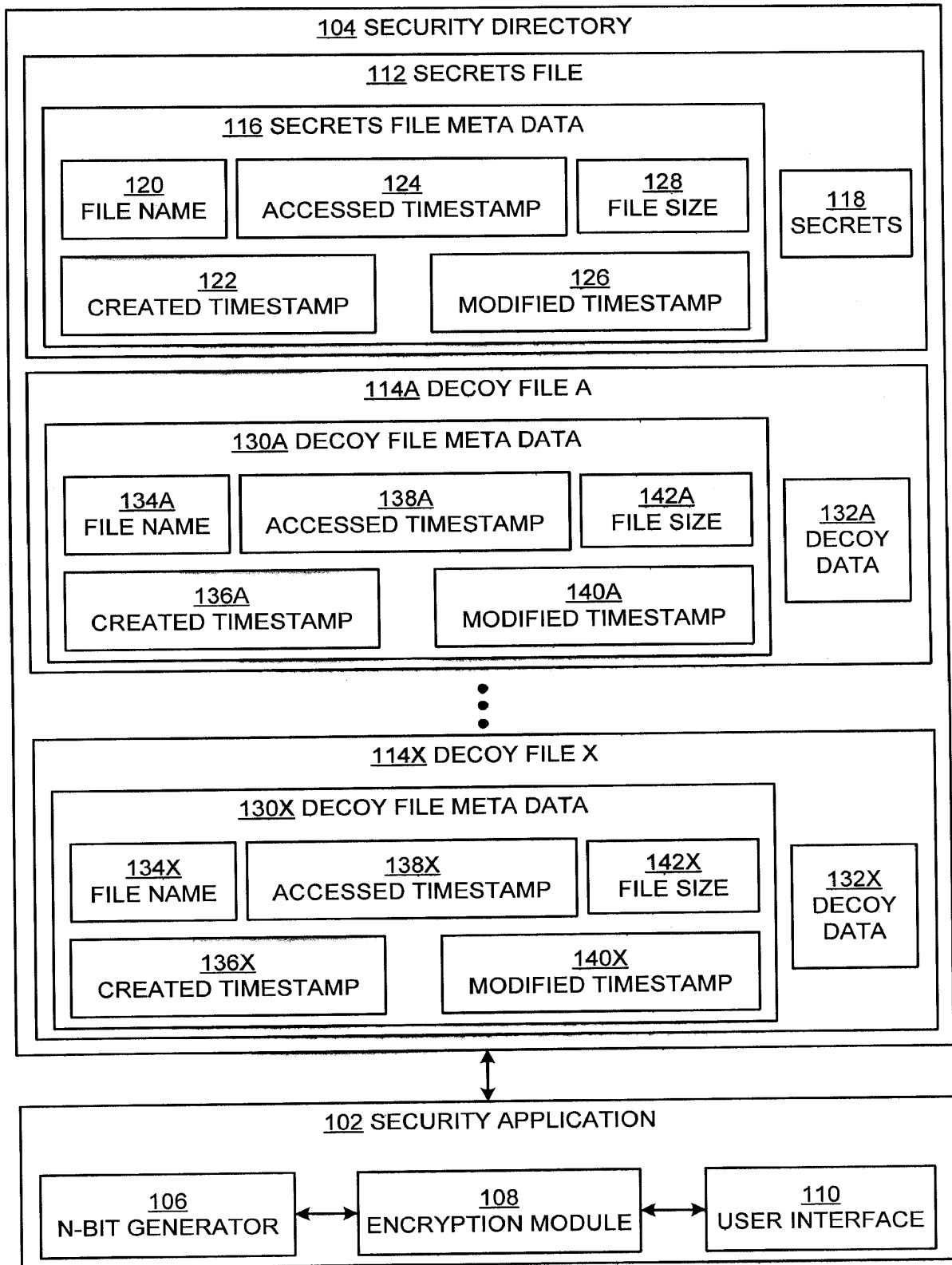


FIG. 1

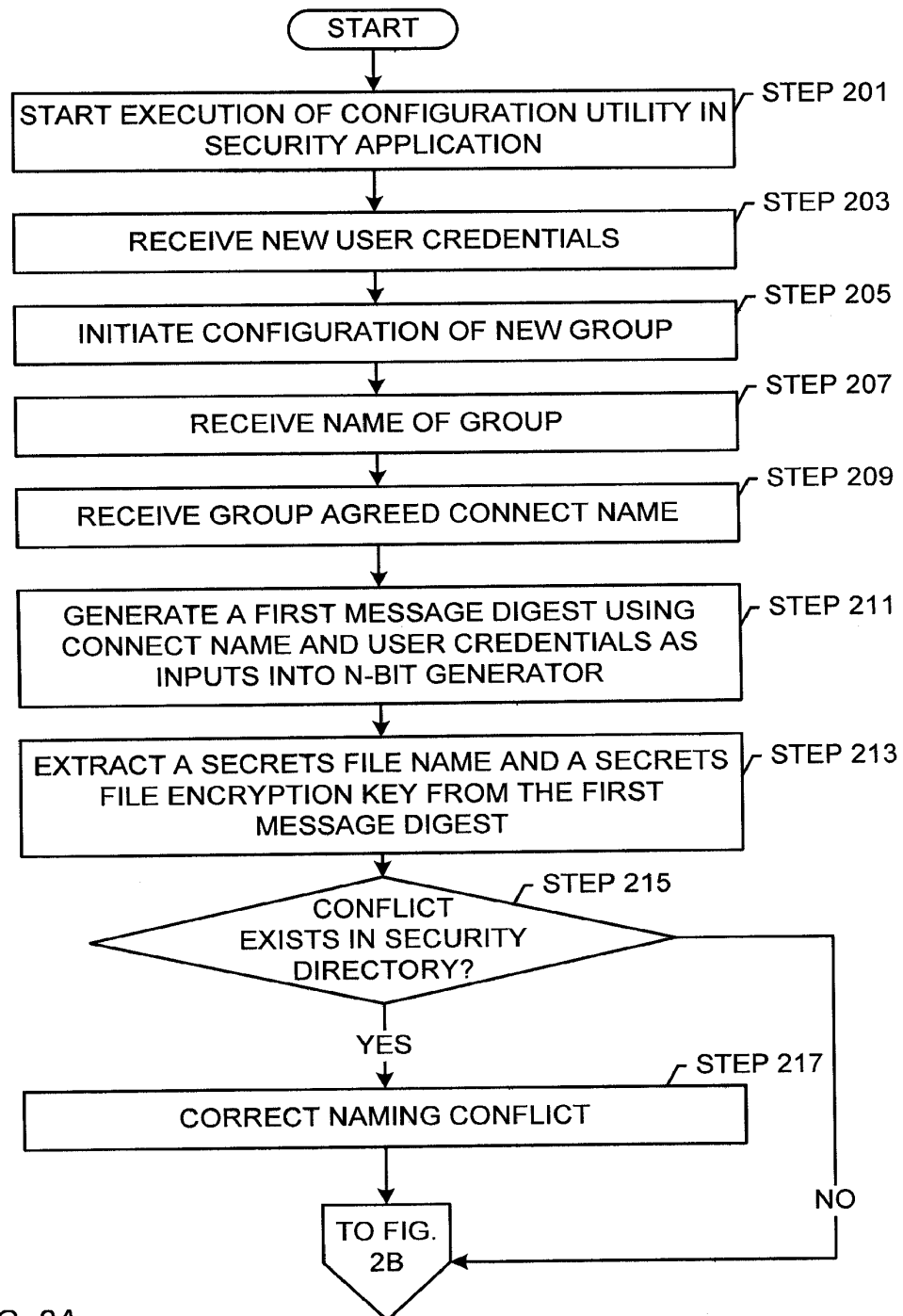
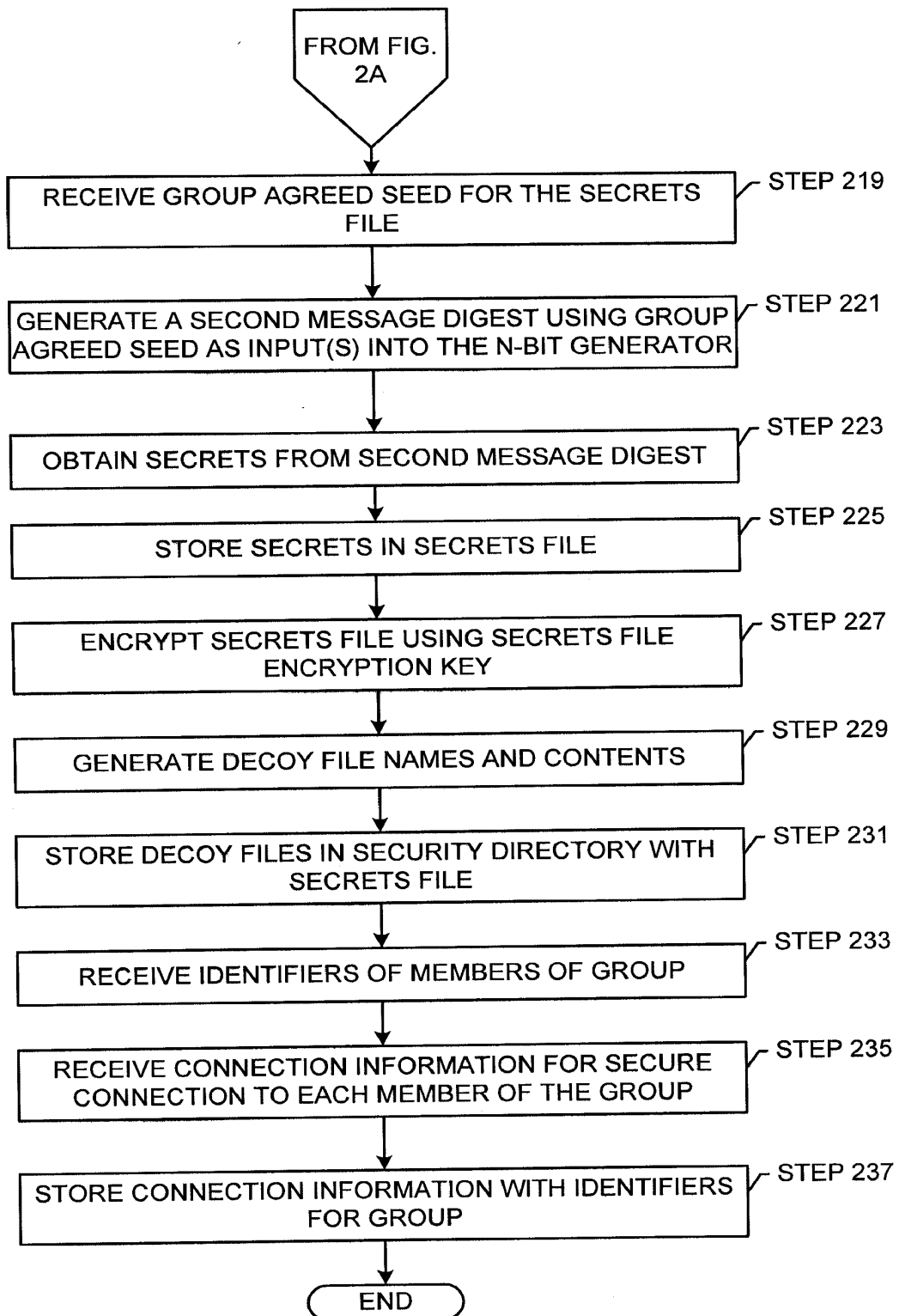
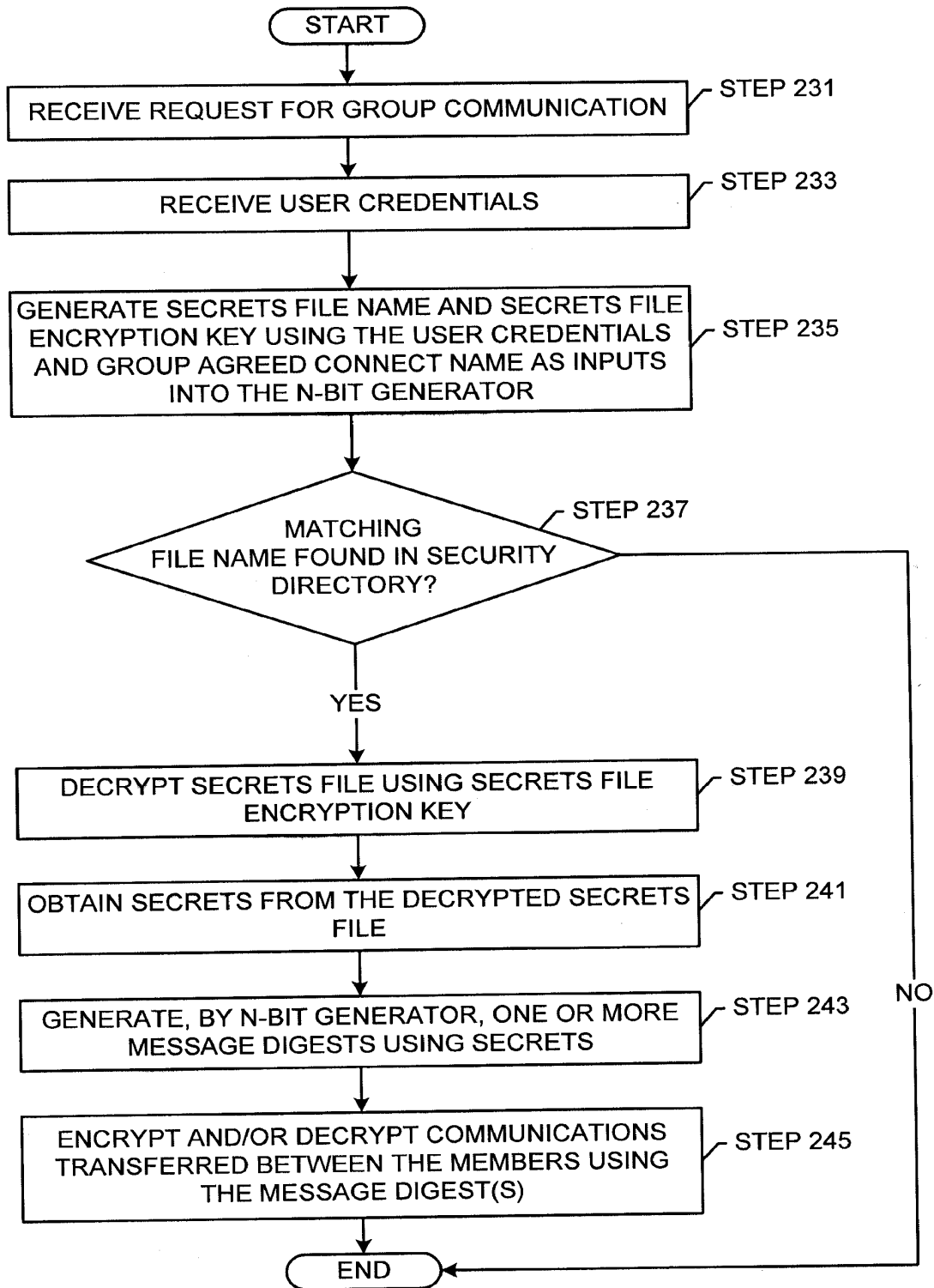
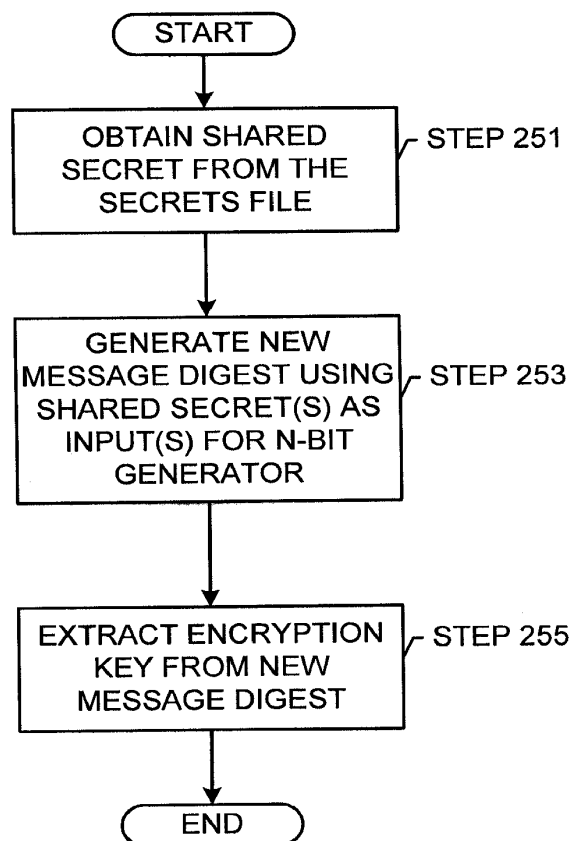
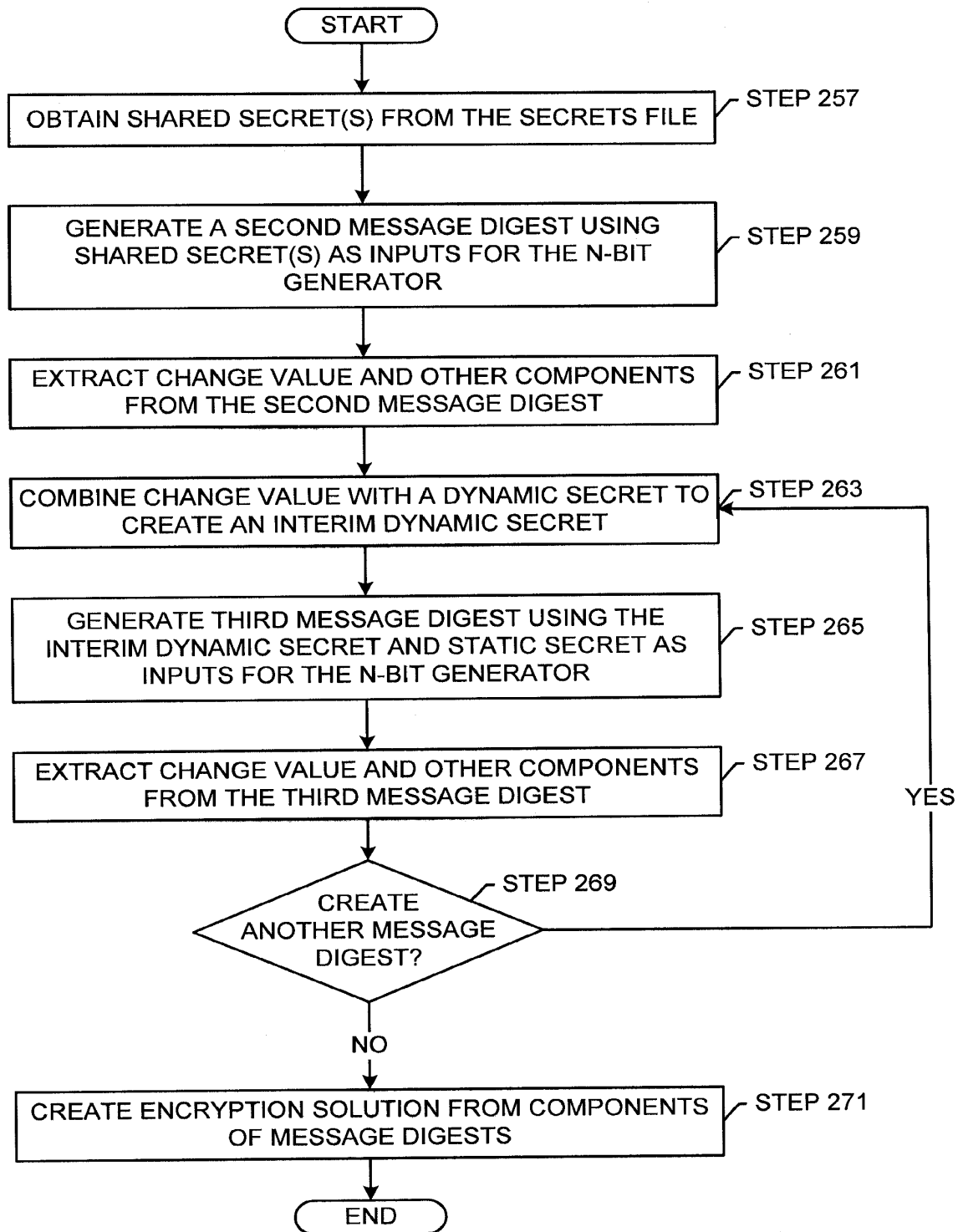


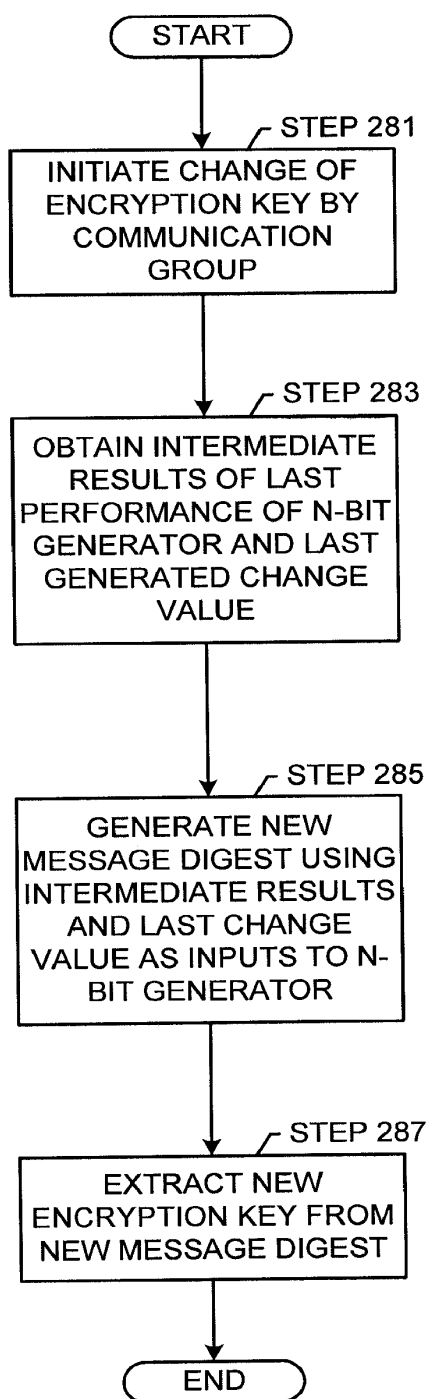
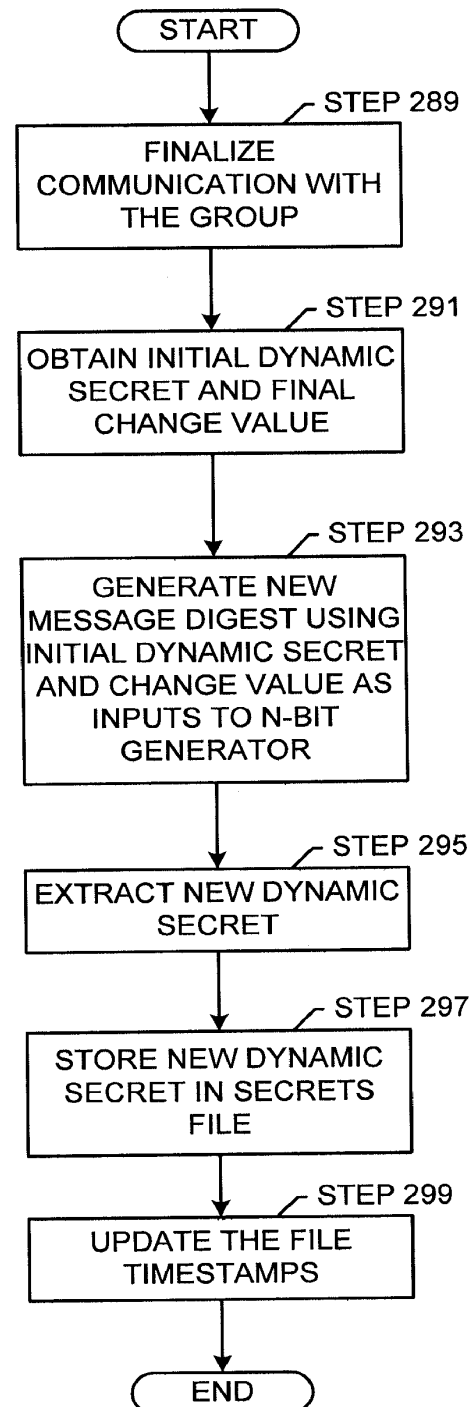
FIG. 2A

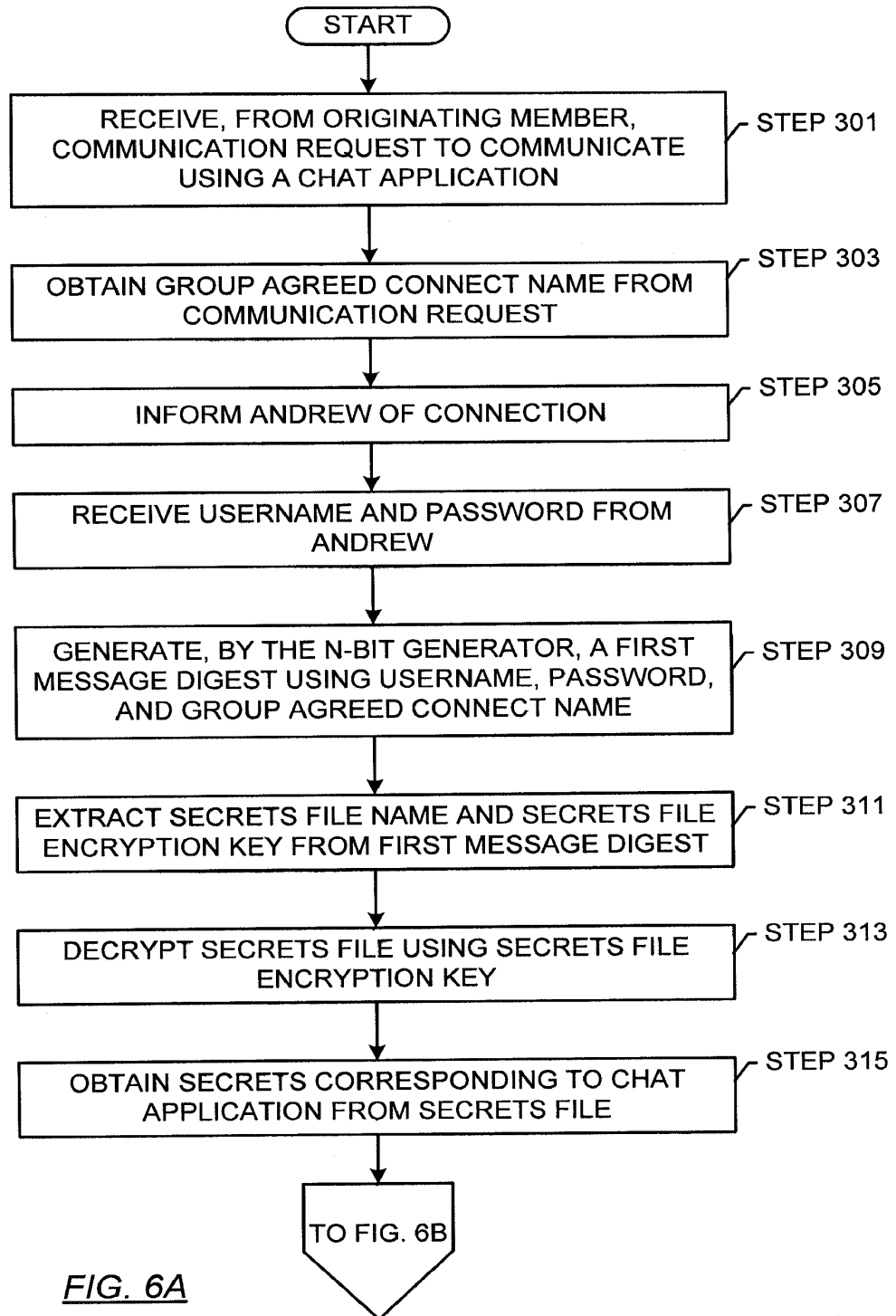
**FIG. 2B**

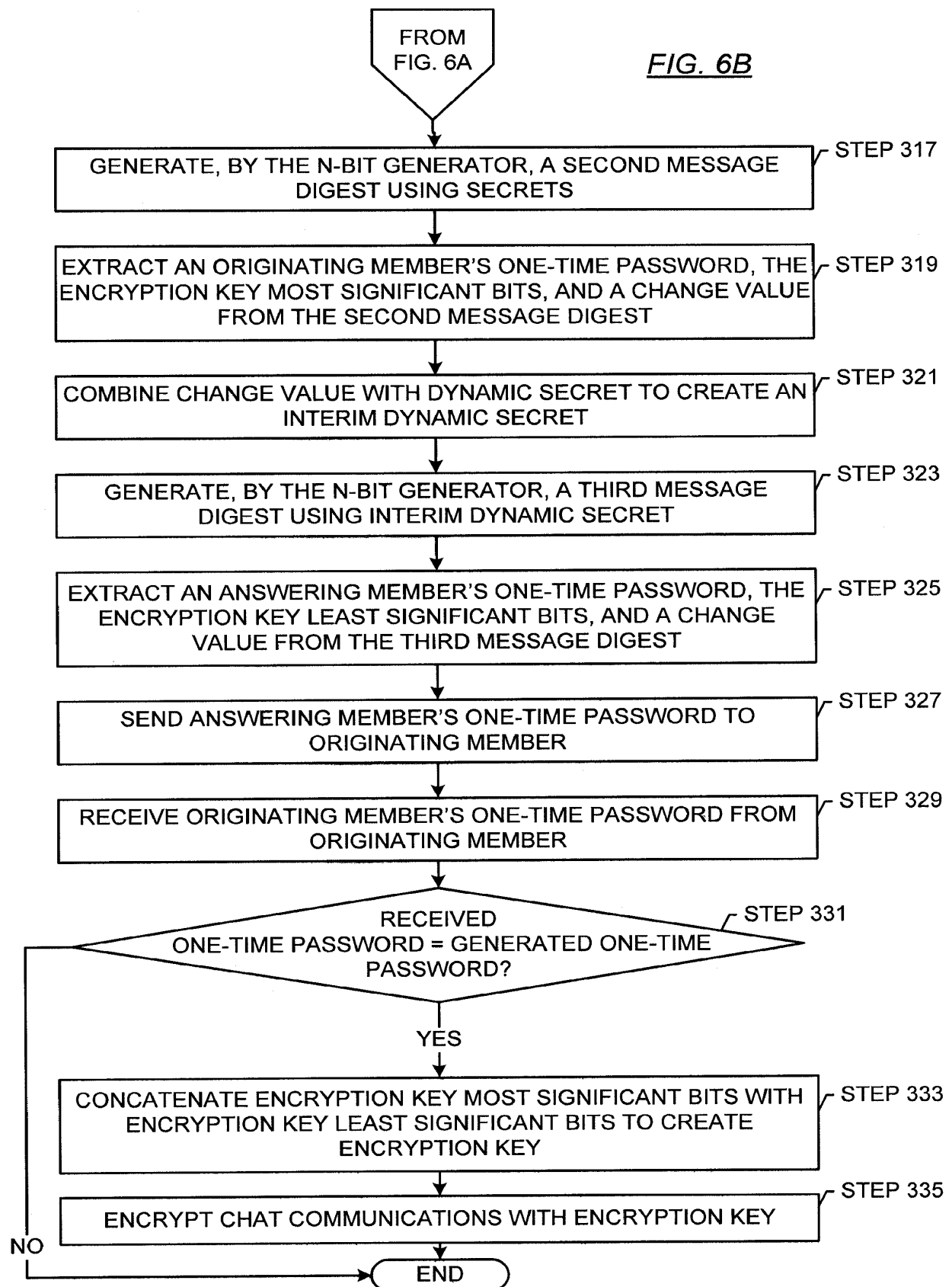
FIG. 3

FIG. 4A

FIG. 4B

FIG. 5AFIG. 5B





350
EXAMPLE SECOND
MESSAGE DIGEST



<u>352</u> ORIGINATING MEMBER ONE TIME PASSWORD	<u>354</u> DISCARD BITS	<u>356</u> SESSION ENCRYPTION KEY MOST SIGNIFICANT BITS (MSB)	<u>358</u> CHANGE VALUE
--	----------------------------	---	-------------------------------

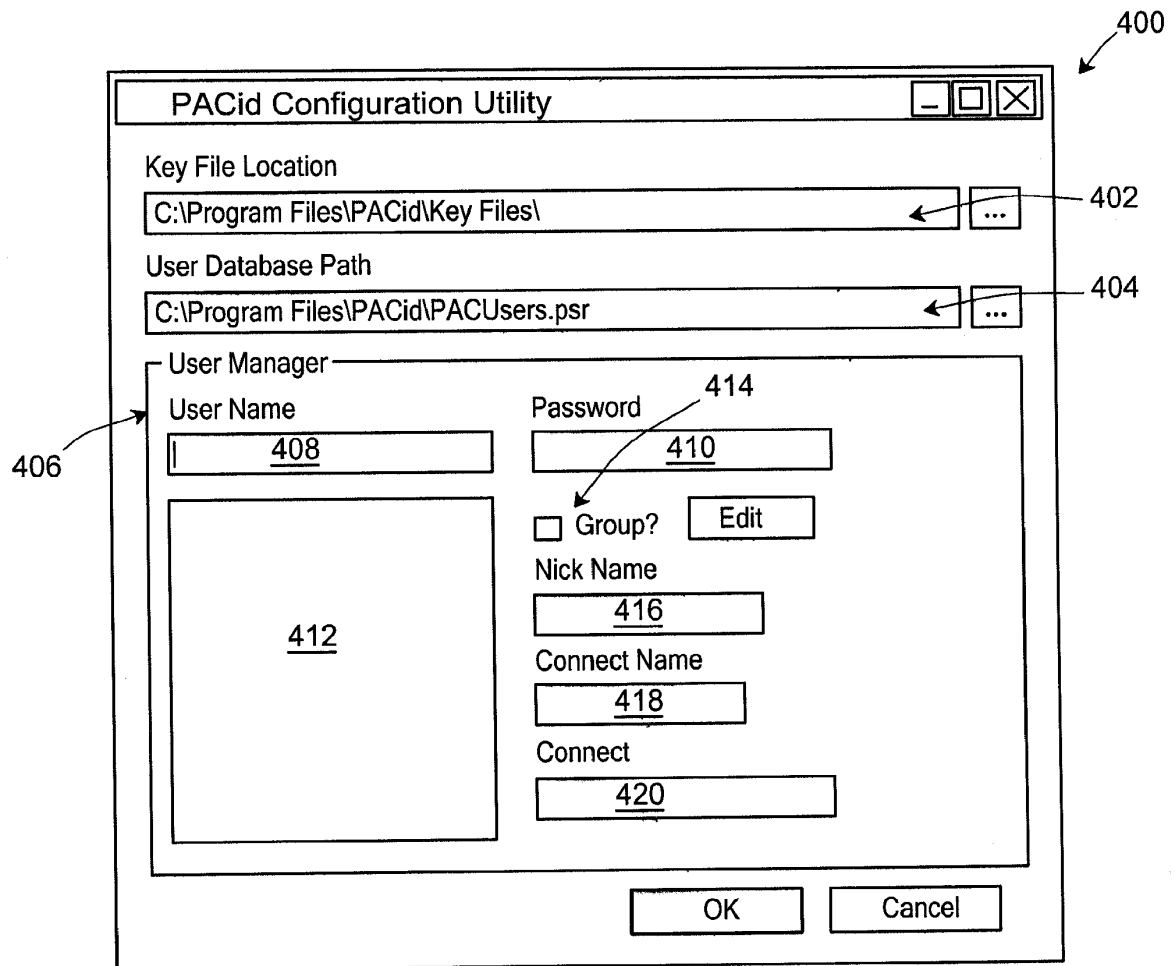
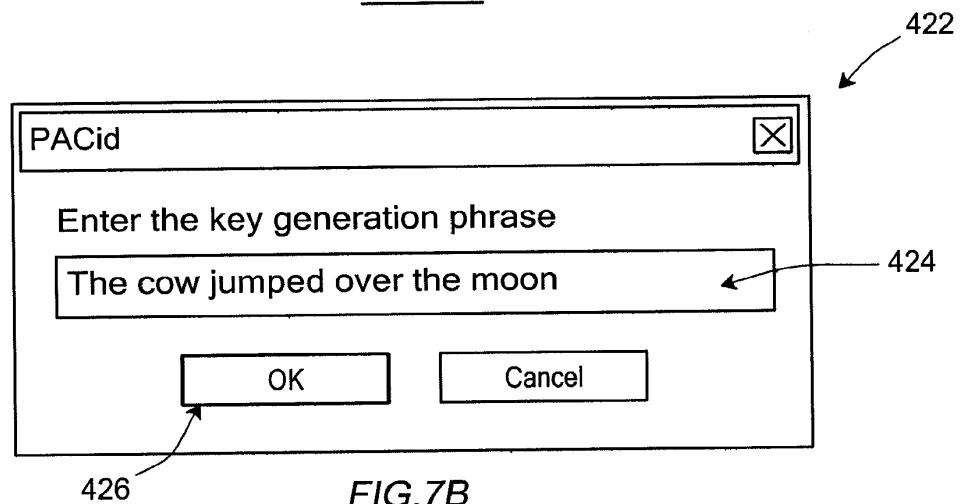
FIG. 6C

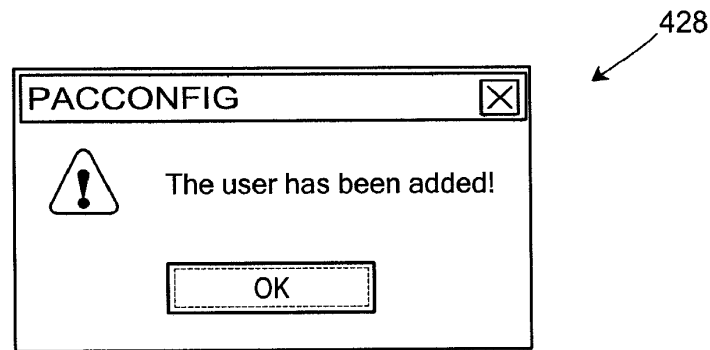
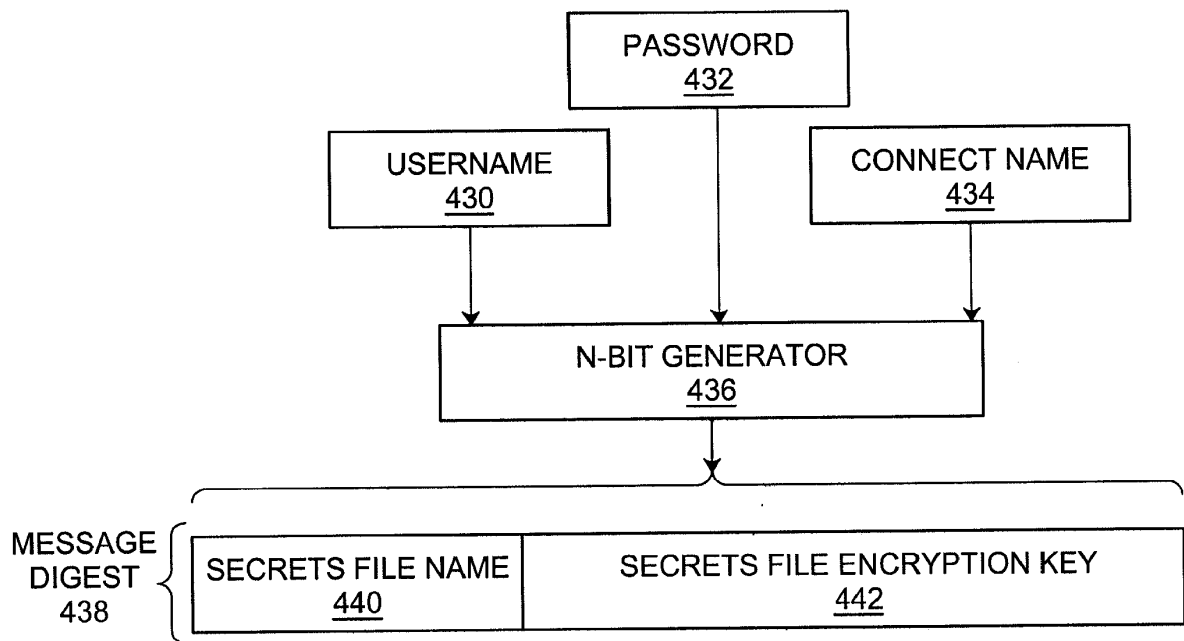
360
EXAMPLE THIRD
MESSAGE DIGEST

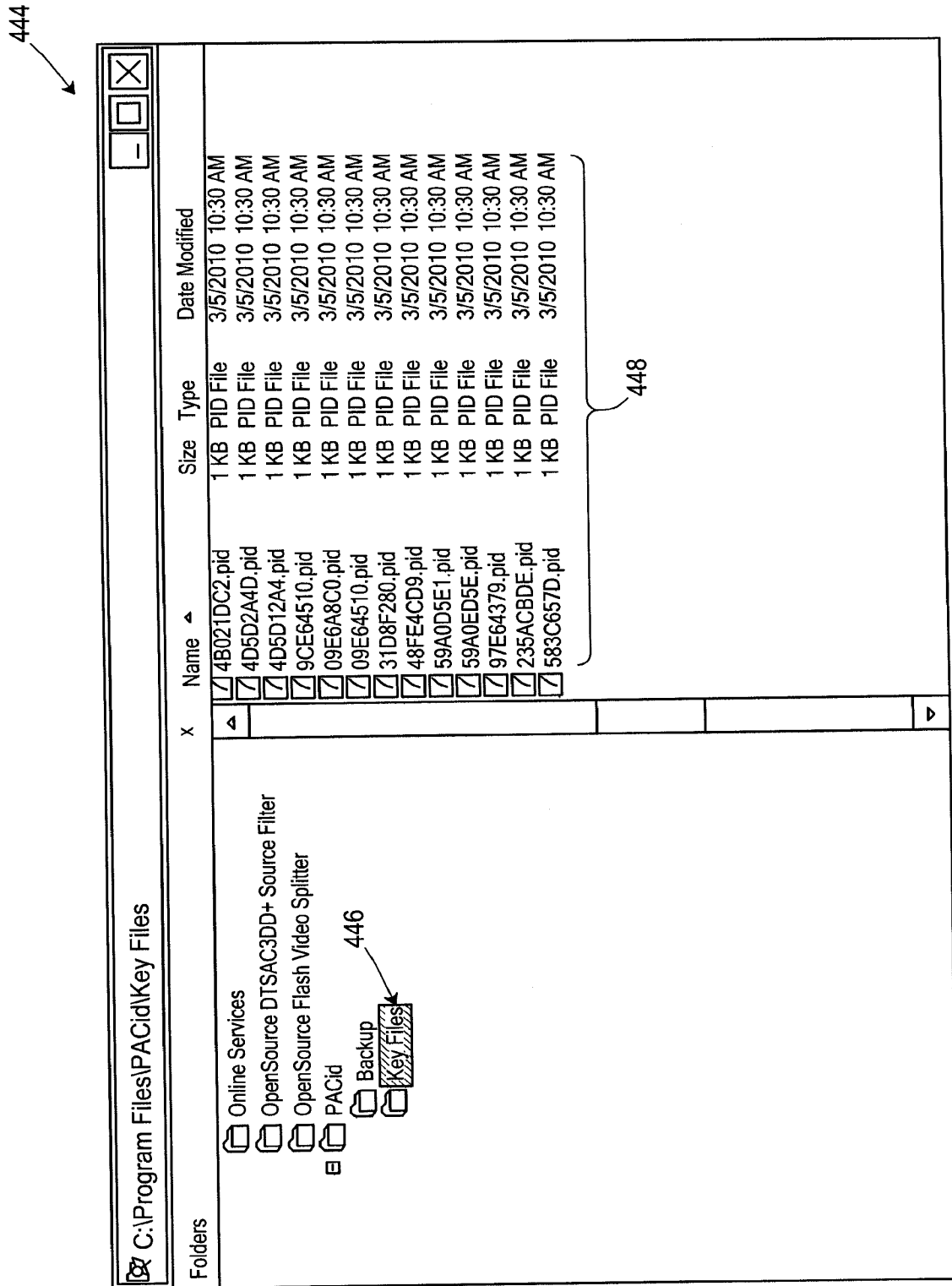


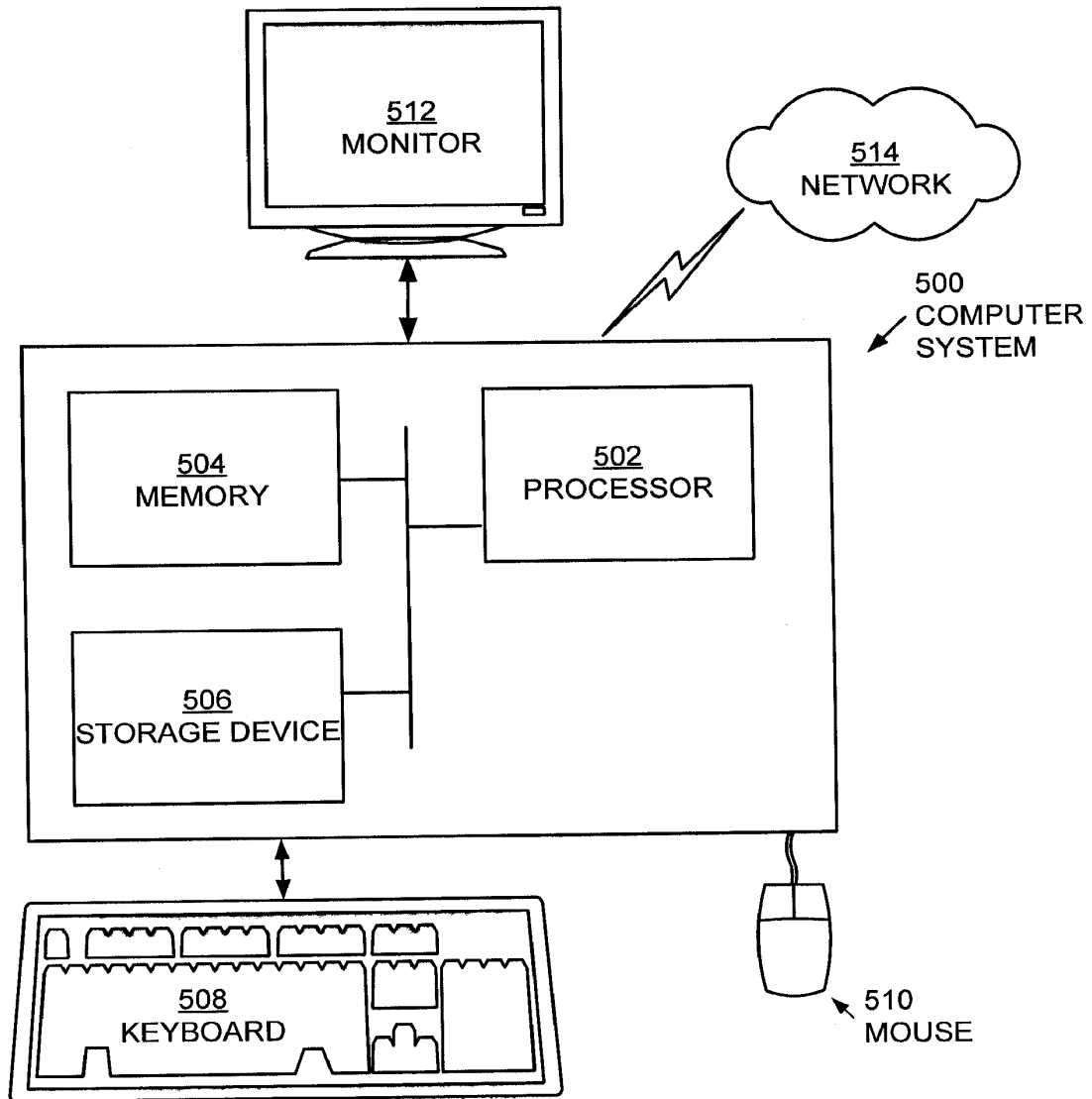
<u>362</u> ANSWERING MEMBER ONE TIME PASSWORD	<u>364</u> DISCARD BITS	<u>366</u> SESSION ENCRYPTION KEY LEAST SIGNIFICANT BITS (LSB)	<u>368</u> CHANGE VALUE
--	----------------------------	--	-------------------------------

FIG. 6D

FIG. 7AFIG. 7B

FIG. 7CFIG. 7D



*FIG. 8*