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
15/977,748	05/11/2018	Mark S. O'Hare	0890103C10D1C2

CONFIRMATION NO. 7200

189503
Security First Innovations, LLC
C/O Farjami & Farjami LLP
26522 La Alameda Ave., Suite 360
Mission Viejo, CA 92691

POA ACCEPTANCE LETTER

OC000000137491266

Date Mailed: 03/06/2023

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 02/15/2023.

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**.

/ylueng/

Google Exhibit 1002
Google v. SFI

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
15/977,748	05/11/2018	Mark S. O'Hare	T00521

CONFIRMATION NO. 7200

33438
TERRILE, CANNATTI & CHAMBERS, LLP
P.O. BOX 203518
AUSTIN, TX 78720

POWER OF ATTORNEY NOTICE

OC000000137491262

Date Mailed: 03/06/2023

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 02/15/2023.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(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**.

/ylueng/

Electronic Acknowledgement Receipt	
EFS ID:	47541457
Application Number:	15977748
International Application Number:	
Confirmation Number:	7200
Title of Invention:	SECURE DATA PARSER METHOD AND SYSTEM
First Named Inventor/Applicant Name:	Mark S. O'Hare
Customer Number:	33438
Filer:	Michael Farjami/Evan Gunderman
Filer Authorized By:	Michael Farjami
Attorney Docket Number:	T00521
Receipt Date:	15-FEB-2023
Filing Date:	11-MAY-2018
Time Stamp:	20:09:37
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		0890103C10D1C2_POA_Feb_15_23.pdf	1160477 1b390f820f3483b1619339c4c8664489627 42681	yes	6

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal Letter	1	1
	Power of Attorney	2	6
Warnings:			
Information:			
	Total Files Size (in bytes):	1160477	

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.

FARJAMI & FARJAMI LLP
AN INTELLECTUAL PROPERTY LAW FIRM
www.farjami.com

26522 La Alameda Avenue, Suite 360
Mission Viejo, California 92691
tel: (949) 282-1000
fax: (949) 282-1002

ELECTRONIC TRANSMISSION COVER SHEET

Date: February 15, 2023

To: United States Patent and Trademark Office
Examiner: Lemma, Samson B.; Art Unit: 2498

Re: **Application Serial No.: 15/977,748**
Filing Date: 5/11/2018; First-Named Inventor: O'Hare
Attorney Docket No.: 0890103C10D1C2

From: Farjami & Farjami LLP

Number of pages including the cover sheet: 6

Message:

Enclosed, please find:

1. Transmittal for Power of Attorney (Form PTO/AIA/82A);
2. Statement Under 37 CFR 3.73(c) (Form PTO/AIA/96); and
3. Power of Attorney Document (Form PTO/AIA/82B)

Authorization is hereby given to the Commissioner to charge any fees associated with this communication or credit any overpayment to Deposit Account **50-0731**.

Thank you.

The documents accompanying this electronic transmission contain PRIVILEGED AND CONFIDENTIAL information intended only for use of the individual or entity named above. If you are not the intended recipient, disclosure, copying, distribution or use of the contents of this electronic transmission information is prohibited. If you have received this electronic transmission in error, please immediately notify us by telephone and return the original electronic transmission to us at the above address via U.S. Postal Service. We will reimburse you for all expenses incurred.

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Attorney Docket No.: 0890103C10D1C2

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: **Security First Innovations, LLC**

Application No./Patent No.: **15/977,748** Filed/Issue Date: **5/11/2018**

Titled: **SECURE DATA PARSER METHOD AND SYSTEM**

Security First Innovations, LLC, a **Limited Liability 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. [X] 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 it's 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 won 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 documents(s) showing the transfer is attached.

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

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

OR

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

1. From: O'Hare, et al. To: SECURITY FIRST CORP.

   The document was recorded in the United States Patent and Trademark Office at Reel 045783, Frame 0985, or for which a copy thereof is attached.

2. From: SECURITY FIRST CORP. To: SECURITY FIRST INNOVATIONS, LLC

   The document was recorded in the United States Patent and Trademark Office at Reel 061262, Frame 0865, or for which a copy thereof is attached.

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

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.

/farshad farjami/	February 15, 2023
Signature	Date
Farshad **Farjami, Esq.**	**41,014**
Printed or Typed Name	Title or Registration Number

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.

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82A (07-13)
Approved for use through 03/31/2021. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	15/977,748
Filing Date	5/11/2018
First Named Inventor	O'Hare
Title	SECURE DATA PARSER METHOD AND SYSTEM
Art Unit	
Examiner Name	
Attorney Docket Number	0890103C10D1C2

SIGNATURE of Applicant or Patent Practitioner

Signature	/Farshad Farjami/	Date (Optional)	2/15/2023
Name	Farshad Farjami	Registration Number	41014
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.

PTO/SB/80 (11-08)
Approved for use through 11/30/2020. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(b).

I hereby appoint:

☑ Practitioners associated with the Customer Number: 189503

OR

☐ Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

as attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(b).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(b) to:

☑ The address associated with Customer Number: 189503

OR

☐ Firm or Individual Name			
Address			
City		State	Zip
Country			
Telephone		Email	

Assignee Name and Address:

Security First Innovations, LLC
44095 Pipeline Plaza, Suite 140
Ashburn, VA 20147

A copy of this form, together with a statement under 37 CFR 3.73(b) (Form PTO/SB/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(b) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature	Leo Guthart	Date	8/30/2020
Name	Mr. Leo Guthart	Telephone	5169460376
Title	Member, Security First Innovations, LLC		

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

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 NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/977,748	11/16/2021	11178116	T00521	7200

33438 7590 10/27/2021

TERRILE, CANNATTI & CHAMBERS, LLP
P.O. BOX 203518
AUSTIN, TX 78720

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

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

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

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

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

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

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

Mark S. O'Hare, Coto De Caza, CA;
Rick L. Orsini, Flower Mound, TX;
Roger S. Davenport, Campbell, TX;
Steven Winick, Roslyn Heights, NY;

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

Security First Corp., Rancho Santa Margarita, CA;

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

IR103 (Rev. 10/09)

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.
15/977,748	05/11/2018	Mark S. O'Hare	T00521	7200

33438 7590 10/20/2021

TERRILE, CANNATTI & CHAMBERS, LLP
P.O. BOX 203518
AUSTIN, TX 78720

EXAMINER	
LEMMA, SAMSON B	

ART UNIT	PAPER NUMBER
2498	

NOTIFICATION DATE	DELIVERY MODE
10/20/2021	ELECTRONIC

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

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

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

USPTO@dockettrak.com
celeste@tcciplaw.com
tmunoz@tcciplaw.com

Response to Rule 312 Communication	Application No.	Applicant(s)	
	15/977,748	O'Hare et al.	
	Examiner	Art Unit	AIA (FITF) Status
	SAMSON B LEMMA	2498	No

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

1. ☑ The amendment filed on 21 June 2021 under 37 CFR 1.312 has been considered, and has been:
   a) ☑ entered.
   b) ☐ entered as directed to matters of form not affecting the scope of the invention.
   c) ☐ disapproved because the amendment was filed after the payment of the issue fee.
      Any amendment filed after the date the issue fee is paid must be accompanied by a petition under 37 CFR 1.313(c)(1) and the required fee to withdraw the application from issue.
   d) ☐ disapproved. See explanation below.
   e) ☐ entered in part. See explanation below.

/SAMSON B LEMMA/
Primary Examiner, Art Unit 2498

REMARKS

The *Present Application* received a Notice of Allowance having a Date Mailed of August, 7, 2020.

A Notice to File Corrected Application Papers ("Notice") having a Date Mailed of September 21, 2020 required corrections to Figures 9 and 48-52b because those Figures did not comply with 37 C.F.R. § 1.84(u)(1).

The relevant portion of 37 C.F.R. § 1.84(u)(1) quoted in the Notice requires:

> 37 CFR 1.84(u)(l) states, "The different views must be numbered in consecutive Arabic numerals, starting with 1 ... Partial views intended to form one complete view, on one or several sheets, must be identified by the same number followed by a capital letter. View numbers must be preceded by the abbreviation 'FIG.' "

Applicant has amended Figures 9 and 48-52b (now Figures 9A, 9B, 48A, 48B, 49A, 49B, 50A, 50B, 51A, 51B, 52A, 52B, 52C, and 52D) to comply with 37 C.F.R. § 1.84(u)(1) as required by the Notice.

Accordingly, Applicant respectfully submits that Applicant has complied with the requirements of the Notice.

Amendment to the Drawings

Figures 9 and 48-52b (now Figures 9A, 9B, 48A, 48B, 49A, 49B, 50A, 50B, 51A, 51B, 52A, 52B, 52C, and 52D) have been amended as indicated in the Replacement Sheets filed herewith.

No new matter has been added.

OK TO ENTER.
10/13/2021.
/S.B.L/

Amendment to the Specification

Paragraphs 0042, 0043, 0080-0084, 0576, 0577, 0582, and 0583 have been amended to correspond with the amended identifiers in the amended drawings.

No new matter has been added.

CONCLUSION

Applicant respectfully submits that all requirements have been met to revive the *Present Application*. Nonetheless, should any issues remain that might be subject to resolution through a telephone interview, the Examiner is requested to telephone the undersigned at 512-338-9100.

CERTIFICATE OF TRANSMISSION

I hereby certify that on June 21, 2021 this correspondence is being transmitted via the U.S. Patent & Trademark Office's electronic filing system.

/Kent B. Chambers/

Respectfully submitted,

/Kent B. Chambers/

Kent B. Chambers
Attorney for Applicant(s)
Reg. No. 38,839

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.
15/977,748	05/11/2018	Mark S. O'Hare	T00521	7200

33438 7590 10/08/2021
TERRILE, CANNATTI & CHAMBERS, LLP
P.O. BOX 203518
AUSTIN, TX 78720

EXAMINER	
LEMMA, SAMSON B	

ART UNIT	PAPER NUMBER
2498	

NOTIFICATION DATE	DELIVERY MODE
10/08/2021	ELECTRONIC

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

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

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

tmunoz@tcciplaw.com
USPTO@dockettrak.com
celeste@tcciplaw.com

Response to Rule 312 Communication	Application No. 15/977,748	Applicant(s)
	Examiner	Art Unit

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

1. ☒ The amendment filed on *25 August 2021* under 37 CFR 1.312 has been considered, and has been:

a) ☒ entered.

b) ☐ entered as directed to matters of form not affecting the scope of the invention.

c) ☐ disapproved because the amendment was filed after the payment of the issue fee.
Any amendment filed after the date the issue fee is paid must be accompanied by a petition under 37 CFR 1.313(c)(1) and the required fee to withdraw the application from issue.

d) ☐ disapproved. See explanation below.

e) ☐ entered in part. See explanation below.

/C. Garner/

Publishing Division

Office of Data Management

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.
15/977,748	05/11 2018	Mark S. O'Hare	T00521	7200

33438 7590 08/25/2021
TERRILE, CANNATTI & CHAMBERS, LLP
P.O. BOX 203518
AUSTIN, TX 78720

EXAMINER
LEMMA, SAMSON B

ART UNIT	PAPER NUMBER
2498	

NOTIFICATION DATE	DELIVERY MODE
08/25/2021	ELECTRONIC

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

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

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

tmunoz@tcciplaw.com
USPTO@dockettrak.com
celeste@tcciplaw.com

UNITED STATES PATENT AND TRADEMARK OFFICE

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

Application No. : 15977748
Applicant : O'Hare
Filing Date : 05/11/2018
Date Mailed : 08/25/2021

NOTICE TO FILE CORRECTED APPLICATION PAPERS

Notice of Allowance Mailed

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

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

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

See attachment(s).

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

/Marty Willis/
Publication Branch
Office of Data Management
(571) 272-4200

Application No. 15977748

IDENTIFICATION OF SPECIFICATION/DRAWING INCONSISTENCIES

☐ On Page of the specification there is a brief description of FIG. , but the drawings filed do not include a drawing with that designation. Applicant must respond either by supplying the omitted drawing or by amending the specification to remove all references to that drawing.

☐ The drawings filed include FIG. , but the specification's brief description of the drawings does not describe a drawing with that designation. Applicant must respond either by amending the specification to add a brief description of that drawing or by correcting the drawings to remove the drawing in question.

☐ In the utility application, drawings are present in the application and are referred to in the detailed description of the invention, but the specification does not contain a brief description of the several views as required by 37 CFR 1.74 and 37 CFR 1.77(b)(9).

☐ The design application does not contain a description of the figure or figures of the drawing as required by 37 CFR 1.153(a) and 37 CFR 1.154(b)(4).

☐ In the plant application, the specification does not contain a brief description of the drawing as required by 37 CFR 1.163(c)(8).

☐ Page of the specification refers to FIG. , but no drawing with that designation is described in the brief description of the drawings and no drawing with that designation is present in the application. Applicant must respond either by amending the specification to remove all references to that drawing, or by supplying that drawing and amending the specification to add a brief description of it.

☐ In the reissue application, FIG. , is labeled as “New” but is not described in the reissue specification’s brief description of the drawings. Applicant must respond by amending the reissue specification’s brief description of the drawings to add a brief description of the new drawing.

☒ OTHER: Please correct and re-submit amended versions of paragraphs [0042] and [0043].

☒ COMMENTS:
Referring to Applicants' 6-21-21 specification amendment, specifically with reference to paragraph [0042] and paragraph [0043]:

Please correct [0042] by deleting all text after "FIGURE" and before "9A".
Please correct [0043] by deleting all text after "FIGURE" and before "9B" .

Electronic Acknowledgement Receipt

EFS ID:	43598934
Application Number:	15977748
International Application Number:	
Confirmation Number:	7200
Title of Invention:	SECURE DATA PARSER METHOD AND SYSTEM
First Named Inventor/Applicant Name:	Mark S. O'Hare
Customer Number:	33438
Filer:	Kent Bryan Chambers/Celeste Scarborough
Filer Authorized By:	Kent Bryan Chambers
Attorney Docket Number:	T00521
Receipt Date:	25-AUG-2021
Filing Date:	11-MAY-2018
Time Stamp:	13:53:19
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	Miscellaneous Incoming Letter	T00521_NtFCAP_2021-08-25.pdf	119937 8b1443fe039ec7fae67bbb9a9c17b60577ad884b	no	3

Warnings:

Information:					
2	Supplemental Response or Supplemental Amendment	T00521_RNtFCAP_2021-08-25.pdf	126948 10b23bb164fd15a47b8c1c1ca09d5e5cd0588dd3	no	3
Warnings:					
Information:					
			Total Files Size (in bytes):	246885	

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/977,748	05/11 2018	Mark S. O'Hare	T00521	7200

33438 7590 08/25/2021
TERRILE, CANNATTI & CHAMBERS, LLP
P.O. BOX 203518
AUSTIN, TX 78720

EXAMINER	
LEMMA, SAMSON B	

ART UNIT	PAPER NUMBER
2498	

NOTIFICATION DATE	DELIVERY MODE
08/25/2021	ELECTRONIC

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

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

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

tmunoz@tcciplaw.com
USPTO@dockettrak.com
celeste@tcciplaw.com

UNITED STATES PATENT AND TRADEMARK OFFICE

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

Application No. : 15977748
Applicant : O'Hare
Filing Date : 05/11/2018
Date Mailed : 08/25/2021

NOTICE TO FILE CORRECTED APPLICATION PAPERS

Notice of Allowance Mailed

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

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

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

See attachment(s).

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

/Marty Willis/
Publication Branch
Office of Data Management
(571) 272-4200

Application No. 15977748

IDENTIFICATION OF SPECIFICATION/DRAWING INCONSISTENCIES

☐ On Page of the specification there is a brief description of FIG. , but the drawings filed do not include a drawing with that designation. Applicant must respond either by supplying the omitted drawing or by amending the specification to remove all references to that drawing.

☐ The drawings filed include FIG. , but the specification's brief description of the drawings does not describe a drawing with that designation. Applicant must respond either by amending the specification to add a brief description of that drawing or by correcting the drawings to remove the drawing in question.

☐ In the utility application, drawings are present in the application and are referred to in the detailed description of the invention, but the specification does not contain a brief description of the several views as required by 37 CFR 1.74 and 37 CFR 1.77(b)(9).

☐ The design application does not contain a description of the figure or figures of the drawing as required by 37 CFR 1.153(a) and 37 CFR 1.154(b)(4).

☐ In the plant application, the specification does not contain a brief description of the drawing as required by 37 CFR 1.163(c)(8).

☐ Page of the specification refers to FIG. , but no drawing with that designation is described in the brief description of the drawings and no drawing with that designation is present in the application. Applicant must respond either by amending the specification to remove all references to that drawing, or by supplying that drawing and amending the specification to add a brief description of it.

☐ In the reissue application, FIG. , is labeled as “New” but is not described in the reissue specification’s brief description of the drawings. Applicant must respond by amending the reissue specification’s brief description of the drawings to add a brief description of the new drawing.

☒ OTHER: Please correct and re-submit amended versions of paragraphs [0042] and [0043].

☒ COMMENTS:
Referring to Applicants' 6-21-21 specification amendment, specifically with reference to paragraph [0042] and paragraph [0043]:

Please correct [0042] by deleting all text after "FIGURE" and before "9A".
Please correct [0043] by deleting all text after "FIGURE" and before "9B" .

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventors:	Mark S O'Hare, Rick L. Orsini, Roger S. Davenport, Steven Winick		
Applicant:	Security First Corp.		
Title:	Secure Data Parser Method and System		
Application No.:	15/977,748	Filed:	May 11, 2018
Confirmation No.	7200		
Examiner:	Lemma, Samson B.	Group Art Unit:	2498
Docket No.:	T00521	Customer No.:	33438

ELECTRONICALLY FILED

Austin, Texas
August 25, 2021

RESPONSE TO NOTICE TO FILE CORRECTED
APPLICATION PAPERS – NOTICE OF ALLOWANCE MAILED

This paper responds to the Notice to File Corrected Application Papers – Notice of Allowance Mailed ("*Notice*"), dated August 25, 2021, having a shortened statutory period expiring October 25, 2021.

The Commissioner is hereby authorized to charge any required, additional fees and credit any overpayments to Deposit Account No. 502264.

AMENDMENT TO THE SPECIFICATION

Please amend ¶0042 as follows:

[0042] FIGURE ~~9, Panel A~~ 9A illustrates a data flow of an enrollment process according to aspects of an embodiment of the invention;

Please amend ¶0043 as follows:

[0043] FIGURE ~~9, Panel B~~ 9B illustrates a flow chart of an interoperability process according to aspects of an embodiment of the invention;

REMARKS

The *Present Application* received a Notice of Allowance having a Date Mailed of August 7, 2020.

A Notice to File Corrected Application Papers ("*Notice*"), having a Date Mailed of August 25, 2021, required corrections to paragraphs [0042] and [0043] of the Specification in compliance with 37 C.F.R. § 1.121.

Applicant has amended paragraphs [0042] and [0043] of the Specification as required by the *Notice*.

Accordingly, Applicant respectfully submits that Applicant has complied with the requirements of the Notice.

Amendment to the Specification

Paragraphs [0042] and [0043] have been amended according to the *Notice*.

No new matter has been added.

CONCLUSION

Applicant has amended the specification in accordance with the requirements of the Notice to File Corrected Application Papers. No new matter has been added.

CERTIFICATE OF TRANSMISSION

I hereby certify that on August 25, 2021 this correspondence is being transmitted via the U.S. Patent & Trademark Office's electronic filing system.

/Kent B. Chambers/

Respectfully submitted,

/Kent B. Chambers/

Kent B. Chambers
Attorney for Applicant(s)
Reg. No. 38,839

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.
15/977,748	05/11/2018	Mark S. O'Hare	T00521	7200

33438 7590 08/11/2021

TERRILE, CANNATTI & CHAMBERS, LLP
P.O. BOX 203518
AUSTIN, TX 78720

EXAMINER	
LEMMA, SAMSON B	

ART UNIT	PAPER NUMBER
2498	

NOTIFICATION DATE	DELIVERY MODE
08/11/2021	ELECTRONIC

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

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

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

USPTO@dockettrak.com
celeste@tcciplaw.com
tmunoz@tcciplaw.com

UNITED STATES PATENT AND TRADEMARK OFFICE

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

In re Application of	:	
O'Hare, et al.	:	
Application No. 15/977,748	:	DECISION ON PETITION
Filed: May 11, 2018	:	
Attorney Docket No. T00521	:	

This is a decision on the petition under 37 CFR 1.137(a), filed June 21, 2021, to revive the above-identified application.

The petition is GRANTED.

The application became abandoned for failure to reply in a timely file a complete reply to the Notice to File Corrected Application Papers (Notice), mailed September 21, 2020. The Notice set a period for reply of two (2) months. No extensions of time under the provisions of 37 CFR 1.136(a) was obtained. Accordingly, the application became abandoned on November 22, 2020. The Office mailed a Notice of Abandonment on February 5, 2021.

The petition satisfies the requirements of 37 CFR 1.137(a) in that petitioner has supplied (1) the reply in the form of replacement sheets for Figure 9, 48-52b, (2) the petition fee of 2100.00, (3) a proper statement of unintentional delay.

An extension of time under 37 CFR 1.136 must be filed prior to the expiration of the maximum extendable period for reply. *See* In re Application of S., 8 USPQ2d 1630, 1631 (Comm'r Pats. 1988). Since the $220.00 extension of time fee submitted on April 7, 2020 was subsequent to the maximum extendable period for reply, this fee is unnecessary and will be credited be to the deposit account.

The application is being forwarded to the Office of Data Management for processing into a patent.

Telephone inquiries concerning this decision should be directed to Paralegal Specialist Debra Wyatt at (571) 272-3621.

/DEBRA WYATT/
Paralegal Specialist, OPET



United States Patent and Trademark Office

Office of the Chief Financial Officer

Document Code:WFEE

User :C48879

Refund Accounting Date:08/10/2021

Effective Date	Sale Item Reference Number	Refund Total
06/21/2021	15977748	$220.00

Document Number	Fee Code	Fee Code Description	Amount Paid	Payment Method	Account Number
I202180C13484097	1251	EXTENSION FOR RESPONSE WITHIN 1ST MONTH	$220.00	Visa	**********6406



United States Patent and Trademark Office

Office of the Chief Financial Officer

Document Code:WFEE

User :C48879

Sale Adjustment Accounting Date:08/10/2021

Effective Date	Sale Accounting Date	Sale Item Reference Number
06/21/2021	08/10/2021	15977748

Document Number	Fee Code	Fee Code Description	Amount Paid	Payment Method
I202180C13484097	1251	EXTENSION FOR RESPONSE WITHIN 1ST MONTH	$220.00	Visa

PTO/AIA/01 (06-12)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

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

Title of Invention	Secure Data Parser Method and System

As the below named inventor, I hereby declare that:

This declaration is directed to:

☐ The attached application, or

■ United States application or PCT international application number 15/977,748 filed on May 11, 2018.

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: Rick L. Orsini Date (Optional) :

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.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Privacy Act Statement

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

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

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

Electronic Acknowledgement Receipt

EFS ID:	43046015
Application Number:	15977748
International Application Number:	
Confirmation Number:	7200
Title of Invention:	SECURE DATA PARSER METHOD AND SYSTEM
First Named Inventor/Applicant Name:	Mark S. O'Hare
Customer Number:	33438
Filer:	Kent Bryan Chambers/Celeste Scarborough
Filer Authorized By:	Kent Bryan Chambers
Attorney Docket Number:	T00521
Receipt Date:	21-JUN-2021
Filing Date:	11-MAY-2018
Time Stamp:	19:17:52
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	Oath or Declaration filed	Declaration_Orsini_15977748.pdf	1517030 fe5e8962047132c662fd79ba1e7d0f0ef1352f28	no	2

Warnings:

Information:	
Total Files Size (in bytes):	1517030

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

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

Doc Code: PET.OP
Document Description: Petition for Review by the Office of Petitions

PTO/SB/64 (01-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR REVIVAL OF AN APPLICATION FOR PATENT ABANDONED UNINTENTIONALLY UNDER 37 CFR 1.137(a) Page 1 of 2	Docket Number (Optional) T00521

First named inventor: Mark S. O'Hare

Application No.: 15/977,748 Art Unit: 2498

Filed: 05/11/2018 Examiner: Lemma, Samson B.

Title: SECURE DATA PARSER METHOD AND SYSTEM

Attention: Office of Petitions
Mail Stop Petition
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450
FAX (571) 273-8300

NOTE: If information or assistance is needed in completing this form, please contact the Office of Petitions at (571) 272-3282.

The above-identified application became abandoned for failure to file a timely and proper reply to a notice or action by the United States Patent and Trademark Office. The date of abandonment is the day after the expiration date of the period set for reply in the Office notice or action plus any extensions of time actually obtained.

APPLICANT HEREBY PETITIONS FOR REVIVAL OF THIS APPLICATION.

NOTE: A grantable petition requires the following items:

(1) Petition fee;
(2) Reply and/or issue fee;
(3) Terminal disclaimer with disclaimer fee – required for all utility and plant applications filed before June 8, 1995, and for all design applications; and
(4) Statement that the entire delay was unintentional.

1. **Petition fee**

☐ Small entity fee $ _____ (37 CFR 1.17(m)). Applicant asserts small entity status. See 37 CFR 1.27.

☐ Micro entity fee $ _____ (37 CFR 1.17(m)). Applicant certifies micro entity status. See 37 CFR 1.29. Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☒ Undiscounted fee $ 2,100 (37 CFR 1.17(m)).

2. **Reply and/or fee**

A The reply and/or fee to the above-noted Office notice or action in the form of

REPLY TO NOTICE TO FILE CORRECTED APPLICATION PAPERS (identify the type of reply):

☐ has been filed previously on _____.

☒ is enclosed herewith.

B The issue fee and publication fee (if applicable) of $ 1,000

☒ has been paid previously on November 3, 2020.

☐ is enclosed herewith.

This collection of information is required by 37 CFR 1.137(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, 1.14 and 41.6. 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: Mail Stop Petition, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Doc Code: PET.OP
Document Description: Petition for Review by the Office of Petitions

PTO/SB/64 (01-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR REVIVAL OF AN APPLICATION FOR PATENT ABANDONED UNINTENTIONALLY UNDER 37 CFR 1.137(a)

3. **Terminal disclaimer with disclaimer fee**

☒ Since this utility/plant application was filed on or after June 8, 1995, no terminal disclaimer is required.

☐ A terminal disclaimer (and disclaimer fee (37 CFR 1.20(d)) of $ _____) disclaiming the required period of time is enclosed herewith (see PTO/SB/63).

4. **STATEMENT:** The entire delay in filing the required reply from the due date for the required reply until the filing of a grantable petition under 37 CFR 1.137(a) was unintentional. [NOTE: The United States Patent and Trademark Office may require additional information if there is a question as to whether either the abandonment or the delay in filing a petition under 37 CFR 1.137(a) was unintentional (MPEP 711.03(c), subsections (III)(C) and (D)).]

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.

/Kent B. Chambers/	June 20, 2021
Signature	Date
Kent B. Chambers	38,839
Typed or Printed Name	Registration Number, if applicable
11675 Jollyville Road, Suite 100	512-338-9100
Address	Telephone Number
Austin, TX 78759	
Address	

Enclosures:

☒ Fee Payment

☒ Reply

☐ Terminal Disclaimer Form

☐ Additional sheet(s) containing statements establishing unintentional delay

☐ Other: _____

CERTIFICATE OF MAILING OR TRANSMISSION [37 CFR 1.8(a)]

I hereby certify that this correspondence is being:

☐ Deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop Petition, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450.

☐ Transmitted by facsimile on the date shown below to the United States Patent and Trademark Office at (571) 273-8300.

Date	Signature
	Typed or printed name of person signing certificate

Privacy Act Statement

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

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

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

PTO/AIA/22 (10-20)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)	Docket Number (Optional) T00521
Application Number 15/977,748	Filed May 11, 2018
For Secure Data Parser Method and System	
Art Unit 2498	Examiner Samson B. Lemma

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

		Fee	Small Entity Fee	Micro Entity Fee	
☑	One month (37 CFR 1.17(a)(1))	$220	$110	$55	$ 220
☐	Two months (37 CFR 1.17(a)(2))	$640	$320	$160	$
☐	Three months (37 CFR 1.17(a)(3))	$1,480	$740	$370	$
☐	Four months (37 CFR 1.17(a)(4))	$2,320	$1,160	$580	$
☐	Five months (37 CFR 1.17(a)(5))	$3,160	$1,580	$790	$

☐ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 502264.

☑ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant.

☑ attorney or agent of record. Registration number 38,839.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/Kent B. Chambers/ — Signature

June 21, 2021 — Date

Kent B. Chambers — Typed or printed name

512.338.9100 — Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☑ * Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.136(a). 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 6 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: Mail Stop PCT, 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 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 NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/977,748	05/11/2018	Mark S. O'Hare	104093-0002-118	7200

15314 7590 09/21/2020

Haley Guiliano LLP (S&L)
75 Broad Street
Suite 1000
New York, NY 10004-3226

EXAMINER	
LEMMA, SAMSON B	

ART UNIT	PAPER NUMBER
2498	

NOTIFICATION DATE	DELIVERY MODE
09/21/2020	ELECTRONIC

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

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

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

hgpatentdocket@hglaw.com
haleyguiliano_PAIR@firsttofile.com

PTOL-90A (Rev. 04/07)

UNITED STATES PATENT AND TRADEMARK OFFICE

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

Application No. : 15977748
Applicant : O'Hare
Filing Date : 05/11/2018
Date Mailed : 09/21/2020

NOTICE TO FILE CORRECTED APPLICATION PAPERS

Notice of Allowance Mailed

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

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

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

See attachment(s).

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

/Naran Hem/
Publication Branch
Office of Data Management
(571) 272-4200

Application No. 15977748 **Drawings filed: 05/11/2018**

DRAWINGS AND BRIEF DESCRIPTION OF DRAWINGS IN NON-COMPLIANCE WITH 37 CFR 1.84(u)(1)

37 CFR 1.84(u)(1) states, "The different views must be numbered in consecutive Arabic numerals, starting with 1 … Partial views intended to form one complete view, on one or several sheets, must be identified by the same number followed by a capital letter. View numbers must be preceded by the abbreviation 'FIG.' "

Other methods of identification are improper, including Roman numerals (FIG. I, FIG, II, etc.) and alphabetic characters (FIG. A, FIG. B, etc.). Abbreviations and words other than "FIG." ("Illustration, 1" "Diagram 2," "Photo 3," etc.) are improper.

☐ Applicant must submit drawings that number the views using consecutive Arabic numerals.

☐ Applicant must amend the brief description of the drawings on Page(s) of the specification to show consecutive Arabic numerals.

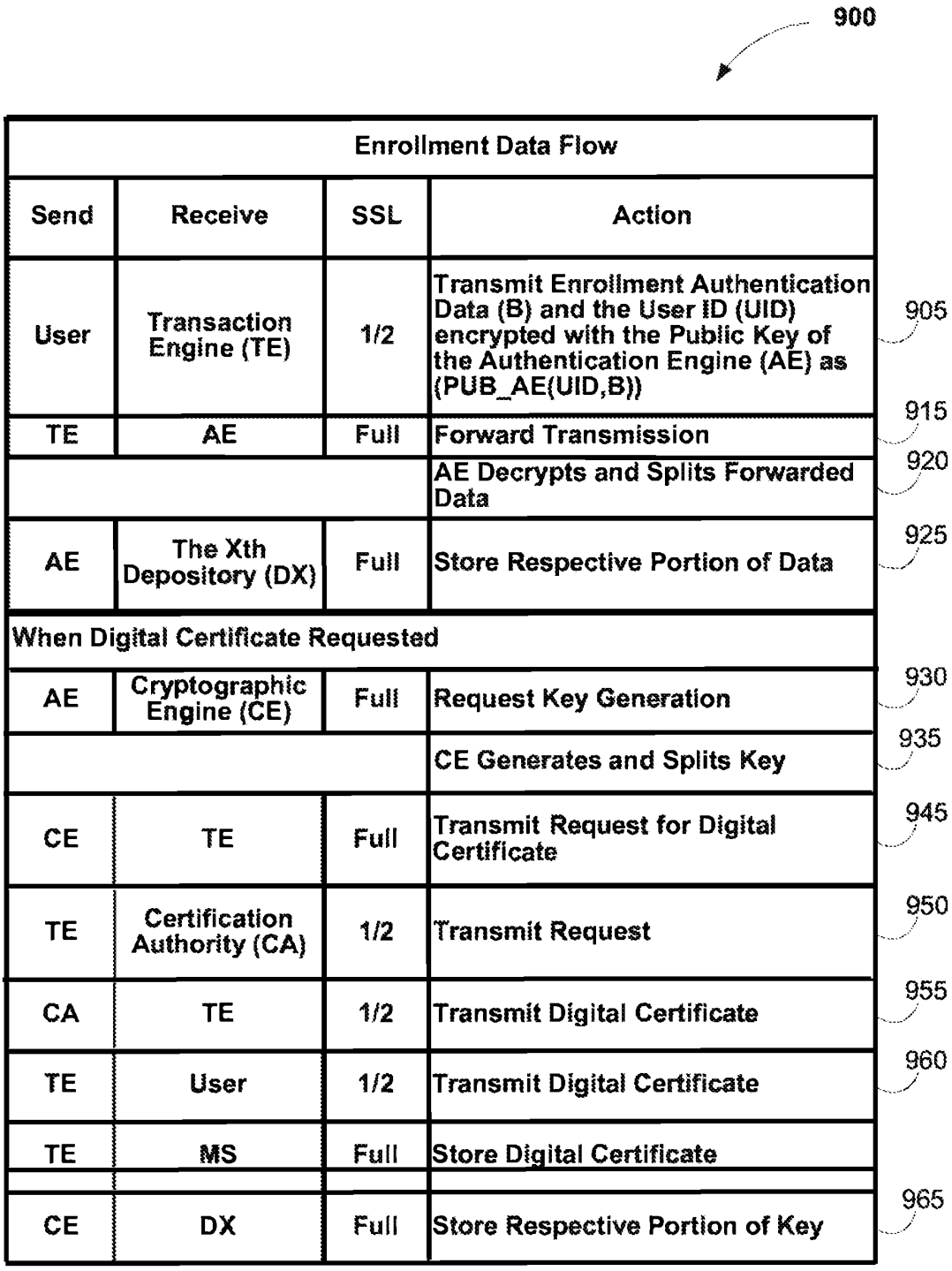
NOTE: Applicant is advised that the detailed description may voluntarily be amended to identify the drawings by Arabic numerals.

☒ The drawing is continued onto a second page (or more) without proper labeling under 37 CFR 1.84(u)(1). FIG(s) **9, 48-52b**

☐ Applicant must submit drawings on which the view numbers are preceded by the abbreviation "FIG."

☐ Applicant must amend the brief description of the drawings on Page(s) of the specification to show view numbers preceded by the abbreviation "FIG."

NOTE: Applicant is advised that the detailed description may voluntarily be amended to show view numbers preceded by the abbreviation "FIG."



Enrollment Data Flow			
Send	**Receive**	**SSL**	**Action**
User	Transaction Engine (TE)	1/2	Transmit Enrollment Authentication Data (B) and the User ID (UID) encrypted with the Public Key of the Authentication Engine (AE) as (PUB_AE(UID,B))
TE	AE	Full	Forward Transmission
			AE Decrypts and Splits Forwarded Data
AE	The Xth Depository (DX)	Full	Store Respective Portion of Data
When Digital Certificate Requested			
AE	Cryptographic Engine (CE)	Full	Request Key Generation
			CE Generates and Splits Key
CE	TE	Full	Transmit Request for Digital Certificate
TE	Certification Authority (CA)	1/2	Transmit Request
CA	TE	1/2	Transmit Digital Certificate
TE	User	1/2	Transmit Digital Certificate
TE	MS	Full	Store Digital Certificate
CE	DX	Full	Store Respective Portion of Key

FIG. 9A

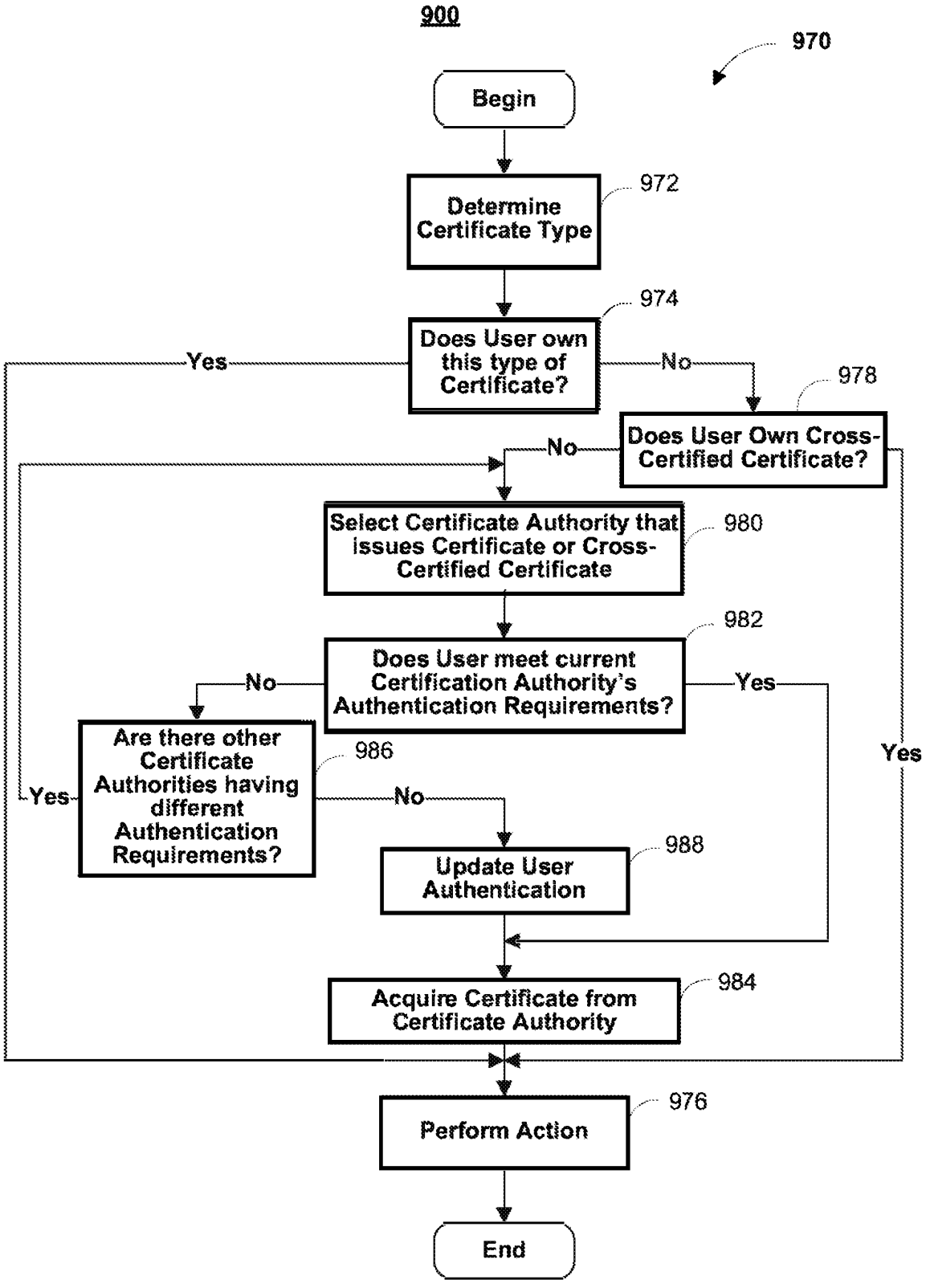

900
970
Begin
Determine Certificate Type
972
Does User own this type of Certificate?
974
Yes
No
Does User Own Cross-Certified Certificate?
978
No
Yes
Select Certificate Authority that issues Certificate or Cross-Certified Certificate
980
Does User meet current Certification Authority's Authentication Requirements?
982
No
Yes
Are there other Certificate Authorities having different Authentication Requirements?
986
Yes
No
Update User Authentication
988
Acquire Certificate from Certificate Authority
984
Perform Action
976
End

FIG. 9B

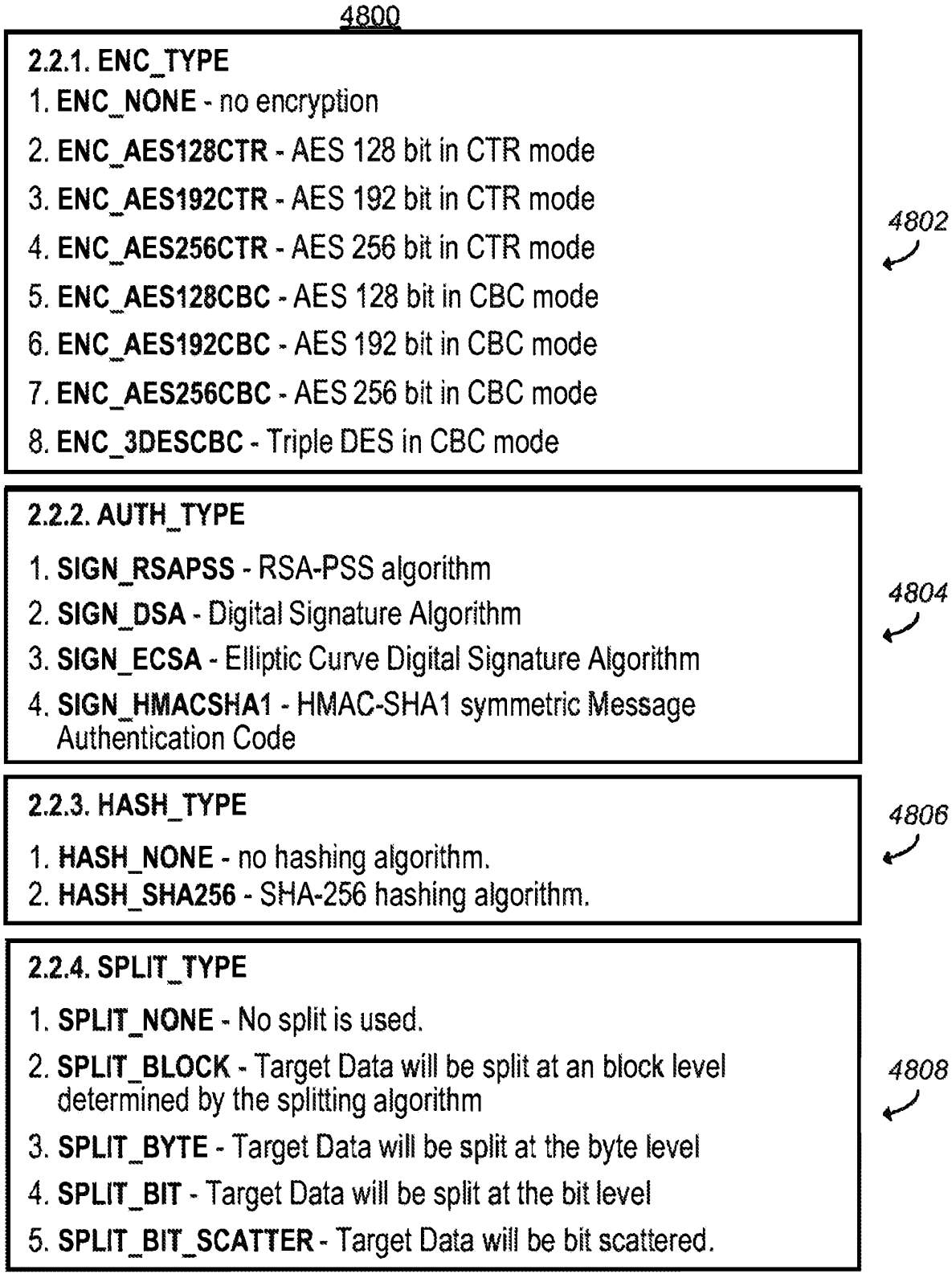

4800
2.2.1. ENC_TYPE
1. ENC_NONE - no encryption
2. ENC_AES128CTR - AES 128 bit in CTR mode
3. ENC_AES192CTR - AES 192 bit in CTR mode
4. ENC_AES256CTR - AES 256 bit in CTR mode
5. ENC_AES128CBC - AES 128 bit in CBC mode
6. ENC_AES192CBC - AES 192 bit in CBC mode
7. ENC_AES256CBC - AES 256 bit in CBC mode
8. ENC_3DESCBC - Triple DES in CBC mode
4802
2.2.2. AUTH_TYPE
1. SIGN_RSAPSS - RSA-PSS algorithm
2. SIGN_DSA - Digital Signature Algorithm
3. SIGN_ECSA - Elliptic Curve Digital Signature Algorithm
4. SIGN_HMACSHA1 - HMAC-SHA1 symmetric Message Authentication Code
4804
2.2.3. HASH_TYPE
1. HASH_NONE - no hashing algorithm.
2. HASH_SHA256 - SHA-256 hashing algorithm.
4806
2.2.4. SPLIT_TYPE
1. SPLIT_NONE - No split is used.
2. SPLIT_BLOCK - Target Data will be split at an block level determined by the splitting algorithm
3. SPLIT_BYTE - Target Data will be split at the byte level
4. SPLIT_BIT - Target Data will be split at the bit level
5. SPLIT_BIT_SCATTER - Target Data will be bit scattered.
4808

FIG. 48A

2.2.5. KEY_TYPE

1. **KEY_SYM** (keys for all symmetric algorithms)
2. **KEY_RSAPUB**
3. **KEY_RSAPRI**
4. **KEY_DSAPUB**
5. **KEY_DSAPRI**
6. **KEY_ECDSAPUB**
7. **KEY_ECDSAPRI**

4810

2.2.6. ERROR_TYPE

1. **ERROR_NONE** - No error
2. **ERROR_NO_MASTER_KEY** - No master key, can not continue.
3. **ERROR_INVALID_CALLBACK** - An invalid callback was registered
4. **ERROR_INVALID_METHOD** - An invalid parse split method occurred.
5. **ERROR_NO_TARGET** - No target was set to parse.
6. **ERROR_NO_TARGET_LENGTH** - Target buffer has no length
7. **ERROR_NOT_ENOUGH_SHARES** - Unable to restore, not enough shares are present.
8. **ERROR_INVALID_SHARE** - An invalid share was set
9. **ERROR_INVALID_KEY** - An invalid key was set
10. **ERROR_INTEGRITY_CHECK** - An integrity check failure occurred
11. **ERROR_NO_MEMORY** - Out of memory

4812

FIG. 48B

4900

4902

Name	Type	Description
originalShare	Share	stores the original unsplit data.
shares	Share []	an array of Share data structures of size MAX_SHARE_COUNT.
shareCount	int	actual number of shares used.
splitEncContext	EncContext *	buffer holding pre-encryption context between calls to doSplit and doRestore.
finalFlag	int	indicates that the final call to doSplit or doRestore will be made next (default = 0).

4904

Name	Type	Description
L	int	total number of mandatory shares (default = 0).
N	int	total number of non-mandatory shares (default = 0).
M	int	total number of non-mandatory shares needed for recovery (default = 0).
splitType	SPLIT_TYPE	the split algorithm to use (default = NONE).
splitEncMode	ENC_TYPE	the encryption mode to use during the split (default = NONE).
preEncMode	ENC_TYPE	the pre-encryption mode to use (default = NONE).
postEncMode	ENC_TYPE	the post-encryption mode to use (default = NONE).
splitHashMode	HASH_TYPE	the hash mode to use (default = HASH_SHA256).
preAuthMode	AUTH_TYPE	the pre-signing mode to use (default = NONE).
postAuthMode	AUTH_TYPE	the post-signing mode to use (default = NONE).
preEncKey	char *	handle for the pre-encryption key (default = NONE).
postEncKey	char *	handle for the post-encryption key (default = NONE).
preAuthKey	char *	handle for the pre-signature key (default = NONE).
postAuthKey	char *	handle for the post-signature key (default = NONE).
maxOrigBufSize	int	max size for the original buffer (default = MAX_ORIG_BUF_SIZE).
maxShareBufSize	int	max size for each share buffer (default = MAX_SHARE_BUF_SIZE).

FIG. 49A

4906

Name	Type	Description
id	char *	unique identifier for this key.
idLen	int	length of buffer holding id.

4908

Name	Type	Description
data	uint8 *	key share data for this share.
dataLen	int	length of data (in bits) of data buffer.

4910

Name	Type	Description
keyId	KeyId	unique identifier for this key.
type	KEY_TYPE	type of key that this.
data	uint8 *	pointer to the buffer holding the key data.
dataLen	int	length of the buffer holding the key data.

4912

Name	Type	Description
data	uint8 *	data buffer for this share.
dataLen	int	length indicating the amount of data found in this share.
encContext	EncContext	data buffer storing the encryption context between calls to doSplit and doRestore.
authContext	SigContext	data buffer storing the authentication context between calls to doSplit and doRestore.
hashContext	HashContext	data buffer storing the hash context between calls to doSplit and doRestore.

FIG. 49B

5002 ↘ 5000

Name	Type	Description
encMode	ENC_TYPE	the type of encryption being used.
...	Union	various types of encryption contexts can be placed here.

5004 ↘

Name	Type	Description
encKeyId	KeyId	unique identifier of the encryption key to use for this context.
currentIV	uint8 *	the current IV being stored for this context.
currentIdLen	int	the length of the current IV in bytes.

5006 ↘

Name	Type	Description
encKeyId	KeyId	unique identifier of the encryption key to use for this context.
currentIV	uint8 *	the current IV being stored for this context.
currentIVLen	int	the length of the current IV in bytes.

5008 ↘

Name	Type	Description
authMode	AUTH_TYPE	the type of authentication being used.
...	Union	various types of authentication contexts can be placed here.

5020 ↘

Name	Type	Description
hashContext	openSSL?	Pointer to the OpenSSL hash context data type.

FIG. 50A

5010

Name	Type	Description
pubKeyId	KeyId	unique identifier of the public key to use for this context.
privKeyId	KeyId	unique identifier of the private key to use for this context.
hashContext	openSSL?	Pointer to the OpenSSL hash context data type.

5012

Name	Type	Description
pubKeyId	KeyId	unique identifier of the public key to use for this context.
privKeyId	KeyId	unique identifier of the private key to use for this context.
hashContext	openSSL?	Pointer to the OpenSSL hash context data type.

5014

Name	Type	Description
pubKeyId	KeyId	unique identifier of the public key to use for this context.
privKeyId	KeyId	unique identifier of the private key to use for this context.
hashContext	openSSL?	Pointer to the OpenSSL hash context data type.

5016

Name	Type	Description
macContext	openSSL?	Pointer to the OpenSSL mac context data type.

5018

Name	Type	Description
hashMode	HASH_TYPE	the type of hashing being used.
...	Union	various types of hashing contexts can be placed here.

FIG. 50B

5100

Share Data
\n----- BEGIN POST-ENC KEY ID -----\n
post-encryption key id
\n----- END POST-ENC KEY ID -----\n
\n----- BEGIN POST-SIG KEY ID -----\n
post-signature key id
\n----- END POST-SIG KEY ID -----\n
\n----- BEGIN POST-ENC HEADER -----\n
post-encrypted header
\n----- END POST-ENC HEADER -----\n
\n----- BEGIN POST-ENC DATA -----\n
post-encrypted data
\n----- END POST-ENC DATA-----\n
\n----- BEGIN POST-ENC FOOTER -----\n
post-encrypted footer
\n----- END POST-ENC FOOTER -----\n
\n----- BEGIN POST-SIG DATA -----\n
post-signature data
\n----- END POST-SIG DATA-----\n

5102

Encrypted footer
\n----- BEGIN SPLIT-HASH DATA -----\n
split-hash data
\n----- END SPLIT-HASH DATA -----\n
\n----- BEGIN PRE-SIG DATA -----\n
pre-signature data
\n----- END PRE-SIG DATA -----\n

5108

FIG. 51A

Post-encrypted footer
\n----- BEGIN ENCRYPTED FOOTER -----\n
encrypted footer
\n----- END ENCRYPTED FOOTER -----\n

5104

Post-encrypted header
\n----- BEGIN HEADER -----\n
Key share (len):key share information\n
Share id (2):share ID\n
L (2):L\n
M (2):M\n
N (2):N\n
Split mode (1):split mode\n
Split-encryption key (len):split-encryption key id\n
Split-encryption IV (len):split-encryption IV data\n
Split-hash mode (1):split-hash mode\n
Original buffer (4):original buffer size\n
Share buffers (4):share buffer size\n
Pre-encryption key (len):pre-encryption key id\n
Pre-signature key (len):pre-signature key id\n
\n----- END HEADER -----\n

5106

FIG. 51B

5200

parser_createParser 5202
Parameters none
Returns Parser *p
Description Allocates the SecureParser context, and sets default values.

parser_destroyParser 5204
Parameters Parser *p
Returns void
Description Destroys the SecureParser context, including parser parameter objects and share buffers.

parser_createKey 5206
Parameters char *id
uint8 *data
size_t length
KEYTYPE type
Returns Key *k
Description Constructs the structure **k** for use with the parser from the unique id, key data buffer, length indicater and key type given.

parser_destroyKey 5208
Parameters Key *k
Returns *none*
Description Destroys the key pointed to by k. Note: Do not destroy a key currently in use with the Parser.

parser_createShare 5210
Parameters int length
Key *encKey
Key *authKey
HASH_MODE h
Returns Share *s
Description Constructs a Share data structure based on the given length, the encryption key type, authentication key type and hash mode.

FIG. 52A

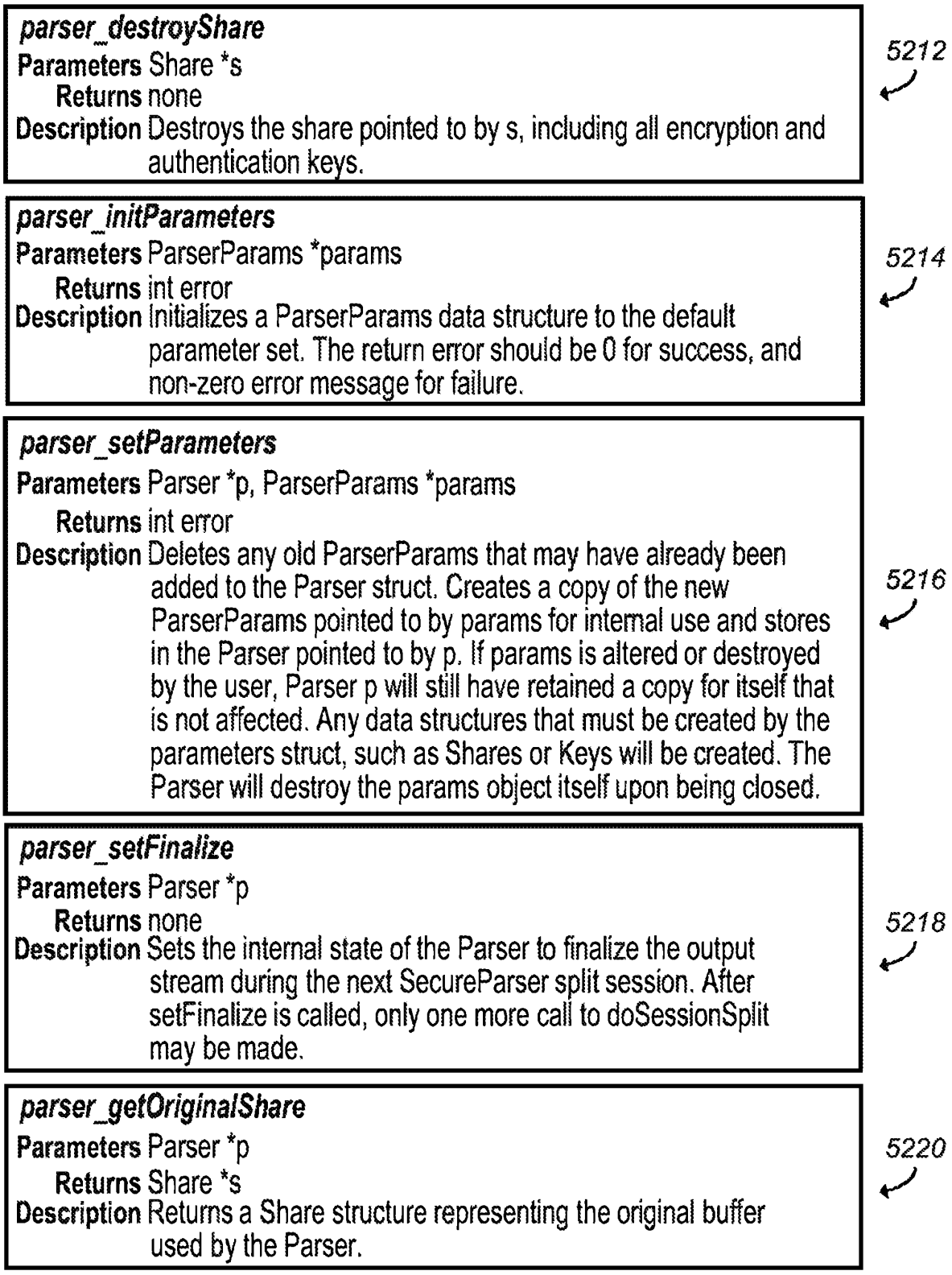

parser_destroyShare
Parameters Share *s
Returns none
Description Destroys the share pointed to by s, including all encryption and authentication keys.
5212
parser_initParameters
Parameters ParserParams *params
Returns int error
Description Initializes a ParserParams data structure to the default parameter set. The return error should be 0 for success, and non-zero error message for failure.
5214
parser_setParameters
Parameters Parser *p, ParserParams *params
Returns int error
Description Deletes any old ParserParams that may have already been added to the Parser struct. Creates a copy of the new ParserParams pointed to by params for internal use and stores in the Parser pointed to by p. If params is altered or destroyed by the user, Parser p will still have retained a copy for itself that is not affected. Any data structures that must be created by the parameters struct, such as Shares or Keys will be created. The Parser will destroy the params object itself upon being closed.
5216
parser_setFinalize
Parameters Parser *p
Returns none
Description Sets the internal state of the Parser to finalize the output stream during the next SecureParser split session. After setFinalize is called, only one more call to doSessionSplit may be made.
5218
parser_getOriginalShare
Parameters Parser *p
Returns Share *s
Description Returns a Share structure representing the original buffer used by the Parser.
5220

FIG. 52B

5200

parser_getShare
Parameters Parser *p,
int ShareID
Returns Share *s
Description Returns a Share containing the Share structure for the Share matching the given ShareID.

5222

parser_doSplit
Parameters Parser *p
Returns int error
Description Performs the SecureParser split. This action treats data that is in the target buffer as input and places split data that is output into buffers for each Share. A return value of 0 indicates success, otherwise a failure has occurred and the error is returned. If setFinalize has been called, this must be the last

5224

parser_doRestore
Parameters Parser *p
Returns int error
Description Performs the SecureParser restore. This action treats all data in share buffers as input and places output data (the reconstructed original data) into the target buffer. A return value of 0 indicates success, otherwise a failure has occured and the error is returned.

5226

parser_generateHeaders
Parameters Parser *p
Returns int error
Description Generates the necessary header information based on the parser's current parameter set and state, and puts this header information appropriately within each Share buffer.

5228

parser_generateFooters
Parameters Parser *p
Returns int error
Description Generates the necessary footer information based on the parser's current parameter set and state, and puts this footer information appropriately within each Share buffer.

5230

FIG. 52C

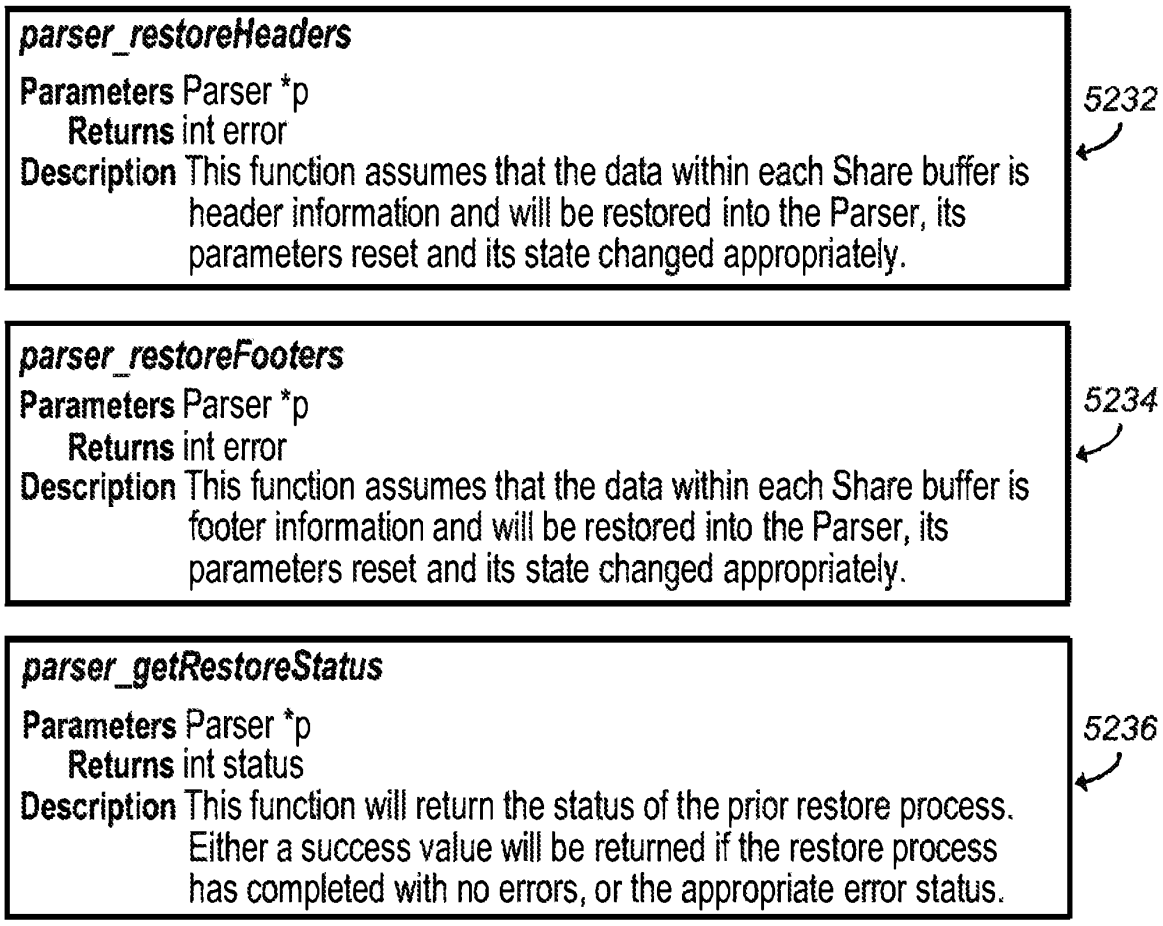

parser_restoreHeaders
Parameters Parser *p
Returns int error
Description This function assumes that the data within each Share buffer is header information and will be restored into the Parser, its parameters reset and its state changed appropriately.
5232
parser_restoreFooters
Parameters Parser *p
Returns int error
Description This function assumes that the data within each Share buffer is footer information and will be restored into the Parser, its parameters reset and its state changed appropriately.
5234
parser_getRestoreStatus
Parameters Parser *p
Returns int status
Description This function will return the status of the prior restore process. Either a success value will be returned if the restore process has completed with no errors, or the appropriate error status.
5236

FIG. 52D

Electronic Patent Application Fee Transmittal

Application Number:	15977748
Filing Date:	11-May-2018
Title of Invention:	SECURE DATA PARSER METHOD AND SYSTEM
First Named Inventor/Applicant Name:	Mark S. O'Hare
Filer:	Kent Bryan Chambers/Celeste Scarborough
Attorney Docket Number:	T00521

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
PET. REVIVE ABANDON APP, DELAY PYMT-RESP	1453	1	2100	2100
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Extension - 1 month with $0 paid	1251	1	220	220
Miscellaneous:				
		Total in USD ($)		**2320**

Electronic Acknowledgement Receipt	
EFS ID:	43045647
Application Number:	15977748
International Application Number:	
Confirmation Number:	7200
Title of Invention:	SECURE DATA PARSER METHOD AND SYSTEM
First Named Inventor/Applicant Name:	Mark S. O'Hare
Customer Number:	33438
Filer:	Kent Bryan Chambers/Celeste Scarborough
Filer Authorized By:	Kent Bryan Chambers
Attorney Docket Number:	T00521
Receipt Date:	21-JUN-2021
Filing Date:	11-MAY-2018
Time Stamp:	18:44:15
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$2320
RAM confirmation Number	E20216KI44384989
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	T00521_Petition_to_Revive_SB-64_2021-06-20.pdf	218709 97ba002e5956bce6a451bdeb28da303932f78ccf	no	3
Warnings:					
Information:					
2	Applicant Arguments/Remarks Made in an Amendment	T00521_Response_with_Petition_to_Revive_2021-06-20.pdf	101821 694158857ea5683bb7635fe90278093369b8af97	no	8
Warnings:					
Information:					
3	Extension of Time	T00521_Extension.pdf	172971 b29edcbd10943547a3dbfcac7e3b6d3eebf34c2b	no	2
Warnings:					
Information:					
4	Miscellaneous Incoming Letter	T00521_NtFCAP_2020-09-21.pdf	108899 01631b1ac353945d9920818a37a2275413cc266f	no	3
Warnings:					
Information:					
5	Drawings-only black and white line drawings	T00521_ReplacementDrawings_a.pdf	9548106 27df18ab239818da3628766d63abbebd884c867b	no	14
Warnings:					
Information:					
6	Fee Worksheet (SB06)	fee-info.pdf	32606 265d36430f3a4493dcbcd7c350c68e0925b8ad33	no	2
Warnings:					
Information:					

Total Files Size (in bytes):	10183112

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Inventor:	Mark S O'Hare		
Applicant:	Security First Corp.		
Title:	Secure Data Parser Method and System		
Application No.:	15/977,748	Filed:	May 11, 2018
Confirmation No.	7200		
Examiner:	Lemma, Samson B.	Group Art Unit:	2498
Docket No.:	T00521	Customer No.:	33438

ELECTRONICALLY FILED

Austin, Texas
June 21, 2021

REPLY TO NOTICE TO FILE CORRECTED APPLICATION PAPERS ACCOMPANYING A PETITION UNDER 37 C.F.R. § 1.137(b) FOR REVIVAL OF AN APPLICATION FOR PATENT ABANDONED UNINTENTIONALLY

The above-identified application became abandoned on January 22, 2021 for failure to timely file a Notice to File Corrected Application Papers in the present application. This Reply and a Petition under 37 C.F.R. § 1.137(b) for revival of an application for patent abandoned unintentionally are being filed within one (1) year of the December 21, 2021 final due date (with 1-month extension) of the Notice to File Corrected Application Papers.

This Reply fully responds to the Notice to File Corrected Application Papers.

AMENDMENT TO THE DRAWINGS

Please amend Figures 9 and 48-52b as indicated in the Replacement Sheets filed herewith.

AMENDMENT TO THE SPECIFICATION

Please amend ¶0042 as follows:

[0042] FIGURE ~~9~~, Panel A 9A illustrates a data flow of an enrollment process according to aspects of an embodiment of the invention;

Please amend ¶0043 as follows:

[0043] FIGURE 9~~, Panel B~~ 9B illustrates a flow chart of an interoperability process according to aspects of an embodiment of the invention;

Please amend ¶0048 as follows:

[0080] ~~FIGURE 48 Panels A and B~~ FIGURES 48A and 48B depict various parameters used in parsing operations in accordance with one embodiment of the present invention.

Please amend ¶0081 as follows:

[0081] ~~FIGURE 49 Panels A and B~~ FIGURES 49A and 49B depict data structures for the parser, keys, and shares in accordance with one embodiment of the present invention.

Please amend ¶0082 as follows:

[0082] ~~FIGURE 50 Panels A and B~~ FIGURES 50A and 50B depict data structures relating to encryption, authentication, and hashing functionality in accordance with one embodiment of the present invention.

Please amend ¶0083 as follows:

[0083] ~~FIGURE 51 Panels A and B~~ FIGURES 51A and 51B depict data formats in accordance with one embodiment of the present invention.

Please amend ¶0084 as follows:

[0084] ~~FIGURE 52A Panels A and B and FIGURE 52B Panels A and B~~ FIGURES 52A, 52B, 52C, and 52D depict a function library in accordance with one embodiment of the present invention.

Please amend ¶0576 as follows:

[0576] As is depicted in ~~FIGURE 48, Panel A, and FIGURE 48, Panel B~~ FIGURES 48A and 48B, various enumerators may indicate parameters used in parsing operations such as operating modes, encryption techniques, etc. For example, encryption type 4802 options may include no encryption, AES 128 bit in CTR mode, AES 192 bit in CTR mode, AES 256 bit in CTR mode, AES 128 bit in CBC mode, AES 192 bit in CBC mode, AES 256 bit in CBC mode, or 3DES in CBC mode. Authentication type 4804 options may include a RSA-PSS technique, a DSA digital signature technique, a _generateFooters function 5230 may generate share footer information for each Message Authentication Code. Hash type 4806 options may include no hashing technique or SHA-256. Split type 4808 options may include no split, block level split as determined by the splitting technique, byte level split, bit level split, or bit scattering. Key type 4810 options may include symmetric keys, RSA public key, RSA private key, DSA public key, DSA private key, ECDSA public key, or ECDSA private key. Error type 4812 options may include no error, no master key, invalid callback, invalid parse split technique, no target set to parse, target buffer has no length, unable to restore because not enough shares are present, invalid share was set, invalid key was set, an integrity check failure occurred, or out of memory.

Please amend ¶0577 as follows:

[0577] ~~FIGURE 49, Panel A and FIGURE 49, Panel B~~ FIGURES 49A and 49B depict data structures for the parser, keys and shares. Parser data structure 4902 may include information related to the data to be split and the splitting process, such as originalShare, shares, shareCount, splitEncContext, and finalFlag. ParserParams data structure 4904 may include information relating to the parameters used in the parsing process, such as L (# of mandatory shares), N (total # of non-mandatory shares), M (# of non-mandatory shares necessary to recover data), splitType, splitEncMode, preEncMode, postEncMode, splitHashMode, preAuthMode, preEncKey, postEncKey, preAuthKey, postAuthKey, maxOrigBufSize, and maxShareBufSize.

Please amend ¶0579 as follows:

[0579] ~~FIGURE 50, Panel A and FIGURE 50, Panel B~~ FIGURES 50A and 50B depict data structures relating to encryption, authentication, and hashing functionality. EncContext data structure 5002 may be utilized in various other data structures, and may include information relating to the type of encryption being used and encryption contexts as described below. EncContext_AESCBC data structure 5004 may include information relating to AES-CBC encryption, including encKeyid, currentIV (initialization vector) and currentIVLen. EncContext AESCTR data structure 5006 may include information relating to AES-CTR encryption, including encKeyid, currentIV (initialization vector) and currentIVLen.

Please amend ¶0582 as follows:

[0582] ~~FIGURE 51, Panel A and FIGURE 51, Panel B~~ FIGURES 51A and 51B depict data formats including share data 5102, post-encrypted footer 5104, post-encrypted header 5106, and encrypted footer 5108. Share data 5102 may include a post-encryption key id, post-signature key id, post-encrypted header 5106, post-encrypted footer 5104, and post-signature data. Post-encrypted footer 5104 may include encrypted footer 5108. Encrypted footer 5108 may include split-hash data, and pre-signature data. Post-encrypted header 5106 may include a key share, share id, L, M, N, split mode, split-encryption key, split-encryption IV, split-hash mode, original buffer, share buffer, pre-encryption key, and pre-signature key.

Please amend ¶0583 as follows:

[0583] The secure parser API may include a function library with various functions as depicted in ~~FIGURE 52A, Panel A, FIGURE 52A, Panel B, FIGURE 52B, Panel A, and FIGURE 52B, Panel B~~ FIGURES 52A, 52B, 52C, and 52D. A number of functions may relate to initializing and ending parser operations. A parser_createParser function 5202 may be called to allocate a secure parser context and set default values for the parser, while a parser_destroyParser function 5204 may be passed a Parser data structure and may destroy the secure parser context, including parser parameter objects and share buffers. A parser_createKey function 5206 may construct the key structure, while a parser_destroyKey function 5208 may destroy the key. A parser_createShare function 5210 may create a share data structure for use with the secure parser, while a parser_destroyShare function 5212 may destroy a share, including all encryption and authentication keys. A parser_initParameters function 5214 may initialize the ParserParams data structure to the default parameter set, while a parser_setParameters 5216 may set any ParserParames settings for the current Parser data structure. A parser_setFinalize function 5218 may set the internal state of the Parser to finalize the output stream during the next split session.

REMARKS

The *Present Application* received a Notice of Allowance having a Date Mailed of August, 7, 2020.

A Notice to File Corrected Application Papers ("Notice") having a Date Mailed of September 21, 2020 required corrections to Figures 9 and 48-52b because those Figures did not comply with 37 C.F.R. § 1.84(u)(1).

The relevant portion of 37 C.F.R. § 1.84(u)(1) quoted in the Notice requires:

> 37 CFR 1.84(u)(l) states, "The different views must be numbered in consecutive Arabic numerals, starting with 1 ... Partial views intended to form one complete view, on one or several sheets, must be identified by the same number followed by a capital letter. View numbers must be preceded by the abbreviation 'FIG.' "

Applicant has amended Figures 9 and 48-52b (now Figures 9A, 9B, 48A, 48B, 49A, 49B, 50A, 50B, 51A, 51B, 52A, 52B, 52C, and 52D) to comply with 37 C.F.R. § 1.84(u)(1) as required by the Notice.

Accordingly, Applicant respectfully submits that Applicant has complied with the requirements of the Notice.

Amendment to the Drawings

Figures 9 and 48-52b (now Figures 9A, 9B, 48A, 48B, 49A, 49B, 50A, 50B, 51A, 51B, 52A, 52B, 52C, and 52D) have been amended as indicated in the Replacement Sheets filed herewith.

No new matter has been added.

Amendment to the Specification

Paragraphs 0042, 0043, 0080-0084, 0576, 0577, 0582, and 0583 have been amended to correspond with the amended identifiers in the amended drawings.

No new matter has been added.

CONCLUSION

Applicant respectfully submits that all requirements have been met to revive the *Present Application*. Nonetheless, should any issues remain that might be subject to resolution through a telephone interview, the Examiner is requested to telephone the undersigned at 512-338-9100.

CERTIFICATE OF TRANSMISSION

I hereby certify that on June 21, 2021 this correspondence is being transmitted via the U.S. Patent & Trademark Office's electronic filing system.

/Kent B. Chambers/

Respectfully submitted,

/Kent B. Chambers/

Kent B. Chambers
Attorney for Applicant(s)
Reg. No. 38,839

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.
15/977,748	05/11/2018	Mark S. O'Hare	T00521	7200

7590 02/05/2021

TERRILE, CANNATTI & CHAMBERS, LLP
P.O. BOX 203518
AUSTIN, TX 78720

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	**PAPER NUMBER**
2498	
NOTIFICATION DATE	**DELIVERY MODE**
02/05/2021	ELECTRONIC

Notice of Abandonment

This application is abandoned in view of:

1. ☑ The applicant's failure to timely file a proper reply to the Office letter mailed on 9-21-20.
   (a) ☐ A reply was received on _____ (with a Certificate of Mailing or Transmission date _____), which is after the expiration of the period for reply (including a total extension of ____ month(s)) which expired on _____.
   (b) ☑ No reply has been received.
2. ☐ Applicant's failure to timely pay the required issue fee and publication fee, if applicable, within the statutory period of three months from the mailing date of the Notice of Allowance (PTOL-85).
   (a) ☐ The issue fee and publication fee, if applicable, was received on _____ (with a Certificate of Mailing or Transmission date _____), which is after the expiration of the statutory period for payment of the issue fee (and publication fee) set in the Notice of Allowance (PTOL-85).
   (b) ☐ The submitted fee of $_____ is insufficient. A balance of $_____ is due.
   The issue fee required by 37 CFR 1.18 is $_____.
   The publication fee, if required by 37 CFR 1.18(d), is $_____.
   (c) ☐ The issue fee and publication fee, if applicable, has not been received.
3. ☐ Applicant's failure to timely file corrected drawings as required by, and within the three-month period set in, the Notice of Allowability (PTO-37).
   (a) ☐ Proposed corrected drawings were received on _____ (with a Certificate of Mailing or Transmission dated _____), which is after the expiration of the period for reply.
   (b) ☐ No corrected drawing have been received.
4. ☐ Applicant's failure to timely file the inventor's oath or declaration no later than the date on which the issue fee was paid as required by the Notice Requiring Inventor's Oath or Declaration (PTO-2306).
   (a) ☐ An inventor's oath or declaration was received on _____ (with a Certificate of Mailing or Transmission date _____), which is after the date on which the issue fee was paid.
   (b) ☐ While an oath or declaration (or substitute statement) for one or more inventors was received, an oath or declaration (or substitute statement) for at least one other inventor has not been received.
   (c) ☐ No inventor's oath or declaration has been received.
5. ☐ Drawings received on _____ were disapproved by examiner. See examiner's response dated _____.
6. ☐ Corrected drawings were received on _____ , which is after the expiration of the one-month period for reply set in examiner's response dated _____.
7. ☐ No corrected drawings have been received in reply to one-month period set in examiner's response dated _____.
8. ☐ The reason(s) below:

Petitions to revive under 37 CFR 1.137(a) or request to withdraw the holding of abandonment under 37 CFR 1.181, should be promptly filed to minimize any negative effects on patent term.

/ATL/

(571)-272-4200 or 1(888)-786-0101
Patent Publication Branch
Office of Data Management
FORM PTO-ABN0 (Rev. 03/17)

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
15/977,748	05/11/2018	Mark S. O'Hare	104093-0002-118

CONFIRMATION NO. 7200

15314
Haley Guiliano LLP (S&L)
75 Broad Street
Suite 1000
New York, NY 10004-3226

POWER OF ATTORNEY NOTICE

OC000000121401676

Date Mailed: 11/19/2020

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 11/16/2020.

- The Power of Attorney to you in this application has been revoked by the applicant. Future correspondence will be mailed to the new address of record(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**.

/qtran/

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
15/977,748	05/11/2018	Mark S. O'Hare	T00521

CONFIRMATION NO. 7200

33438
TERRILE, CANNATTI & CHAMBERS, LLP
P.O. BOX 203518
AUSTIN, TX 78720

POA ACCEPTANCE LETTER

OC000000121401705

Date Mailed: 11/19/2020

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 11/16/2020.

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**.

/qtran/

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82A (07-13)
Approved for use through 03/31/2021. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	15/977,748
Filing Date	May 11, 2018
First Named Inventor	Mark S. O'Hare
Title	Secure Data Parser Method and System
Art Unit	2498
Examiner Name	Samson B. Lemma
Attorney Docket Number	T00521

SIGNATURE of Applicant or Patent Practitioner

Signature	/Kent B. Chambers/	Date (Optional)	November 16, 2020
Name	Kent B. Chambers	Registration Number	38,839
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)			

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☑ *Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82B (07-13)
Approved for use through 03/31/2021. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☑ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: 33438

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):

Security First Corp.

☐ 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	Andrew S. Price		
Title	CFO		

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.

PTO/AIA/82C (07-13)
Approved for use through 03/31/2021. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

POWER OF ATTORNEY BY APPLICANT

No more than ten (10) patent practitioners total may be appointed as set forth below by name and registration number. This page need not be submitted if appointing the Patent Practitioner(s) associated with a Customer Number (see form PTO/AIA/82B):

Name	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 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.

Electronic Acknowledgement Receipt	
EFS ID:	41136569
Application Number:	15977748
International Application Number:	
Confirmation Number:	7200
Title of Invention:	SECURE DATA PARSER METHOD AND SYSTEM
First Named Inventor/Applicant Name:	Mark S. O'Hare
Customer Number:	15314
Filer:	Kent Bryan Chambers/Celeste Scarborough
Filer Authorized By:	Kent Bryan Chambers
Attorney Docket Number:	104093-0002-118
Receipt Date:	16-NOV-2020
Filing Date:	11-MAY-2018
Time Stamp:	17:42:52
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	Power of Attorney	T00521_POA_82A.pdf	182481 fd0d73b51735f9e184c3117597a5d276033c7a26	no	1

Warnings:

Information:					
2	Power of Attorney	SecurityFirst_POA_82B.pdf	189734 46d2dc88cf8db0f87d2e41a49f19f2167b6db9f9	no	3
Warnings:					
Information:					
			Total Files Size (in bytes):	372215	

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.

PART B - FEE(S) TRANSMITTAL

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

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

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

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

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

15314 7590 08/07/2020

Haley Guiliano LLP (S&L)
75 Broad Street
Suite 1000
New York, NY 10004-3226

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

Certificate of Mailing or Transmission

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

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/977,748	05/11/2018	Mark S. O'Hare	104093-0002-118	7200

TITLE OF INVENTION: SECURE DATA PARSER METHOD AND SYSTEM

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1000	$0.00	$0.00	$1000	11/09/2020

EXAMINER	ART UNIT	CLASS-SUBCLASS
LEMMA, SAMSON B	2498	726-005000

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

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

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

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

1 _____
2 _____
3 _____

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

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

(A) NAME OF ASSIGNEE	(B) RESIDENCE: (CITY and STATE OR COUNTRY)
Security First Corp.	Rancho Santa Margarita, California

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

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

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

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

☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. 502264

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 /Kent B. Chambers/ Date November 3, 2020

Typed or printed name Kent B. Chambers Registration No. 38,839

Electronic Patent Application Fee Transmittal

Application Number:	15977748
Filing Date:	11-May-2018
Title of Invention:	SECURE DATA PARSER METHOD AND SYSTEM
First Named Inventor/Applicant Name:	Mark S. O'Hare
Filer:	Kent Bryan Chambers/Celeste Scarborough
Attorney Docket Number:	104093-0002-118

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
UTILITY APPL ISSUE FEE	1501	1	1000	1000

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**1000**

Electronic Acknowledgement Receipt	
EFS ID:	41021608
Application Number:	15977748
International Application Number:	
Confirmation Number:	7200
Title of Invention:	SECURE DATA PARSER METHOD AND SYSTEM
First Named Inventor/Applicant Name:	Mark S. O'Hare
Customer Number:	15314
Filer:	Kent Bryan Chambers/Celeste Scarborough
Filer Authorized By:	Kent Bryan Chambers
Attorney Docket Number:	104093-0002-118
Receipt Date:	03-NOV-2020
Filing Date:	11-MAY-2018
Time Stamp:	13:25:11
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$1000
RAM confirmation Number	E2020A3D25285943
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)	T00521_IssueFeeXmtl_2020-11-07_.pdf	867049 de43218523d8ee86843c8f2f15dabe8d2dec120d	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30422 b72b5ba22f45a8801182482d1fcb1127619d9bda	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	897471		

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/977,748	05/11/2018	Mark S. O'Hare	104093-0002-118	7200

15314 7590 09/21/2020

Haley Guiliano LLP (S&L)
75 Broad Street
Suite 1000
New York, NY 10004-3226

EXAMINER	
LEMMA, SAMSON B	

ART UNIT	PAPER NUMBER
2498	

NOTIFICATION DATE	DELIVERY MODE
09/21/2020	ELECTRONIC

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

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

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

hgpatentdocket@hglaw.com
haleyguiliano_PAIR@firsttofile.com

PTOL-90A (Rev. 04/07)

UNITED STATES PATENT AND TRADEMARK OFFICE

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

Application No. : 15977748
Applicant : O'Hare
Filing Date : 05/11/2018
Date Mailed : 09/21/2020

NOTICE TO FILE CORRECTED APPLICATION PAPERS

Notice of Allowance Mailed

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

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

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

See attachment(s).

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

/Naran Hem/
Publication Branch
Office of Data Management
(571) 272-4200

Application No. 15977748 **Drawings filed: 05/11/2018**

DRAWINGS AND BRIEF DESCRIPTION OF DRAWINGS IN NON-COMPLIANCE WITH 37 CFR 1.84(u)(1)

37 CFR 1.84(u)(1) states, "The different views must be numbered in consecutive Arabic numerals, starting with 1 … Partial views intended to form one complete view, on one or several sheets, must be identified by the same number followed by a capital letter. View numbers must be preceded by the abbreviation 'FIG.' "

Other methods of identification are improper, including Roman numerals (FIG. I, FIG, II, etc.) and alphabetic characters (FIG. A, FIG. B, etc.). Abbreviations and words other than "FIG." ("Illustration, 1" "Diagram 2," "Photo 3," etc.) are improper.

☐ Applicant must submit drawings that number the views using consecutive Arabic numerals.

☐ Applicant must amend the brief description of the drawings on Page(s) of the specification to show consecutive Arabic numerals.

NOTE: Applicant is advised that the detailed description may voluntarily be amended to identify the drawings by Arabic numerals.

☒ The drawing is continued onto a second page (or more) without proper labeling under 37 CFR 1.84(u)(1). FIG(s) **9, 48-52b**

☐ Applicant must submit drawings on which the view numbers are preceded by the abbreviation "FIG."

☐ Applicant must amend the brief description of the drawings on Page(s) of the specification to show view numbers preceded by the abbreviation "FIG."

NOTE: Applicant is advised that the detailed description may voluntarily be amended to show view numbers preceded by the abbreviation "FIG."

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

15314 7590 08/07/2020

Haley Guiliano LLP (S&L)
75 Broad Street
Suite 1000
New York, NY 10004-3226

EXAMINER
LEMMA, SAMSON B

ART UNIT	PAPER NUMBER
2498	

DATE MAILED: 08/07/2020

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/977,748	05/11/2018	Mark S. O'Hare	104093-0002-118	7200

TITLE OF INVENTION: SECURE DATA PARSER METHOD AND SYSTEM

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1000	$0.00	$0.00	$1000	11/09/2020

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

PART B - FEE(S) TRANSMITTAL

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

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

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

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

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

15314 7590 08/07/2020
Haley Guiliano LLP (S&L)
75 Broad Street
Suite 1000
New York, NY 10004-3226

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

Certificate of Mailing or Transmission

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

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/977,748	05/11/2018	Mark S. O'Hare	104093-0002-118	7200

TITLE OF INVENTION: SECURE DATA PARSER METHOD AND SYSTEM

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1000	$0.00	$0.00	$1000	11/09/2020

EXAMINER	ART UNIT	CLASS-SUBCLASS
LEMMA, SAMSON B	2498	726-005000

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

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

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

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

1_____
2_____
3_____

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

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

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

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

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

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

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

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

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

❑ Applicant certifying micro entity status. See 37 CFR 1.29

❑ Applicant asserting small entity status. See 37 CFR 1.27

❑ Applicant changing to regular undiscounted fee status.

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

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

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/977,748	05/11/2018	Mark S. O'Hare	104093-0002-118	7200

15314 7590 08/07/2020

Haley Guiliano LLP (S&L)
75 Broad Street
Suite 1000
New York, NY 10004-3226

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	**PAPER NUMBER**
2498	

DATE MAILED: 08/07/2020

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

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

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

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

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

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

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

Privacy Act Statement

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

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

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

Notice of Allowability	Application No. 15/977,748	Applicant(s) O'Hare et al.	
	Examiner SAMSON B LEMMA	Art Unit 2498	AIA (FITF) Status No

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

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

1. ☑ This communication is responsive to RCE filed on 07/24/2020.
   ☐ 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 2-25 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

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

   Certified copies:

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

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

   * Certified copies not received: _____ .

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

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

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

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

Attachment(s)

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

/SAMSON B LEMMA/
Primary Examiner, Art Unit 2498

DETAILED ACTION

1. This office action is in response to RCE filed on 07/24/2020. Claims 2-25 are pending and claims 1, 10, 16 and 22 are independent. Each independent claim is amended.

Notice of Pre-AIA or AIA Status

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

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

Continued Examination Under 37 CFR 1.114

4. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on July 24, 2020 has been entered.

Allowable Subject Matter

5. Claims 2-25 are allowed.

6. The following is an examiner's statements of reasons for allowance:

7. The following references/prior arts disclose the general subject matter recited in independent claims 2, 10, 16 and 22.

8. As per independent claims 2, 10, 16 and 22 Dickinson discloses as **method for securing a data set** *[See page 2, lines 25-30, "According to yet another aspect of the invention, the trust engine includes multiple depositories for storing portions of each cryptographic key and authentication data. The portions are created through a data splitting process that prohibits reconstruction without a predetermined portion from more than one depository. According to another embodiment, the multiple depositories are geographically remote such that a rogue employee or otherwise compromised system at one depository will not provide access to a user's key or authentication data."]***, the method comprising:**

distributing the data set into a plurality of data chunks, wherein none of the data chunks are, by themselves, sufficient to reconstruct the data set *[See figure 8, ref. 835, see at least page 20 lines 5-8, According to another embodiment of the invention, the depository system 700 comprises multiple geographically separated independent data storage systems. By distributing the sensitive data into distinct and independent storage facilities D1 through D4, some or all of which may be advantageously geographically separated, the depository system 700 provides redundancy along with additional security measures. For example, according to one embodiment, only data from two of the multiple data storage facilities, D1 through D4, are needed to decipher and reassemble the sensitive data. See also page 21, lines 10-14, Based on the foregoing, the data splitting process 800 advantageously places portions of the sensitive data in each of the four data storage facilities D1 through D4, such that no single data storage facility D1 through D4 includes sufficient encrypted data to recreate the original sensitive data S.]***;**

~~encrypting~~ **each of the data chunks is XORed** ~~**a respective one of a plurality of encryption**~~ *~~keys~~ [See page 20, lines 10-11, 'the data stored in each data storage facility is randomized and undecipherable, comprises of any individual data storage facility does not necessarily comprises the sensitive data. See page 21, lines 10-14, "Based on the foregoing, the data splitting process 800 advantageously places portions of the sensitive data in each of the four data storage facilities D1 through D4, such that no single data storage facility D1 through D4 includes sufficient encrypted data to recreate the original sensitive data S. As mentioned in the foregoing, such randomization of the data into individually unusable encrypted portions increases security and provides for maintained trust in the data even if one of the data storage facilities, D1 through D4, is compromised".See also figure 8, 825 and 830 wherein each chunk of data S is encrypted or XORed with the key such as a random numbers A and C]*

~~**obfuscating each of the plurality of different encryption keys**~~

and storing the plurality of data chunks ~~**with the plurality of obfuscated different encryption keys**~~ **on a plurality of different storage devices [See figure 8, 835, and** *See page 21, lines 10-14, "Based on the foregoing, the data splitting process 800 advantageously places/stores portions of the sensitive data in each of the four data storage facilities D1 through D4, such that no single data storage facility D1 through D4 includes sufficient encrypted data to recreate the original sensitive data S. As mentioned in the foregoing, such randomization of the data into individually unusable encrypted portions increases security and provides for maintained trust in the data even if one of the data storage facilities, D1 through D4, is compromised"]***.**

Dickinson substantially discloses all the limitation recited in the claim but even if it assumed that it does not explicitly disclose the limitation,"

obfuscating each of the plurality of different encryption keys and
storing the plurality of data chunks with the plurality of obfuscated different encryption keys on a plurality of different storage devices.

However Bolosky discloses:

"encrypting each data chunk of data (that is, by itself, not sufficient to reconstruct the data) with a respective key" *[See paragraph 0145 and figure 8, ref. 806 and 810 and claim 81, "A component in a distributed file system in which file are stored across multiple distributed computers, the component comprising: a segmenting module to divide a file into multiple blocks; a hash module to hash each of the blocks to produce block hash values; a cryptographic engine to encrypt the blocks using their corresponding block hash values as encryption keys to produce encrypted blocks. As shown on figure 8 and figure 9, none of the blocks are by themselves are sufficient to reconstruct the big file F by itself.]*

obfuscating each of the plurality of different encryption keys. *[See paragraph 0146 and figure 8, ref. 814(A), the leaf node containing an access value formed by encrypting the block hash value/(that corresponds to the each encryption keys) for the corresponding encrypted block using an access key]*

storing the plurality of data chunks with the plurality of obfuscated different encryption keys on a plurality of different storage devices*[See at least figure 2, ref. 240 and claim 81, "a component in a distributed file system in which file are stored across multiple distributed computers, the component comprising a segmenting module to divide a file into multiple blocks; a hash module to hash each of the blocks to produce block hash values; a cryptographic engine to encrypt the blocks using their corresponding block hash values as encryption keys to produce encrypted blocks; and an index builder to create an indexing structure for indexing individual encrypted blocks, the indexing structure containing a leaf node for each corresponding encrypted block, the leaf node containing an access value formed by encrypting the block hash value for the corresponding encrypted block using an access key and a verification value formed by hashing the corresponding encrypted block"].*

However, the above prior arts of record including the rest of the cited prior arts either taken alone or in combination neither anticipates nor renders obvious the claimed subject matter of the instant application that is taken as a whole including the specific functional recited in the amended independent claims 2, 10, 16 and 22.
For this reason, the specific claim limitations recited in independent claims 2, 10, 16 and 22 taken as whole are found to be allowable.

9. The dependent claims 3-9, 11-15, 17-21 and 23-25 which are dependent on the above independent claims 2, 10, 16 and 22 being further limiting to the independent claim, definite and enabled by the specification are also allowed.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SAMSON B LEMMA whose telephone number is 571-272-3806. The examiner can normally be reached on M-F 8am-10pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Shaw Yin Chen can be reached on 571-272-8593. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

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.

/SAMSON B LEMMA/
Primary Examiner, Art Unit 2498

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/977,748	O'Hare et al.
	Examiner	**Art Unit**
	SAMSON B LEMMA	2498

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

CLAIMS

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

CLAIM		DATE								
Final	Original	04/05/2019	01/15/2020	08/01/2020						
	1	-	-	-						
1	2	✓	✓	=						
2	3	✓	✓	=						
3	4	✓	✓	=						
4	5	✓	✓	=						
5	6	✓	✓	=						
6	7	✓	✓	=						
7	8	✓	✓	=						
8	9	✓	✓	=						
9	10	✓	✓	=						
10	11	✓	✓	=						
11	12	✓	✓	=						
12	13	✓	✓	=						
13	14	✓	✓	=						
14	15	✓	✓	=						
15	16	✓	✓	=						
16	17	✓	✓	=						
17	18	✓	✓	=						
18	19	✓	✓	=						
19	20	✓	✓	=						
20	21	✓	✓	=						
21	22	✓	✓	=						
22	23	✓	✓	=						
23	24	✓	✓	=						
24	25	✓	✓	=						

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/977,748	O'Hare et al.
	Examiner	Art Unit
	SAMSON B LEMMA	2498

CPC						
Symbol					Type	Version
H04L	/	63	/	0428	F	2013-01-01
H04L	/	67	/	108	I	2013-01-01
G06F	/	16	/	22	I	2019-01-01
G06F	/	21	/	606	I	2013-01-01
G06F	/	21	/	62	I	2013-01-01
H04L	/	9	/	085	I	2013-01-01
H04L	/	9	/	3226	I	2013-01-01
H04L	/	9	/	3263	I	2013-01-01
H04L	/	63	/	04	I	2013-01-01
H04L	/	63	/	08	I	2013-01-01
H04L	/	69	/	14	I	2013-01-01
G06F	/	21	/	602	I	2013-01-01
H04L	/	63	/	0876	I	2013-01-01
G06F	/	21	/	6218	I	2013-01-01
H04L	/	63	/	0823	I	2013-01-01
G06F	/	11	/	1092	A	2013-01-01
H04L	/	2209	/	80	A	2013-01-01

CPC Combination Sets								
Symbol					Type	Set	Ranking	Version
	/		/					

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	24	
/SAMSON B LEMMA/ Primary Examiner, Art Unit 2498	01 August 2020	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	24

U.S. Patent and Trademark Office — Part of Paper No.: 20200730

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/977,748	O'Hare et al.
	Examiner	**Art Unit**
	SAMSON B LEMMA	2498

INTERNATIONAL CLASSIFICATION				
CLAIMED				
G06F	/	7	/	04

NON-CLAIMED				
	/		/	

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**

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

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	24	
/SAMSON B LEMMA/ Primary Examiner, Art Unit 2498	01 August 2020	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	24

U.S. Patent and Trademark Office — Part of Paper No.: 20200730

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/977,748	O'Hare et al.
	Examiner	**Art Unit**
	SAMSON B LEMMA	2498

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

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
	1	9	10	18	19										
1	2	10	11	19	20										
2	3	11	12	20	21										
3	4	12	13	21	22										
4	5	13	14	22	23										
5	6	14	15	23	24										
6	7	15	16	24	25										
7	8	16	17												
8	9	17	18												

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	24	
/SAMSON B LEMMA/ Primary Examiner, Art Unit 2498	01 August 2020	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	24

U.S. Patent and Trademark Office — Part of Paper No.: 20200730

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/977,748	O'Hare et al.
	Examiner	Art Unit
	SAMSON B LEMMA	2498

CPC - Searched*		
Symbol	**Date**	**Examiner**
H04L63/04;0428;08;0823;0876	08/01/2020	SL
G06F21/602;606;62;6218	08/01/2020	SL
H04L9/085;3226;3263	08/01/2020	SL
H04L2209/80	08/01/2020	SL

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

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**
726	5	08/01/2020	SL

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

Search Notes		
Search Notes	**Date**	**Examiner**
H04L63/$, G06F21/$, H04L9/$, H04L2209/$, 726/$ (With text Search)	08/01/2020	SL
East and Interference Search (See attachment)	08/01/2020	SL
NPL (IEEE, ACM DIGITAL LIBRARY, GOOGLE, GOOGLE PATENT, GOOGLE SCHOLAR, IP.COM...)	08/01/2020	SL
INVENTOR NAME SEARCH	08/01/2020	SL

/SAMSON B LEMMA/ Primary Examiner, Art Unit 2498	

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/977,748	O'Hare et al.
	Examiner	Art Unit
	SAMSON B LEMMA	2498

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**
Interference Search History Printout		08/01/2020	SL

/SAMSON B LEMMA/ Primary Examiner, Art Unit 2498	

Discover | PAT | 2. A method for securing a... | + 0 mods | 0 filters

STIC

Visuals | Query | Results | 0 Selected | Relevance | None | None

1 - 50 16,150,979 results

1. **Receipt, data reduction, and storage of encrypted data**

   Embodiments relate to processing streams of encrypted data received from multiple users. A received encrypted data stream is separated into one or more encrypted data chunks, placing the data chunk(s) into a sub-stream, and decrypting the data chunks into plaintext. One or more advanced data...

   CURRENT ASSIGNEES: INTL BUSINESS MACHINES CORP
   US10425228 | US PATENTS | 24-SEP-2019

2. **Secure data parser method and system**

   A secure data parser is provided that may be integrated into any suitable system for securely storing and communicating data. The secure data parser parses data and then splits the data into multiple portions that are stored or communicated distinctly. Encryption of the original data, the portions...

   CURRENT ASSIGNEES: SECURITY FIRST CORP
   US20180367509 | US APPLICATIONS | 20-DEC-2018

3. **Receipt, Data Reduction, and Storage of Encrypted Data**

   Embodiments relate to processing streams of encrypted data received from multiple users. A received encrypted data stream is separated into one or more encrypted data chunks, placing the data chunk(s) into a sub-stream, and decrypting the data chunks into plaintext. One or more advanced data...

   CURRENT ASSIGNEES: INTL BUSINESS MACHINES CORP
   US20170170961 | US APPLICATIONS | 15-JUN-2017

4. **Communication system and method**

   There is provided a system, including a network that is defined by its novel approach to privacy, security and freedom for its users, namely privacy by allowing access anonymously, security by encrypting and obfuscating resources and freedom by allowing users to anonymously and irrefutably be seen...

   CURRENT ASSIGNEES: MAIDSAFE FNDN
   US20170005788 | US APPLICATIONS | 05-JAN-2017

5. **Communication system and method**

   There is provided a system, including a network that is defined by its novel approach to privacy, security and freedom for its users, namely privacy by allowing access anonymously, security by encrypting and obfuscating resources and freedom by allowing users to anonymously and irrefutably be seen...

   CURRENT ASSIGNEES: MAIDSAFE FNDN [+1]
   US20140237614 | US APPLICATIONS | 21-AUG-2014

6. **Communication system and method**

   There is provided a system, including a network that is defined by its novel approach to privacy, security and freedom for its users, namely privacy by allowing access anonymously, security by encrypting and obfuscating resources and freedom by allowing users to anonymously and irrefutably be seen...

   CURRENT ASSIGNEES: MAIDSAFE FNDN
   US9411976 | US PATENTS | 09-AUG-2016

Top 1500 results

Relevance VIEW

0 Results
239 Results
1261 Results
0 Results
0 Results

Publication Date VIEW

2001 2020

First Cur Assignees by Relevance VIEW

INTL BUSINESS MACHINES ... (129)
SECURITY FIRST CORP (257)
MAIDSAFE FNDN (21)
SAS INST INC (2)
TOPIA TECH INC (7)
HEWLETT PACKARD ENTPR... (12)
IRVINE DAVID (12)

More Visuals

Result #1 PREV NEXT

Patents (data) (authentication) (plurality) (key) (engine) before:priority:2(

data; authentication; plurality; key; engine; Before: priority 2004-10-25;

About 8,572 results Download with Concepts Side-by-side

Sort by · Relevance · Group by · None · Deduplicate by · Family · Results / page · 10 ·

Secure **data** parser method and system



WO ~~EP~~ US ~~CN~~ AU ~~BR~~ CA *HK* · US8332638B2 · Rick L. Orsini · Security First Corp.
Priority 1999-09-20 · Filed 2012-02-17 · Granted 2012-12-11 · Published 2012-12-11
Each enrollment **authentication data** identifies one of multiple users and each of the multiple users is associated with one or more different **keys** from the **plurality** of private cryptographic **keys**. The cryptographic system also may comprise an **authentication engine** which compares **authentication data** ...

Secure **Data** Parser Method and System

AU · AU2015227516A1 · Roger Davenport · Security First Corp.
Priority 2003-06-11 · Filed 2015-09-18 · Published 2015-10-08
88 including in the **plurality** of shares **data** indicative of the first **key**; encrypting the **plurality** of shares; causing each of the **plurality** of shares ... **engine** system 1300 employs the nearest one of a **plurality** of geographically separated trust **engines**, 1305 through 1320, to perform the **authentication** ...

Cryptographic module for secure processing of value-bearing items



WO EP US ~~AU~~ · US8041644B2 · Craig L. Ogg · Stamps.Com
Priority 1999-10-18 · Filed 2010-05-18 · Granted 2011-10-18 · Published 2011-10-18
... the security device transaction **data** is related to the one of the **plurality** of users; a cryptographic **engine** for cryptographically protecting **data**; ... operations required for encryption/decryption, **authentication**, and **key** management. RNG 308 generates the required **data** for the Cipher **Engine**.

Electronic commerce with cryptographic **authentication**



WO ~~EP~~ US ~~AU~~ · US20160149873A1 · Alexander G. Dickinson · Security First Corporation
Priority 1999-09-20 · Filed 2015-10-05 · Published 2016-05-26
... from a **plurality** of private cryptographic **keys** stored on the trust **engine**. The method also comprises receiving at a trust **engine**, transaction **data** ... The particular private cryptographic **key** need not be released from the secure server. **Data** indicating the status of the **authentication** may then be ...

Context sensitive dynamic **authentication** in a cryptographic system



US · US8214650B2 · Alexander G. Dickinson · Security First Corporation
Priority 1999-09-20 · Filed 2010-09-09 · Granted 2012-07-03 · Published 2012-07-03
... as in claim 41 further comprising providing the user with a **plurality** of **authentication** techniques which may be used to generate the user **data**. ... 700 for the signing party, and takes actions to provide appropriate matching **keys**. According to still another embodiment, the **authentication engine**

Cryptographic server with provisions for interoperability between cryptographic ...



US · US8494966B2 · Alexander G. Dickinson · Security First Corp.
Priority 1999-09-20 · Filed 2009-08-17 · Granted 2013-07-23 · Published 2013-07-23
According to yet another embodiment, the trust **engine** may include a redundancy module for polling a **plurality** of **authentication** results to ensure ... , at STEP 1015 , encrypts at least the current **authentication data** "B" and the transaction ID, with the public **key** of the **authentication engine** 215 ,

Methods and apparatus for performing **authentication** and decryption



US · US8458461B2 · Joseph Tardo · Broadcom Corporation
Priority 2002-05-31 · Filed 2010-07-26 · Granted 2013-06-04 · Published 2013-06-04
201 can include other components as well, such as a public **key engine** or cores for performing other **authentication** and encryption algorithms. ... decrypting a first block in a record comprising a **plurality** of encrypted blocks, the first block including a padding length; determining a **data** ...

Smartcard transaction method and system using signature recognition

US · US7533827B2 · David S. Bonalle · American Express Travel Related Services Company, Inc.
Priority 2004-07-01 · Filed 2007-09-26 · Granted 2009-05-19 · Published 2009-05-19

Security **engine** 1304 may utilize various **authentication**, **data** encryption, and digital signature techniques in connection with incoming and outgoing ... hotel rooms. In an exemplary embodiment, **key**-of-the-room EF 910 may comprise a **plurality** of alphanumeric **key** values as shown in Table 34 below.

Smartcard transaction method and system using voiceprint recognition

US • US7494058B2 • David S. Bonalle • American Express Travel Related Services Company, Inc.
Priority 2004-07-01 • Filed 2007-09-26 • Granted 2009-02-24 • Published 2009-02-24

. In this regard, security **engine** 1602 may utilize various **authentication**, **data** encryption, and digital signature techniques in connection with ... hotel rooms. In an exemplary embodiment, **key**-of-the-room EF 910 may comprise a **plurality** of alphanumeric **key** values as shown in Table 34 below.

Methods and systems for encoding and protecting **data** using digital signature ...

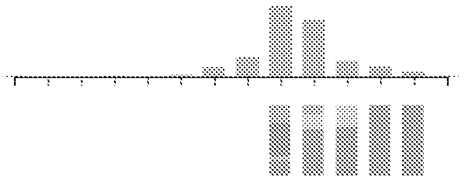


WO US A1 • US20130279741A1 • Xavier Serret-Avila • Intertrust Technologies Corporation
Priority 1999-06-08 • Filed 2013-05-10 • Published 2013-11-07

wherein retrieving the **plurality** of payloads further comprises: identifying a set of mark holder candidates in the electronic **data**; using each **key** of ... that is extracted from a given block (e.g., a block 502 received at time t), is provided to signature **verification engine** 512 , which is operable to ...

Next › » About 8,572 results

Top 1000 results by filing date



Relative count of top 5 values

Assignees	Inventors	CPCs
American Express Travel Related Services Company, Inc.		6.6%
Broadcom Corporation		3.4%
Silverbrook Research Pty Ltd		3.1%
Storymail, Inc.		2.8%
ソニー株式会社		2.5%

Expand

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	2	"20180367509"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/03 00:10
L2	300,238	((G06F21/602 OR G06F21/606 OR G06F21/62 OR G06F21/6218 OR H04L2209/80 OR H04L63/04 OR H04L63/0428 OR H04L63/08 OR H04L63/0823 OR H04L63/0876 OR H04L9/085 OR H04L9/3226 OR H04L9/3263 OR G06F16/22).CPC.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/03 00:12
L3	21,249	((G06F21/602).CPC.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/03 00:14
L4	12,947	((G06F21/606).CPC.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/03 00:15
L5	15,975	((G06F21/62).CPC.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/03 00:16
L6	42,599	((G06F21/6218).CPC.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/03 00:16
L7	27,533	((H04L2209/80).CPC.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/03 00:16

L8	8,649	((H04L63/04).CPC.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/03 00:16
L9	67,551	((H04L63/0428).CPC.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/03 00:17
L10	79,257	((H04L63/08).CPC.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/03 00:17
L11	36,658	((H04L63/0823).CPC.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/03 00:17
L12	22,295	((H04L63/0876).CPC.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/03 00:18
L13	7,076	((H04L9/085).CPC.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/03 00:18
L14	15,902	((H04L9/3226).CPC.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/03 00:19
L15	17,698	((H04L9/3263).CPC.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/03 00:19

L16	13,167	((G06F16/22).CPC.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/03 00:19
L17	13,052	(plurality with (chunk$1 or portion or data$1 or block$1) with encrypt$) and distribut$5	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/03 00:29
L18	1,293	(plurality with (chunk$1 or portion or data$1 or block$1) with encrypt$) same distribut$5 same stor$5	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/03 00:29
L19	642	(plurality with (chunk$1 or portion or data$1 or block$1) with encrypt$) same key same distribut$5 same stor$5	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/03 00:30
L21	108	19 and 3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/03 00:40
L22	15	19 and 4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/03 00:40
L23	49	19 and 5	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/03 00:41
L24	112	19 and 6	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/03 00:41

L25	30	19 and 7	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/03 00:41
L27	141	19 and 9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/03 00:41
L28	24	19 and 10	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/03 00:41
L29	10	19 and 11	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/03 00:41
L30	16	19 and 12	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/03 00:41
L31	10	19 and 11	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/03 00:42
L32	16	19 and 12	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/03 00:42
L33	92	19 and 13	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/03 00:42

L34	40	19 and 15	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/03 00:43
L39	2	(obfuscat$4 with different with encryption with key$1) and (plurality with different with storage with device$1)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/03 00:53

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L40	2	(obfuscat$4 with different with encryption with key$1) and (plurality with different with storage with device$1)	US-PGPUB; USPAT	OR	OFF	2020/08/03 00:53

8/3/2020 12:54:37 AM
C:\Users\slemma\Documents\EAST\Workspaces\15977748.wsp

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. 7200

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
15/977,748	05/11/2018 **RULE**	726	2498	104093-0002-118

APPLICANTS
Security First Corp., Rancho Santa Margarita, CA;

INVENTORS
Mark S. O'Hare, Coto De Caza, CA;
Rick L. Orsini, Flower Mound, TX;
Roger S. Davenport, Campbell, TX;
Steven Winick, Roslyn Heights, NY;

**** CONTINUING DATA** **************************
This application is a CON of 13/915,081 06/11/2013 PAT 9992170
which is a DIV of 13/468,383 05/10/2012 PAT 9338140
which is a CON of 11/258,839 10/25/2005 PAT 8266438
which claims benefit of 60/718,185 09/16/2005
and claims benefit of 60/622,146 10/25/2004

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

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****
06/04/2018

		STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /SAMSON B LEMMA/ Examiner's Signature	☐ Met after Allowance Initials	CA	68	24	4

ADDRESS

Haley Guiliano LLP (S&L)
75 Broad Street
Suite 1000
New York, NY 10004-3226
UNITED STATES

TITLE

SECURE DATA PARSER METHOD AND SYSTEM

FILING FEE RECEIVED		
3540	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

BIB (Rev. 05/07).

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 15/977,748	Filing Date 05/11/2018	☐ To be Mailed

ENTITY: ☑ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $100 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $460 =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT	07/24/2020	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 24	Minus	** 24	= 0		x $100 =	0
	Independent (37 CFR 1.16(h))	* 4	Minus	*** 4	= 0		x $460 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

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

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.	SLIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/MONIQUE BENJAMIN/
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".	
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.	

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

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

PTO/SB/30 (11-17)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Request for Continued Examination (RCE) Transmittal

Address to:
Mail Stop RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Application Number	15/977,748
Filing Date	2018-05-11
First Named Inventor	Mark S. O'Hare
Art Unit	2498
Examiner Name	Samson B. Lemma
Attorney Docket Number	104093-0002-118

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. See Instruction Sheet for RCEs (not to be submitted to the USPTO) on page 2.

1. Submission required under 37 CFR 1.114 Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

   a. ☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

      i. ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

      ii. ☐ Other _____

   b. ☑ Enclosed

      i. ☑ Amendment/Reply

      ii. ☐ Affidavit(s)/ Declaration(s)

      iii. ☐ Information Disclosure Statement (IDS)

      iv. ☐ Other _____

2. Miscellaneous

   a. ☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of _____ months. (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

   b. ☐ Other _____

3. Fees The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.

   a. ☑ The Director is hereby authorized to charge the following fees, any underpayment of fees, or credit any overpayments, to Deposit Account No. 06-1075 .

      i. ☑ RCE fee required under 37 CFR 1.17(e)

      ii. ☑ Extension of time fee (37 CFR 1.136 and 1.17)

      iii. ☐ Other _____

   b. ☐ Check in the amount of $ _____ enclosed

   c. ☐ Payment by credit card (Form PTO-2038 enclosed)

   d. ☑ Payment by EFS-Web

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Signature	/Maxim Rapoport/	Date	July 24, 2020
Name (Print/Type)	Maxim Rapoport	Registration No.	67,675

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being EFS-Web transmitted to the United States Patent and Trademark Office (USPTO), deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop RCE, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450 or facsimile transmitted to the USPTO on the date shown below.

Signature			
Name (Print/Type)		Date	

This collection of information is required by 37 CFR 1.114. 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: Mail Stop RCE, 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.

Docket No.: 104093-0002-118

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	:	Security First Corp.	
Inventors	:	Mark S. O'Hare, et al.	
Application No.	:	15/977,748	Confirmation No.: 7200
Filed	:	May 11, 2018	
For	:	SECURE DATA PARSER METHOD AND SYSTEM	
Group Art Unit	:	2498	
Examiner	:	Samson B. Lemma	

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

REPLY TO FINAL OFFICE ACTION

Sir:

In response to the Final Office Action dated January 24, 2020, Applicant respectfully requests reconsideration in view of the following remarks:

Claim Amendments begin on page 2 of this Reply.

Remarks begin on page 7 of this Reply.

CLAIM AMENDMENTS

This listing will replace all prior version and listings of claims in the above-identified patent application.

Listing of the Claims

1. (Canceled)

2. (Currently Amended) A method for securing a data set, the method comprising:

distributing the data set into a plurality of data chunks, wherein none of the data chunks are, by themselves, sufficient to reconstruct the data set;

encrypting each of the data chunks with a respective one of a plurality of encryption keys;

obfuscating each of the plurality of different encryption keys; and

separately storing each data chunk of the plurality of data chunks together with one of the plurality of obfuscated different encryption keys on a plurality of different storage devices.

3. (Previously Presented) The method of claim 2, wherein obfuscating each of the plurality of different encryption keys comprises performing a transform on data indicative of at least one of the plurality of different encryption keys.

4. (Previously Presented) The method of claim 3, wherein performing a transform on data indicative of at least one of the plurality of different encryption keys comprises performing an all-or-nothing transform on the data indicative of at least one of the plurality of different encryption keys.

5. (Previously Presented) The method of claim 2, wherein obfuscating each of the plurality of different encryption keys comprises applying Shamir's Secret Sharing algorithm to data indicative of at least one of the plurality of different encryption keys.

6. (Previously Presented) The method of claim 2, wherein storing the plurality of data chunks together with the plurality of obfuscated different encryption keys comprises storing each of the plurality of data chunks together with a respective one of the plurality of obfuscated different encryption keys.

7. (Previously Presented) The method of claim 2, wherein storing the plurality of data chunks together with the plurality of obfuscated different encryption keys comprises including, with a data chunk of the plurality of data chunks, data indicative of an encryption key that was used to encrypt a different data chunk of the plurality of data chunks.

8. (Previously Presented) The method of claim 2, wherein distributing the data set into a plurality of data chunks comprises using a random technique or pseudorandom technique.

9. (Previously Presented) The method of claim 2, further comprising generating the data set by encrypting primary data.

10. (Currently Amended) A method for securing a data set, the method comprising:

distributing the data set into a plurality of data chunks, wherein none of the data chunks are, by themselves, sufficient to reconstruct the data set;

encrypting each of the data chunks with a respective one of a plurality of encryption keys;

transforming each of the plurality of different encryption keys; and

separately storing each data chunk of the plurality of data chunks together with one of the plurality of transformed different encryption keys on a plurality of different storage devices.

11. (Previously Presented) The method of claim 10, wherein transforming each of the plurality of different encryption keys comprises performing an all-or-nothing transform on data indicative of at least one of the plurality of different encryption keys.

12. (Previously Presented) The method of claim 10, wherein storing the plurality of data chunks with the plurality of transformed different encryption keys comprises storing each of the plurality of data chunks with a respective one of the plurality of transformed different encryption keys.

13. (Previously Presented) The method of claim 10, wherein storing the plurality of data chunks with the plurality of transformed different encryption keys comprises including, with a data chunk of the plurality of data chunks, data indicative of an encryption key of the plurality of encryption keys that was used to encrypt a different data chunk of the plurality of data chunks.

14. (Previously Presented) The method of claim 10, wherein distributing the data set into a plurality of data chunks comprises using a random technique or pseudorandom technique.

15. (Previously Presented) The method of claim 10, further comprising generating the data by encrypting primary data.

16. (Currently Amended) A computer system for securing a data set, the system comprising:

at least one hardware processor, configured to:

access the data set;

distribute the data set into a plurality of data chunks, wherein none of the data chunks are, by themselves, sufficient to reconstruct the data set;

encrypt each of the data chunks with a respective one of a plurality of encryption keys;

obfuscate each of the plurality of different encryption keys; and

storing the plurality of data chunks together with the plurality of obfuscated different encryption keys;

separately store each data chunk of the plurality of data chunks together with one of the plurality of obfuscated different encryption keys, wherein the plurality of data chunks is stored on a plurality of different storage devices.

17. (Previously Presented) The computer system of claim 16, wherein, when obfuscating each of the plurality of different encryption keys, the at least one hardware processor is configured to

perform a transform on data indicative of at least one of the plurality of different encryption keys.

18. (Previously Presented) The computer system of claim 17, wherein, when performing a transform on data indicative of at least one of the plurality of different encryption keys, the at least one hardware processor is configured to perform an all-or-nothing transform on the data indicative of at least one of the plurality of different encryption keys.

19. (Previously Presented) The computer system of claim 16, wherein, when obfuscating each of the plurality of different encryption keys, the at least one hardware processor is configured to apply Shamir's Secret Sharing algorithm to data indicative of at least one of the plurality of different encryption keys.

20. (Previously Presented) The computer system of claim 16, wherein, when storing the plurality of data chunks together with the plurality of obfuscated different encryption keys, the at least one hardware processor is configured to store each of the plurality of data chunks together with a respective one of the plurality of obfuscated different encryption keys.

21. (Previously Presented) The computer system of claim 16, wherein, when storing the plurality of data chunks together with the plurality of obfuscated different encryption keys, the at least one hardware processor is configured to include, with a data chunk of the plurality of data chunks, data indicative of an encryption key that was used to encrypt a different data chunk of the plurality of data chunks.

22. (Currently Amended) A computer system for securing a data set, the system comprising:

at least one hardware processor, configured to:

access the data set;

distribute the data set into a plurality of data chunks, wherein none of the data chunks are, by themselves, sufficient to reconstruct the data set;

encrypt each of the data chunks with a respective one of a plurality of encryption keys;

transform each of the plurality of different encryption keys; and

storing the plurality of data chunks together with the plurality of transformed different encryption keys;

separately store each data chunk of the plurality of data chunks together with one of the plurality of transformed different encryption keys, wherein the plurality of data chunks is stored on a plurality of different storage devices.

23. (Previously Presented) The computer system of claim 22, wherein, when transforming each of the plurality of different encryption keys, the at least one hardware processor is configured to perform an all-or-nothing transform on data indicative of at least one of the plurality of different encryption keys.

24. (Previously Presented) The computer system of claim 22, wherein, when storing the plurality of data chunks with the plurality of transformed different encryption keys, the at least one hardware processor is configured to store each of the plurality of data chunks with a respective one of the plurality of transformed different encryption keys.

25. (Previously Presented) The computer system of claim 22, wherein, when storing the plurality of data chunks with the plurality of transformed different encryption keys, the at least one hardware processor is configured to include, with a data chunk of the plurality of data chunks, data indicative of an encryption key of the plurality of encryption keys that was used to encrypt a different data chunk of the plurality of data chunks.

REMARKS

Introduction

Claims 2-25 are pending in this application.

Claims 2-25 are rejected under 35 U.S.C. § 103 as being unpatentable over Dickinson, PCT Publication No. WO 01/22322 A2 (hereinafter "Dickinson") in view of Bolosky, U.S. Patent Application Publication No. 2002/0194209 (hereinafter "Bolosky").

Claims 2, 10, 16, 22 are amended to clarify the claimed subject matter. Applicant respectfully submits that the claim amendments are fully supported by the originally filed specification and no new matter has been added. The support for the claim amendments may be found throughout the Specification, and in particular in paragraphs [0431] and [0431]-[0438] of the Specification as published. Accordingly, no new matter is added. By making these amendments, Applicant is not conceding that the previously pending claims are not patentable and reserves the right to later pursue such claims in this application or in a continuation application.

The Examiner's rejection is respectfully traversed.

Applicants' Response to 35 U.S.C. § 103 Rejection

Claims 2-25 are rejected under 35 U.S.C. § 103 as being unpatentable over Dickinson in view of Bolosky.

Claim 2 is directed to securing a dataset. The method comprises distributing the data set into a plurality of data chunks, where none of the data chunks are (by themselves) sufficient to reconstruct the data set. Each respective data chunk is then encrypted with a respective encryption key of a plurality of encryption keys. Each of the keys is then obfuscated. As amended, claim 2 further recites separately storing each data chunk of the plurality of data chunks together with one of the plurality of obfuscated different encryption keys on a plurality of different storage devices.

Applicant respectfully submits that the combination of Dickinson and Bolosky fails to teach or render obvious storing each of the plurality of data chunks together with a respective one of the plurality of obfuscated different encryption keys.

The Office Action acknowledges that Dickinson fails to teach any kind of obfuscating different encryption keys and storing such keys. *See* Office Action, p. 8 and 9 (where the obfuscating language is crossed out when describing teachings of Dickinson). The Office Action, instead, relies on Bolosky for this element of claim 2.

Bolosky describes breaking file F into segments F^0, F^1, F^2, . . . , F^{n-1}. Each segment is hashed to produce values $h(F^i)$. Each hash is then used to encrypt its respective segment to create encrypted portion $E_{h(F^i)}(F^i)$. *See* Bolosky, para. 0145. The hashes themselves can also be encrypted with a key K to create access value $E_K(h(F^i))$ which is alleged to correspond to an obfuscated encryption keys of claim 2.

However, there is no disclosure in Bolosky that recites separately storing each data chunk with one of the plurality of obfuscated different encryption keys. However, to the extent Bolosky describes storing encryption keys ($h(F^i)$), such keys are all stored in a single metadata stream 404 that includes values for decrypting all encrypted blocks of data stream 402. See Bolosky para. [0103] and FIG. 4 of Bolosky. Consequently, Bolosky merely describes a single data stream that stores all of the data and keys for decrypting all of the data, which is not the same as separate storing as require by amended claim 2.

For at least these reasons, Applicant respectfully submits that claim 2 is patentable over the combination of Dickinson and Bolosky and respectfully requests withdrawal of § 103 rejection of claim 2. Claims 10, 16, and 22 were rejected for the same reason/rational as that of the above independent claim 2. Therefore, claims 10, 16, and 22 are patentable over the combination of Dickinson and Bolosky for the similar reasons as recited above with respect to claim 2.

Applicant respectfully requests withdrawal of the § 103 rejection of claims 2, 10, 16, 22, and all claims that depend from these independent claims.

Conclusion

In view of the above amendments and remarks, the pending application is in condition for allowance. Accordingly, reconsideration and prompt allowance are respectfully requested.

Applicant believes no fees are due with this response other than those on the Fee Transmittal filed herewith. However, if any additional fees are due, please charge our Deposit Account No. 06-1075, from which the undersigned is authorized to draw.

Dated: July 24, 2020

Respectfully submitted,

By: /Maxim Rapoport/
Maxim Rapoport
Registration No.: 67,675
HALEY GUILIANO LLP
Customer No. 15314
75 Broad Street, Suite 1000
New York, New York 10004
(646) 973-2500
Attorney for Applicant

Electronic Patent Application Fee Transmittal

Application Number:	15977748
Filing Date:	11-May-2018
Title of Invention:	SECURE DATA PARSER METHOD AND SYSTEM
First Named Inventor/Applicant Name:	Mark S. O'Hare
Filer:	Maxim Rapoport/Linda Blake
Attorney Docket Number:	104093-0002-118

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 3 months with $0 paid	1253	1	1400	1400
Miscellaneous:				
RCE- 1ST REQUEST	1801	1	1300	1300
		Total in USD ($)		**2700**

Electronic Acknowledgement Receipt	
EFS ID:	40095191
Application Number:	15977748
International Application Number:	
Confirmation Number:	7200
Title of Invention:	SECURE DATA PARSER METHOD AND SYSTEM
First Named Inventor/Applicant Name:	Mark S. O'Hare
Customer Number:	15314
Filer:	Maxim Rapoport/Linda Blake
Filer Authorized By:	Maxim Rapoport
Attorney Docket Number:	104093-0002-118
Receipt Date:	24-JUL-2020
Filing Date:	11-MAY-2018
Time Stamp:	13:17:29
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$2700
RAM confirmation Number	E20207ND17538835
Deposit Account	061075
Authorized User	Linda Blake
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.21 (Miscellaneous fees and charges) 37 CFR 1.20 (Post Issuance fees)	

37 CFR 1.19 (Document supply fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.16 (National application filing, search, and examination fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Extension of Time	104093-0002-118_EOT.pdf	855538 73e117f083536bb373818198a4555f8abe93300b	no	2
Warnings:					
Information:					
2	Request for Continued Examination (RCE)	104093-0002-118_RCE.pdf	62558 ccfcb32b81184106f5c1ae89462c4a9b959e8c9f	no	1
Warnings:					
This is not a USPTO supplied RCE SB30 form.					
Information:					
3		104093-0002-118_Reply.pdf	179661 284a5381c0595f4053e1103677fbbe6a68ef30ff	yes	9

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment Submitted/Entered with Filing of CPA/RCE	1	1
	Claims	2	6
	Applicant Arguments/Remarks Made in an Amendment	7	9

Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	32311 8b30bf4f1ce0364b1e7919b2f4d854324849a72d	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1130068		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

PTO/AIA/22 (03-13)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)

Docket Number (Optional): 104093-0002-118

Application Number: 15/977,748
Filed: 2018-05-11

For: SECURE DATA PARSER METHOD AND SYSTEM

Art Unit: 2498
Examiner: Samson B. Lemma

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Fee	Small Entity Fee	Micro Entity Fee	
☐ One month (37 CFR 1.17(a)(1))	$200	$100	$50	$
☐ Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$
☑ Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$ 1400
☐ Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐ Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☐ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 06-1075.

☑ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant.

☑ attorney or agent of record. Registration number 67,675.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/Maxim Rapoport/ — Signature
July 24, 2020 — Date
Maxim Rapoport — Typed or printed name
646-973-2500 — Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☑ * Total of one forms are submitted.

This collection of information is required by 37 CFR 1.136(a). 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 6 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: Mail Stop PCT, 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 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 NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/977,748	05/11/2018	Mark S. O'Hare	104093-0002-118	7200

15314 7590 01/24/2020

Haley Guiliano LLP (S&L)
75 Broad Street
Suite 1000
New York, NY 10004-3226

EXAMINER	
LEMMA, SAMSON B	

ART UNIT	PAPER NUMBER
2498	

NOTIFICATION DATE	DELIVERY MODE
01/24/2020	ELECTRONIC

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

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

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

haleyguiliano_PAIR@firsttofile.com
hgpatentdocket@hglaw.com

Office Action Summary	Application No. 15/977,748	Applicant(s) O'Hare et al.	
	Examiner SAMSON B LEMMA	Art Unit 2498	AIA (FITF) Status No

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

Period for Reply

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

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

Status

1)☑ Responsive to communication(s) filed on 10/18/2019.

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

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

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

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

Disposition of Claims*

5) ☑ Claim(s) 2-25 is/are pending in the application.

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

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 2-25 is/are rejected.

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

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

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

Application Papers

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

11)☑ The drawing(s) filed on 05/11/2018 is/are: a)☑ accepted or b)☐ objected to by the Examiner.

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

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

Priority under 35 U.S.C. § 119

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

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

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

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

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

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

Attachment(s)

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

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

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

4) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to the amendment filed on 10/18/2019. Claims 2-25 are pending in which claims 1, 10, 16 and 22 are independent.

Notice of Pre-AIA or AIA Status

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

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

Information Disclosure Statement

4. The information disclosure statements (IDS) submitted on 10/18/2019 has been considered. The submission is in compliance with the provisions of 37 CFR 1.97. Form PTO-1449 is signed and attached hereto.

Response to Arguments

5 Referring to the 35 U.S.C. 103 rejection, applicant's remarks/arguments filed on October 18, 2019 have also been fully considered but are not moot because the arguments do not apply to any of the references being used in the current rejection.

6. **Regarding independent claims 1, 10, 16 and 22**, Applicant's representative argued **that the combination of Dickinson and Goldwasser fails to teach or suggest "encrypting each data chunk of data (that is, by itself, not sufficient to reconstruct the data) with a respective key**, obfuscating each of these keys, and storing the obfuscated keys with the data chunks" [See page 7 of applicant's submitted argument]

7. Without agreeing with this argument, examiner would like to point out that new reference submitted with the IDS filed on 10/18/2019, US Patent No. 2002/0194209 A1 to William J. Bolosky (herein after referred as **Bolosky**) discloses this particular argued limitation/concept.

In particular Bolosky on figure 8 discloses this argued limitation.

Bolosky referring to figure 8; figure 2 and 5 on at least paragraph 0145 and abstract discloses the following indicating that the files are divided into multiple blocks and each blocks contains a portion of the file and as shown on figure 8, ref. 808 each blocks is hashed to generate each block's hash values. Then each blocks is encrypted using the block's hash value and none of the blocks are by themselves are sufficient to reconstruct the big file F by itself.

In particular on paragraph 0145 Bolosky discloses the following:

"In the first phase, the control module **220** employs the segmenter **222** to divide a file F into "n" multiple blocks **502**(**0**)-**502**(n−1) at operation **806**. Each block contains a portion of the file, which is illustrated as file segments F^0, F^1, F^2, . . . , F^{n-1} in blocks **502**. At operation **808**, the control module **220** invokes the hash module **226** to hash each block **502**(**0**)-**502**(n−1) to produce intermediate hash values $h(F^i)$. At operation **810**, the control module **220** calls the cryptographic engine **224** to encrypt each block **502**(**0**)-**502**(n−1) using that block's hash value, or $E_{h(Fi)}(F^i)$."

Furthermore the hash value of each block is also encrypted by the access key. Futhermore on

paragraph 0146 and figure 8, ref. 814 (A) it has been disclosed that the Hash value of each block that meets the limitation "encryption key" is also encrypted by using the key K as shown on figure 8, ref. 812.

Thus, in order to show how each and every limitation argued by the applicant's argument is disclosed by Bolosky, examiner would map each argued limitation with the corresponding citation as follows:

Bolosky discloses:

"encrypting each data chunk of data (that is, by itself, not sufficient to reconstruct the data) with a respective key" *[See paragraph 0145 and figure 8, ref. 806 and 810 and claim 81, "A component in a distributed file system in which file are stored across multiple distributed computers, the component comprising: a segmenting module to divide a file into multiple blocks; a hash module to hash each of the blocks to produce block hash values; a cryptographic engine to encrypt the blocks using their corresponding block hash values as encryption keys to produce encrypted blocks. As shown on figure 8 and figure 9, none of the blocks are by themselves are sufficient to reconstruct the big file F by itself.]*

obfuscating each of the plurality of different encryption keys. *[See paragraph 0146 and figure 8, ref. 814(A), the leaf node containing an access value formed by encrypting the block hash value/(that corresponds to the each encryption keys) for the corresponding encrypted block using an access key]*

storing the plurality of data chunks with the plurality of obfuscated different encryption keys on a plurality of different storage devices*[See at least figure 2, ref.*

240 and claim 81, "a component in a distributed file system in which file are stored across multiple distributed computers, the component comprising a segmenting module to divide a file into multiple blocks; a hash module to hash each of the blocks to produce block hash values; a cryptographic engine to encrypt the blocks using their corresponding block hash values as encryption keys to produce encrypted blocks; and an index builder to create an indexing structure for indexing individual encrypted blocks, the indexing structure containing a leaf node for each corresponding encrypted block, the leaf node containing an access value formed by encrypting the block hash value for the corresponding encrypted block using an access key and a verification value formed by hashing the corresponding encrypted block"].

Thus, even though examiner doesn't agree with the applicant's argument, as it is explained above, each and every argued limitation is disclosed by the Bolosky's prior art that is cited in the IDS filed on October 18, 2019.

8. Thus, in response to the 35 U.S.C. 103 rejection set forth in the previous office action, Applicant presented argument regarding at least each independent claim, presumably to

overcome the 103 rejection. However, the new prior art cited in the submitted IDS is found to disclose each limitations argued by the applicant's representative.

Applicant's submission of **an information disclosure statement** under 37 CFR 1.97(c) **prompted the new ground(s) of rejection presented in this Office action**.

Accordingly, THIS ACTION IS MADE FINAL.

The analysis of the claims under consideration, follows in the corresponding section below.

Claim Rejections - 35 USC § 103

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

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

10. Claims 2-4, 6-18 and 20-25 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Alexander Dickinson (hereinafter referred to as Dickinson) (International Publication No. WO 01/22322 A2. (March 29, 2001) (This reference is cited in the IDS and submitted in the parent application) in view of William J. Bolosky

(herein after referred as **Bolosky**) (US Publication No. 2002/0194209 A1) (Dec. 19, 2002) (This reference is cited in the IDS filed on October 18, 2019]

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

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

11. As per independent claim 2 Dickinson discloses as **method for securing a data set** *[See page 2, lines 25-30, "According to yet another aspect of the invention, the trust engine includes multiple depositories for storing portions of each cryptographic key and authentication data. The portions are created through a data splitting process that prohibits reconstruction without a predetermined portion from more than one depository. According to another embodiment, the multiple depositories are geographically remote such that a rogue employee or otherwise compromised system at one depository will not provide access to a user's key or authentication data."]***, the method comprising:**

distributing the data set into a plurality of data chunks, wherein none of the data chunks are, by themselves, sufficient to reconstruct the data set *[See figure 8, ref. 835, see at least page 20 lines 5-8, According to another embodiment of the invention, the depository system 700 comprises multiple geographically separated independent data storage systems. By distributing the sensitive data into distinct and independent storage facilities D1 through D4, some or all of which may be advantageously geographically separated, the depository system 700 provides redundancy along with*

additional security measures. For example, according to one embodiment, only data from two of the multiple data storage facilities, D1 through D4, are needed to decipher and reassemble the sensitive data. See also page 21, lines 10-14, Based on the foregoing, the data splitting process 800 advantageously places portions of the sensitive data in each of the four data storage facilities D1 through D4, such that no single data storage facility D1 through D4 includes sufficient encrypted data to recreate the original sensitive data S.];

~~encrypting~~ each of the data chunks is XORed ~~a respective one of a plurality of encryption~~ *~~keys~~ [See page 20, lines 10-11, 'the data stored in each data storage facility is randomized and undecipherable, comprises of any individual data storage facility does not necessarily comprises the sensitive data. See page 21, lines 10-14, "Based on the foregoing, the data splitting process 800 advantageously places portions of the sensitive data in each of the four data storage facilities D1 through D4, such that no single data storage facility D1 through D4 includes sufficient encrypted data to recreate the original sensitive data S. As mentioned in the foregoing, such randomization of the data into individually unusable encrypted portions increases security and provides for maintained trust in the data even if one of the data storage facilities, D1 through D4, is compromised".See also figure 8, 825 and 830 wherein each chunk of data S is encrypted or XORed with the key such as a random numbers A and C]*

~~obfuscating each of the plurality of different encryption keys~~

and storing the plurality of data chunks ~~with the plurality of obfuscated different encryption keys~~ on a plurality of different storage devices [See figure 8, 835, and *See page 21, lines 10-14, "Based on the foregoing, the data splitting process 800 advantageously places/stores portions of the sensitive data in each of the four data storage facilities D1 through D4, such that no single data storage facility D1 through D4 includes sufficient encrypted data to recreate the original sensitive data S. As mentioned in the foregoing, such randomization of the data into individually unusable encrypted portions increases security and provides for maintained trust in the data even if one of the data storage facilities, D1 through D4, is compromised"}***.**

Dickinson substantially discloses all the limitation recited in the claim but even if it assumed that it does not explicitly disclose the limitation,"

obfuscating each of the plurality of different encryption keys and
storing the plurality of data chunks with the plurality of obfuscated different encryption keys on a plurality of different storage devices.

Bolosky, the new reference submitted with the IDS discloses:

"encrypting each data chunk of data (that is, by itself, not sufficient to reconstruct the data) with a respective key" *[See paragraph 0145 and figure 8, ref. 806 and 810 and claim 81, "A component in a distributed file system in which file are stored across multiple distributed computers, the component comprising: a segmenting module to divide a file into multiple blocks; a hash module to hash each of the blocks to produce block hash values; a cryptographic engine to encrypt the blocks using their corresponding block hash values as encryption keys to produce encrypted blocks. As*

shown on figure 8 and figure 9, none of the blocks are by themselves are sufficient to reconstruct the big file F by itself.]

obfuscating each of the plurality of different encryption keys. *[See paragraph 0146 and figure 8, ref. 814(A), the leaf node containing an access value formed by encrypting the block hash value/(that corresponds to the each encryption keys) for the corresponding encrypted block using an access key]*

storing the plurality of data chunks with the plurality of obfuscated different encryption keys on a plurality of different storage devices*[See at least figure 2, ref. 240 and claim 81, "a component in a distributed file system in which file are stored across multiple distributed computers, the component comprising a segmenting module to divide a file into multiple blocks; a hash module to hash each of the blocks to produce block hash values; a cryptographic engine to encrypt the blocks using their corresponding block hash values as encryption keys to produce encrypted blocks; and an index builder to create an indexing structure for indexing individual encrypted blocks, the indexing structure containing a leaf node for each corresponding encrypted block, the leaf node containing an access value formed by encrypting the block hash value for the corresponding encrypted block using an access key and a verification value formed by hashing the corresponding encrypted block"].*

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to implement in the system of Dickinson, a mechanism such as "**obfuscating each of the plurality of different encryption keys** and **storing the plurality of data chunks with the plurality of obfuscated different encryption keys on a plurality of different storage devices as taught by** Bolosky because this would enhance and strengthen the security of the system by keeping the secrecy of the encryption/decryption key by further encrypting or obfuscating each of the different encryption keys and storing the data chunks in a pluralities of locations. [Bolsky at least figure 8]

12. **As per independent claim 10, independent claim 10 is rejected for the same reason/rational as that of the above independent claim 2.**

13. **As per independent claim 16, independent claim 16 is also rejected for the same reason/rational as that of the above independent claim 2.**

14. **As per independent claim 22, independent claim 22 is rejected for the same reason/rational as that of the above independent claim 2.**

15. **As per dependent claim 3 and 17 the combination of Dickinson and Bolosky discloses a system/method as applied to claims above. Furthermore Dickinson discloses the method/system, wherein obfuscating each of the plurality of different encryption keys comprises performing a transform on data indicative of**

at least one of the plurality of different encryption keys. [*See figure 8, 825 and 830 wherein each different keys such as random numbers A and B is obfuscated by the XOR operations.See also Bolosky at least figure 8 and claim 81***]**

16. **As per dependent claim 4 and 18 the combination of Dickinson and Bolosky discloses a system/method as applied to claims above. Furthermore Dickinson discloses the method/system, wherein performing a transform on data indicative of at least one of the plurality of different encryption keys comprises performing an all-or-nothing transform on the data indicative of at least one of the plurality of different encryption keys.** *[See figure 8, 825 and 830 wherein each different keys such as random numbers A and B is obfuscated by the XOR operations]*

17. **As per dependent claim 6 and 20 the combination of Dickinson and Bolosky discloses a system/method as applied to claims above. Furthermore Dickinson discloses the method/system, wherein storing the plurality of data chunks together with the plurality of obfuscated different encryption keys comprises storing each of the plurality of data chunks together with a respective one of the plurality of obfuscated different encryption keys [See figure 8, 835, and** *See page 21, lines 10-14, "Based on the foregoing, the data splitting process 800 advantageously places/stores portions of the sensitive data in each of the four data storage facilities D1 through D4, such that no single data storage facility D1 through D4 includes sufficient encrypted data to recreate the original sensitive data S. As mentioned in the foregoing, such randomization of the data into individually unusable encrypted portions increases*

security and provides for maintained trust in the data even if one of the data storage facilities, D1 through D4, is compromised" and See Goldwasser column 4, lines 9-21 and lines 31-46, "In preferred embodiments, the encrypted information is divided into a plurality of portions separately escrowed with different trustees of the first entity. The first entity is the government and the trustees are obligated under certain conditions to disclose the escrowed portions to the government, whereby the government can monitor the encrypted communications. At least a predetermined number of the escrowed portions must be combined to achieve recovery within the predetermined level of computational difficulty. The computational difficulty required to recover the encrypted communication decreases with increasing numbers of escrowed portions combined to achieve recovery" and "In preferred embodiments of the verifiable partial key escrow method, the first information (e.g., a portion of the secret key) provided to the first entity comprises information about a disclosed portion of the secret key, and there remains an undisclosed portion of the secret key. The disclosed portion is divided into a plurality of portions separately escrowed with different trustees. The verification information is used to verify the size of the undisclosed portion and that the disclosed portion is a part of the secret key. The disclosed portion may comprise some of the bits of the secret key, and the verification information may be used to verify that the number of undisclosed bits is small enough to permit recovery to be within the predetermined level of computational difficulty, and that the disclosed bits are part of the secret key. The first entity must gain possession of a predetermined minimum number of the escrowed portions before the undisclosed portion of the secret key can be recovered within the predetermined level of computational difficulty"*}*.*

18. **As per dependent claim 7 and 21 the combination of Dickinson and Bolosky discloses a system/method as applied to claims above. Furthermore Dickinson discloses the method/system, wherein, storing the plurality of data chunks together with the plurality of obfuscated different encryption keys comprises including, with a data chunk of the plurality of data chunks, data indicative of an encryption key that was used to encrypt a different data chunk of the plurality of data chunks. [See figure 8, 835, and** *See page 21, lines 10-14, "Based on the foregoing, the data splitting process 800 advantageously places/stores portions of the sensitive data in each of the four data storage facilities D1 through D4, such that no single data storage facility D1 through D4 includes sufficient encrypted data to recreate the original sensitive data S. As mentioned in the foregoing, such randomization of the data into individually unusable encrypted portions increases security and provides for maintained trust in the data even if one of the data storage facilities, D1 through D4, is compromised" and See Goldwasser column 4, lines 9-21 and lines 31-46,* "In preferred embodiments, the encrypted information is divided into a plurality of portions separately escrowed with different trustees of the first entity. The first entity is the government and the trustees are obligated under certain conditions to disclose the escrowed portions to the government, whereby the government can monitor the encrypted communications. At least a predetermined number of the escrowed portions must be combined to achieve recovery within the predetermined level of computational difficulty. The computational difficulty required to recover the encrypted communication decreases with increasing numbers of escrowed portions combined to achieve recovery" and "In preferred embodiments of the verifiable partial key escrow method, the first information (e.g., a portion of the secret key) provided to the first entity comprises information about a disclosed portion of the secret key, and there remains an undisclosed portion of the secret key. The disclosed portion is divided into a plurality of portions separately

escrowed with different trustees. The verification information is used to verify the size of the undisclosed portion and that the disclosed portion is a part of the secret key. The disclosed portion may comprise some of the bits of the secret key, and the verification information may be used to verify that the number of undisclosed bits is small enough to permit recovery to be within the predetermined level of computational difficulty, and that the disclosed bits are part of the secret key. The first entity must gain possession of a predetermined minimum number of the escrowed portions before the undisclosed portion of the secret key can be recovered within the predetermined level of computational difficulty"*]*.

19. **As per dependent claim 8 the combination of Dickinson and Bolosky discloses a system/method as applied to claims above. Furthermore Dickinson discloses the method/system, wherein, distributing the data set into a plurality of data chunks comprises using a random technique or pseudorandom technique.** *[See page 20, lines 10-11, 'the data stored in each data storage facility is randomized and undecipherable, comprises of any individual data storage facility does not necessarily comprises the sensitive data. See page 21, lines 10-14, "Based on the foregoing, the data splitting process 800 advantageously places portions of the sensitive data in each of the four data storage facilities D1 through D4, such that no single data storage facility D1 through D4 includes sufficient encrypted data to recreate the original sensitive data S. As mentioned in the foregoing, such randomization of the data into individually unusable encrypted portions increases security and provides for maintained trust in the data even if one of the data storage facilities, D1 through D4, is compromised".See also figure 8, 825 and 830 wherein each chunk of data S is encrypted or XORed with the key such as a random numbers A and C]*

20. **As per dependent claim 9 the combination of Dickinson and Bolosky discloses a system/method as applied to claims above. Furthermore Dickinson discloses the method/system, further comprising generating the data set by encrypting primary data** *[See page 20, lines 10-11, 'the data stored in each data storage facility is randomized and undecipherable, comprises of any individual data storage facility does not necessarily comprises the sensitive data. See page 21, lines 10-14, "Based on the foregoing, the data splitting process 800 advantageously places portions of the sensitive data in each of the four data storage facilities D1 through D4, such that no single data storage facility D1 through D4 includes sufficient encrypted data to recreate the original sensitive data S. As mentioned in the foregoing, such randomization of the data into individually unusable encrypted portions increases security and provides for maintained trust in the data even if one of the data storage facilities, D1 through D4, is compromised".See also figure 8, 825 and 830 wherein each chunk of data S is encrypted or XORed with the key such as a random numbers A and C. See also Goldwasser, see at least column 4, lines 9-21"*In preferred embodiments, the encrypted information is divided into a plurality of portions separately escrowed with different trustees of the first entity. The first entity is the government and the trustees are obligated under certain conditions to disclose the escrowed portions to the government, whereby the government can monitor the encrypted communications. At least a predetermined number of the escrowed portions must be combined to achieve recovery within the predetermined level of computational difficulty. The computational difficulty required to recover the encrypted communication decreases with increasing numbers of escrowed portions combined to achieve recovery"*]*

21. **As per dependent claim 11, dependent claim 11 is rejected for the same reason/rational as that of the above dependent claim 4.**

22. **As per dependent claim 12, dependent claim 12 is also rejected for the same reason/rational as that of the above independent claim 6.**

23. **As per dependent claim 13, dependent claim 13 is also rejected for the same reason/rational as that of the above independent claim 7.**

24. **As per dependent claim 14 the combination of Dickinson and Bolosky discloses a system/method as applied to claims above. Furthermore Dickinson discloses the method/system, wherein, distributing the data set into a plurality of data chunks comprises using a random technique or pseudorandom technique.** *[See page 20, lines 10-11, 'the data stored in each data storage facility is randomized and undecipherable, comprises of any individual data storage facility does not necessarily comprises the sensitive data. See page 21, lines 10-14, "Based on the foregoing, the data splitting process 800 advantageously places portions of the sensitive data in each of the four data storage facilities D1 through D4, such that no single data storage facility D1 through D4 includes sufficient encrypted data to recreate the original sensitive data S. As mentioned in the foregoing, such randomization of the data into individually unusable encrypted portions increases security and provides for maintained trust in the data even if one of the data storage facilities, D1 through D4, is compromised".See also*

figure 8, 825 and 830 wherein each chunk of data S is encrypted or XORed with the key such as a random numbers A and C]

25. **As per dependent claim 15 the combination of Dickinson and Bolosky discloses a system/method as applied to claims above. Furthermore Dickinson discloses the method/system, further comprising generating the data set by encrypting primary data** *[See page 20, lines 10-11, 'the data stored in each data storage facility is randomized and undecipherable, comprises of any individual data storage facility does not necessarily comprises the sensitive data. See page 21, lines 10-14, "Based on the foregoing, the data splitting process 800 advantageously places portions of the sensitive data in each of the four data storage facilities D1 through D4, such that no single data storage facility D1 through D4 includes sufficient encrypted data to recreate the original sensitive data S. As mentioned in the foregoing, such randomization of the data into individually unusable encrypted portions increases security and provides for maintained trust in the data even if one of the data storage facilities, D1 through D4, is compromised".See also figure 8, 825 and 830 wherein each chunk of data S is encrypted or XORed with the key such as a random numbers A and C. See also Goldwasser, see at least column 4, lines 9-21"*In preferred embodiments, the encrypted information is divided into a plurality of portions separately escrowed with different trustees of the first entity. The first entity is the government and the trustees are obligated under certain conditions to disclose the escrowed portions to the government, whereby the government can monitor the encrypted communications. At least a predetermined number of the escrowed portions must be combined to achieve recovery within the predetermined level of computational difficulty. The computational difficulty

required to recover the encrypted communication decreases with increasing numbers of escrowed portions combined to achieve recovery"*]*

26. **As per dependent claim 23, dependent claim 23 is rejected for the same reason/rational as that of the above dependent claim 4.**

27. **As per dependent claim 24, dependent claim 24 is also rejected for the same reason/rational as that of the above independent claim 6.**

28. **As per dependent claim 25, dependent claim 25 is also rejected for the same reason/rational as that of the above independent claim 7.**

29. Claims 5 **and 19** are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Alexander Dickinson (hereinafter referred to as Dickinson) (International Publication No. WO 01/22322 A2. (March 29, 2001) (This reference is cited in the IDS and submitted in the parent application) **in view William J. Bolosky (herein after referred as Bolosky) (US Publication No. 2002/0194209 A1) (Dec. 19, 2002) (This reference is cited in the IDS filed on October 18, 2019] and further** in view of Shafi GoldWasser (herein after referred as **GoldWasser)** (US Patent No. 5,768,388, Date of Patent: Jun 16, 1998)

30. **As per dependent claim 5 and 19 the combination of Dickinson and Bolosky discloses a system/method as applied to claims above. Furthermore Bolosky further discloses** when a computing device attempts to write a file to the distributed file system **150** and receives a write lock for a file or directory, the computing device generates a symmetric encryption key called the "lock-secret key." The computing device breaks the **lock-secret key into multiple pieces and distributes the pieces to the directory servers using a cryptographic secret sharing technique**. [See paragraphs 0139 and 0132]

The combination of Dickinson and Bolosky doesn't explicitly disclose S**hamir's Secret Sharing algorithm** to data indicative of at least one of the plurality of different encryption keys. Or the limitation: "wherein obfuscating each of the plurality of different encryption keys comprises applying Shamir's Secret Sharing algorithm to data indicative of at least one of the plurality of different encryption keys"

However, GoldWasser on at least column 2, lines 60-*column 3, lines 5 and also column 4, lines 9-21 discloses the following that meets the above limitation,*

"*Encrypt for each pair T_i^P, the first member of the pair t.sub.f[1] using key K_i of "short" length (i.e that is feasible for the government to recover for individual wiretaps), using one of the encryption algorithms E discussed in the previous section . Let $C_i = E(t_i^1)$. Now the users "escrows" C_i for all i=1 . . . L. The escrow can be done as a split-key escrow by sharing C_i* ***using a shamir secret-sharing scheme among the trustees****, or any other secret sharing scheme, or simply sending the entire C_i for all i to the government (if there is only one trustee)"*

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to implement in the system of Dickinson and Bolosky, a mechanism such as "obfuscating each of the plurality of different encryption keys comprises applying **Shamir's Secret Sharing algorithm** to data indicative of at least one of the plurality of different encryption keys" as taught by GoldWasser because this would enhance and strengthen the security of the system by keeping the secrecy of the encryption/decryption key by applying one of the known secret sharing algorithm. [See GoldWasser at least column 2, lines 60-*column 3, lines 5 and also column 4, lines 9-21*]

Conclusion

Applicant's submission of **an information disclosure statement under 37 CFR 1.97(c) with** the fee set forth in 37 CFR 1.17(p) on 11/08/2019 prompted the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 609.04(b). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SAMSON B LEMMA whose telephone number is 571-272-3806. The examiner can normally be reached on M-F 8am-10pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor Yin-Chen Shaw can be reached on 571-272-8593. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

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).

/SAMSON B LEMMA/
Primary Examiner, Art Unit 2498

Notice of References Cited	Application/Control No. 15/977,748	Applicant(s)/Patent Under Reexamination O'Hare et al.	
	Examiner SAMSON B LEMMA	Art Unit 2498	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-7043637-B2	05-2006	Bolosky; William J.	H04L9/0656	713/171
	B					
	C					
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/977,748	O'Hare et al.
	Examiner	**Art Unit**
	SAMSON B LEMMA	2498

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

CLAIMS

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

CLAIM		DATE								
Final	Original	04/05/2019	01/15/2020							
	1	-	-							
	2	✓	✓							
	3	✓	✓							
	4	✓	✓							
	5	✓	✓							
	6	✓	✓							
	7	✓	✓							
	8	✓	✓							
	9	✓	✓							
	10	✓	✓							
	11	✓	✓							
	12	✓	✓							
	13	✓	✓							
	14	✓	✓							
	15	✓	✓							
	16	✓	✓							
	17	✓	✓							
	18	✓	✓							
	19	✓	✓							
	20	✓	✓							
	21	✓	✓							
	22	✓	✓							
	23	✓	✓							
	24	✓	✓							
	25	✓	✓							

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/977,748	O'Hare et al.
	Examiner	Art Unit
	SAMSON B LEMMA	2498

CPC - Searched*		
Symbol	**Date**	**Examiner**
H04L63/04;0428;08;0823;0876	04/05/2019	SL
G06F21/602;606;62;6218	04/05/2019	SL
H04L9/085;3226;3263	04/05/2019	SL
H04L2209/80	04/05/2019	SL

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

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**
726	5	04/05/2019	SL

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

Search Notes		
Search Notes	**Date**	**Examiner**
H04L63/$, G06F21/$, H04L9/$, H04L2209/$, 726/$ (With text Search)	01/15/2020	SL
East (See attachment)	01/15/2020	SL
NPL (IEEE, ACM DIGITAL LIBRARY, GOOGLE, GOOGLE PATENT, GOOGLE SCHOLAR, IP.COM...)	01/15/2020	SL
INVENTOR NAME SEARCH	01/15/2020	SL

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/977,748	O'Hare et al.
	Examiner	Art Unit
	SAMSON B LEMMA	2498

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

October 18, 2019

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	15/977,748
				Filing Date	May 11, 2018
				First Named Inventor	Mark S. O'Hare
(Use as many sheets as necessary)				Art Unit	2498
				Examiner Name	Samson B. Lemma
Sheet	1	of	1	Attorney Docket Number	104093-0002-118

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		20020194209	12-19-2002	Bolosky	
		20100158244	06-24-2010	Sun	
		20110296440	12-01-2011	Laurich	
		20140201539	07-17-2014	Astigarraga	
		20150378842	12-31-2015	Tomlinson	
		8,644,502	02-04-2014	Orsini	
		9,275,071	03-01-2016	O'Hare	
		9,317,705	04-19-2016	O'Hare	
		9,338,140	05-10-2016	O'Hare	
		9,954,680	04-24-2018	Machani	
		10,108,807	10-23-2018	O'Hare	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

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.	T[1]

Examiner Signature	/SAMSON B LEMMA/	Date Considered	01/20/2020

*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.

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

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	12162	(plurality with (chunk$1 or portion or data$1 or block$1) with encrypt$) and distribut$5	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/01/19 21:32
L2	1167	(plurality with (chunk$1 or portion or data$1 or block$1) with encrypt$) same distribut$5 same stor$5	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/01/19 21:33
L3	575	(plurality with (chunk$1 or portion or data$1 or block$1) with encrypt$) same key same distribut$5 same stor$5	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/01/19 21:33
L4	576	(plurality with (chunk$1 or portion or data$1 or block$1) with (encrypt$ or obfuscat$5)) same key same distribut$5 same stor$5	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/01/19 21:34
L5	294	(plurality with (chunk$1 or portion or data$1 or block$1) with (encrypt$ or obfuscat$5)) same key same distribut$5 same stor$5 and (encrypt$ or obfuscat$5) with different with encrypt$ with key$1	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/01/19 21:36
L6	3	"20020194209"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/01/19 21:38
L8	3	"20020194209"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/01/19 21:38
L9	2	"20100158244"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/01/19 22:08
L10	3	"20110296440"	US-PGPUB; USPAT;	OR	OFF	2020/01/19 22:09

			USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
L11	3	"20140201539"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/01/19 23:08
L12	3	"20150378842"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/01/19 23:09
L14	2	("8644502").pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/01/19 23:09
L15	2	("9275071").pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/01/19 23:10
L16	6	("9317705").pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/01/19 23:10
L17	3	("9338140").pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/01/19 23:10
L18	5	("9954680").pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/01/19 23:10
L19	4	("10108807").pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/01/19 23:10
L22	3	"20020194209" and (encrypt$ or obfuscat$)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/01/19 23:12
L23	1	"20020194209" and (encrypt$ or obfuscat$) and reconstruct$	US-PGPUB; USPAT;	OR	OFF	2020/01/19 23:55

			USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
L24	1	"20020194209" and (encrypt$ or obfuscat$) and reconstruct$ and stor$5	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/01/19 23:57

EAST Search History (Interference)

< This search history is empty>

1/ 20/ 2020 12:42:21 AM
C:\ Users\ slemma\ Documents\ EAST\ Workspaces\ 16587641.wsp

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. 7200

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
15/977,748	05/11/2018 RULE	726	2498	104093-0002-118

APPLICANTS

Security First Corp., Rancho Santa Margarita, CA;

INVENTORS

Mark S. O'Hare, Coto De Caza, CA;
Rick L. Orsini, Flower Mound, TX;
Roger S. Davenport, Campbell, TX;
Steven Winick, Roslyn Heights, NY;

**** CONTINUING DATA ***************************

This application is a CON of 13/915,081 06/11/2013 PAT 9992170
which is a DIV of 13/468,383 05/10/2012 PAT 9338140
which is a CON of 11/258,839 10/25/2005 PAT 8266438
which claims benefit of 60/718,185 09/16/2005
and claims benefit of 60/622,146 10/25/2004

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

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****

06/04/2018

Foreign Priority claimed ❑ Yes ☑ No 35 USC 119(a-d) conditions met ❑ Yes ☑ No Verified and Acknowledged /SAMSON B LEMMA/ Examiner's Signature	❑ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		CA	68	24	4

ADDRESS

Haley Guiliano LLP (S&L)
75 Broad Street
Suite 1000
New York, NY 10004-3226
UNITED STATES

TITLE

SECURE DATA PARSER METHOD AND SYSTEM

FILING FEE RECEIVED	FEES: Authority has been given in Paper	❑ All Fees
3540	No._____ to charge/credit DEPOSIT ACCOUNT	❑ 1.16 Fees (Filing)
	No._____ for following:	❑ 1.17 Fees (Processing Ext. of time)
		❑ 1.18 Fees (Issue)
		❑ Other _____
		❑ Credit

BIB (Rev. 05/07).

October 18, 2019

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	15/977,748
				Filing Date	May 11, 2018
				First Named Inventor	Mark S. O'Hare
				Art Unit	2498
(Use as many sheets as necessary)				Examiner Name	Samson B. Lemma
Sheet	1	of	1	Attorney Docket Number	104093-0002-118

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		20020194209	12-19-2002	Bolosky	
		20100158244	06-24-2010	Sun	
		20110296440	12-01-2011	Laurich	
		20140201539	07-17-2014	Astigarraga	
		20150378842	12-31-2015	Tomlinson	
		8,644,502	02-04-2014	Orsini	
		9,275,071	03-01-2016	O'Hare	
		9,317,705	04-19-2016	O'Hare	
		9,338,140	05-10-2016	O'Hare	
		9,954,680	04-24-2018	Machani	
		10,108,807	10-23-2018	O'Hare	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

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.	T[1]

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.

Docket No.: 104093-0002-118

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	:	Security First Corp.	
Inventors	:	Mark S. O'Hare, et al.	
Application No.	:	15/977,748	Confirmation No.: 7200
Filed	:	May 11, 2018	
For	:	SECURE DATA PARSER METHOD AND SYSTEM	
Group Art Unit	:	2498	
Examiner	:	Samson B. Lemma	

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

REPLY TO OFFICE ACTION

Sir:

In response to the Office Action dated April 18, 2019, Applicant respectfully requests reconsideration in view of the following remarks:

Listing of the Claims begin on page 2 of this Reply.
Remarks begin on page 7 of this Reply.

LISTING OF THE CLAIMS

This listing will replace all prior version and listings of claims in the above-identified patent application.

Listing of the Claims

1. (Canceled)

2. (Previously Presented) A method for securing a data set, the method comprising:

distributing the data set into a plurality of data chunks, wherein none of the data chunks are, by themselves, sufficient to reconstruct the data set;

encrypting each of the data chunks with a respective one of a plurality of encryption keys;

obfuscating each of the plurality of different encryption keys; and

storing the plurality of data chunks with the plurality of obfuscated different encryption keys on a plurality of different storage devices.

3. (Previously Presented) The method of claim 2, wherein obfuscating each of the plurality of different encryption keys comprises performing a transform on data indicative of at least one of the plurality of different encryption keys.

4. (Previously Presented) The method of claim 3, wherein performing a transform on data indicative of at least one of the plurality of different encryption keys comprises performing an all-or-nothing transform on the data indicative of at least one of the plurality of different encryption keys.

5. (Previously Presented) The method of claim 2, wherein obfuscating each of the plurality of different encryption keys comprises applying Shamir's Secret Sharing algorithm to data indicative of at least one of the plurality of different encryption keys.

6. (Previously Presented) The method of claim 2, wherein storing the plurality of data chunks together with the plurality of obfuscated different encryption keys comprises storing each of the plurality of data chunks together with a respective one of the plurality of obfuscated different encryption keys.

7. (Previously Presented) The method of claim 2, wherein storing the plurality of data chunks together with the plurality of obfuscated different encryption keys comprises including, with a data chunk of the plurality of data chunks, data indicative of an encryption key that was used to encrypt a different data chunk of the plurality of data chunks.

8. (Previously Presented) The method of claim 2, wherein distributing the data set into a plurality of data chunks comprises using a random technique or pseudorandom technique.

9. (Previously Presented) The method of claim 2, further comprising generating the data set by encrypting primary data.

10. (Previously Presented) A method for securing a data set, the method comprising:

distributing the data set into a plurality of data chunks, wherein none of the data chunks are, by themselves, sufficient to reconstruct the data set;

encrypting each of the data chunks with a respective one of a plurality of encryption keys;

transforming each of the plurality of different encryption keys; and

storing the plurality of data chunks with the plurality of transformed different encryption keys on a plurality of different storage devices.

11. (Previously Presented) The method of claim 10, wherein transforming each of the plurality of different encryption keys comprises performing an all-or-nothing transform on data indicative of at least one of the plurality of different encryption keys.

12. (Previously Presented) The method of claim 10, wherein storing the plurality of data chunks with the plurality of transformed different encryption keys comprises storing each of the plurality of data chunks with a respective one of the plurality of transformed different encryption keys.

13. (Previously Presented) The method of claim 10, wherein storing the plurality of data chunks with the plurality of transformed different encryption keys comprises including, with a data chunk of the plurality of data chunks, data indicative of an encryption key of the plurality of encryption keys that was used to encrypt a different data chunk of the plurality of data chunks.

14. (Previously Presented) The method of claim 10, wherein distributing the data set into a plurality of data chunks comprises using a random technique or pseudorandom technique.

15. (Previously Presented) The method of claim 10, further comprising generating the data by encrypting primary data.

16. (Previously Presented) A computer system for securing a data set, the system comprising:

at least one hardware processor, configured to:

access the data set;

distribute the data set into a plurality of data chunks, wherein none of the data chunks are, by themselves, sufficient to reconstruct the data set;

encrypt each of the data chunks with a respective one of a plurality of encryption keys;

obfuscate each of the plurality of different encryption keys; and

storing the plurality of data chunks together with the plurality of obfuscated different encryption keys;

store the plurality of data chunks together with the plurality of obfuscated different encryption keys, wherein the plurality of data chunks is stored on a plurality of different storage devices.

17. (Previously Presented) The computer system of claim 16, wherein, when obfuscating each of the plurality of different encryption keys, the at least one hardware processor is configured to

perform a transform on data indicative of at least one of the plurality of different encryption keys.

18. (Previously Presented) The computer system of claim 17, wherein, when performing a transform on data indicative of at least one of the plurality of different encryption keys, the at least one hardware processor is configured to perform an all-or-nothing transform on the data indicative of at least one of the plurality of different encryption keys.

19. (Previously Presented) The computer system of claim 16, wherein, when obfuscating each of the plurality of different encryption keys, the at least one hardware processor is configured to apply Shamir's Secret Sharing algorithm to data indicative of at least one of the plurality of different encryption keys.

20. (Previously Presented) The computer system of claim 16, wherein, when storing the plurality of data chunks together with the plurality of obfuscated different encryption keys, the at least one hardware processor is configured to store each of the plurality of data chunks together with a respective one of the plurality of obfuscated different encryption keys.

21. (Previously Presented) The computer system of claim 16, wherein, when storing the plurality of data chunks together with the plurality of obfuscated different encryption keys, the at least one hardware processor is configured to include, with a data chunk of the plurality of data chunks, data indicative of an encryption key that was used to encrypt a different data chunk of the plurality of data chunks.

22. (Previously Presented) A computer system for securing a data set, the system comprising:

at least one hardware processor, configured to:

access the data set;

distribute the data set into a plurality of data chunks, wherein none of the data chunks are, by themselves, sufficient to reconstruct the data set;

encrypt each of the data chunks with a respective one of a plurality of encryption keys;

transform each of the plurality of different encryption keys; and

storing the plurality of data chunks together with the plurality of transformed different encryption keys;

store the plurality of data chunks together with the plurality of transformed different encryption keys, wherein the plurality of data chunks is stored on a plurality of different storage devices.

23. (Previously Presented) The computer system of claim 22, wherein, when transforming each of the plurality of different encryption keys, the at least one hardware processor is configured to perform an all-or-nothing transform on data indicative of at least one of the plurality of different encryption keys.

24. (Previously Presented) The computer system of claim 22, wherein, when storing the plurality of data chunks with the plurality of transformed different encryption keys, the at least one hardware processor is configured to store each of the plurality of data chunks with a respective one of the plurality of transformed different encryption keys.

25. (Previously Presented) The computer system of claim 22, wherein, when storing the plurality of data chunks with the plurality of transformed different encryption keys, the at least one hardware processor is configured to include, with a data chunk of the plurality of data chunks, data indicative of an encryption key of the plurality of encryption keys that was used to encrypt a different data chunk of the plurality of data chunks.

REMARKS

Introduction

Claims 2-25 are pending in this application.

Claims 2-25 are rejected under 35 U.S.C. § 103 as being unpatentable over Dickinson, PCT Publication No. WO 01/122322 A2 (hereinafter "Dickinson") in view of Goldwasser, U.S. Patent No. 5,768,388 (hereinafter "Goldwasser").

The Examiner's rejection is respectfully traversed.

Applicants' Response to 35 U.S.C. § 103 Rejection

Claims 2-25 are rejected under 35 U.S.C. § 103 as being unpatentable over Dickinson in view of Goldwasser.

Claim 2 is directed to securing a dataset. The method comprises distributing the data set into a plurality of data chunks, where none of the data chunks are (by themselves) sufficient to reconstruct the data set. Each respective data chunk is then encrypted with a respective encryption key of a plurality of encryption keys. Each of the keys is then obfuscated. The method further includes storing the plurality of data chunks with the plurality of obfuscated different encryption keys on a plurality of different storage devices.

Applicants respectfully submit that the combination of Dickinson and Goldwasser fails to teach or suggest encrypting each data chunk of data (that is, by itself, not sufficient to reconstruct the data) with a respective key, obfuscating each of these keys, and storing the obfuscated keys with the data chunks.

The Office Action relies on FIG. 8 of Dickinson (and associated technique described in page 21, lines 10-14 of Dickinson) as allegedly showing storage of obfuscated keys (with data chunks of data (that are not sufficient to reconstruct the data) encrypted by those keys. Office Action, p. 6. FIG. 8 of Dickinson is reproduced below for reference:

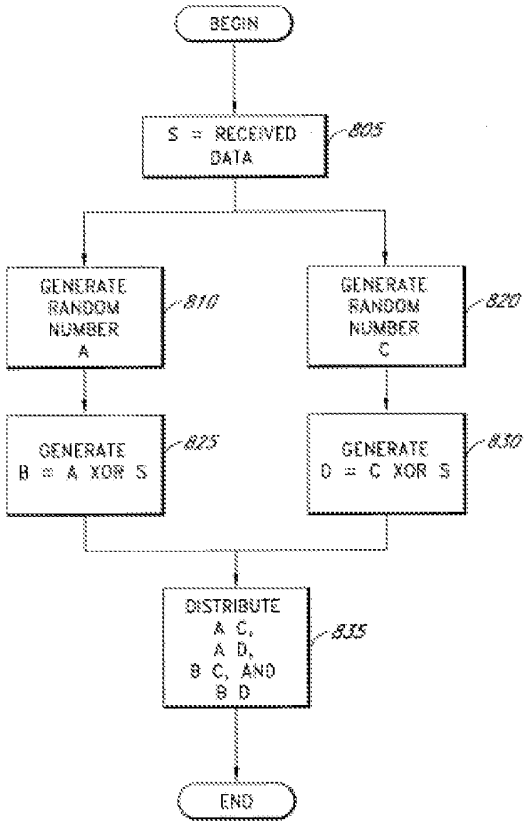


FIG. 8 of Dickinson

FIG. 8 of Dickinson shows a technique for securing received data S. First, random numbers A and C being generated. Then numbers B and D are generated as follows: B=A XOR S and D = C XOR S. Pairs A&C, A&D, B&C, and B&D are then distributed to storage.

The Office Action appears to equate numbers A and C with encryption keys, and received data "S" with chunks, as recited by claim 2.

First, Applicant notes that the XOR operation with A and B (even if, arguendo, A and B are encryption keys) is not performed on **chunks** of the dataset S that are not sufficient to reconstruct the data set S. Instead, the XOR operation with numbers A and B is performed on the **entire dataset S**. For at least this reason the technique of FIG. 8 cannot correspond to storing a plurality of data chunks with a plurality of obfuscated different encryption keys, because the techniques of FIG. 8 do not use encryption keys to encrypt **separate chunks** of the initial data set, much less obfuscate and store such keys, as required by claim 2.

Second, the technique of FIG. 8 cannot correspond to storing the plurality of data chunks with the plurality of obfuscated different encryption keys because, contrary to that that limitation, numbers A and C (to the extent they are keys) are stored in plain text without obfuscation (e.g., as parts of pairs A&C, B&D, and B&C).

Furthermore, Goldwasser fails to cure the aforementioned deficiency of Dickson. Goldwasser describes a secrete key being split into n pieces and escrowed with different trustees. Goldwasser col. 2: 10-15. However, such pieces of the key are not used by Goldwasser to encrypt different chunks of data. Instead, only the single complete key is used for data encryption. Therefore, storage of "n pieces" of a single key, as described by Goldwasser does not amount to storing the plurality of data chunks with the plurality of obfuscated different encryption keys that were used to encrypt those chunks, as required by claim 2.

For at least these reasons, Applicants respectfully submit that claim 2 is patentable over the combination of Dickinson and Goldwasser and respectfully requests withdrawal of § 103 rejection of claim 2. Claims 10, 16, and 22 were rejected for "for the same reason/rational as that of the above independent claim 2." Office Action, p. 9. Therefore, claims 10, 16, and 22 are patentable over the combination of Dickinson and Goldwasser for the similar reasons as recited above with respect to claim 2.

Applicants respectfully request withdrawal of the § 103 rejection of claims 2, 10, 16, 22, and all claims that depend from these independent claims.

Conclusion

In view of the above amendments and remarks, the pending application is in condition for allowance. Accordingly, reconsideration and prompt allowance are respectfully requested.

Applicant believes no fees are due with this response other than those on the Fee Transmittal filed herewith. However, if any additional fees are due, please charge our Deposit Account No. 06-1075, from which the undersigned is authorized to draw.

Dated: October 18, 2019

Respectfully submitted,

By: /Maxim Rapoport/
Maxim Rapoport
Registration No.: 67,675
HALEY GUILIANO LLP
75 Broad Street, Suite 1000
New York, New York 10004
(646) 973-2500
Attorney for Applicant

Electronic Patent Application Fee Transmittal

Application Number:	15977748
Filing Date:	11-May-2018
Title of Invention:	SECURE DATA PARSER METHOD AND SYSTEM
First Named Inventor/Applicant Name:	Mark S. O'Hare
Filer:	Maxim Rapoport/Maria Marley
Attorney Docket Number:	104093-0002-118

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 3 months with $0 paid	1253	1	1400	1400
Miscellaneous:				
SUBMISSION- INFORMATION DISCLOSURE STMT	1806	1	240	240
		Total in USD ($)		**1640**

Electronic Acknowledgement Receipt	
EFS ID:	37494437
Application Number:	15977748
International Application Number:	
Confirmation Number:	7200
Title of Invention:	SECURE DATA PARSER METHOD AND SYSTEM
First Named Inventor/Applicant Name:	Mark S. O'Hare
Customer Number:	15314
Filer:	Maxim Rapoport/Maria Marley
Filer Authorized By:	Maxim Rapoport
Attorney Docket Number:	104093-0002-118
Receipt Date:	18-OCT-2019
Filing Date:	11-MAY-2018
Time Stamp:	12:36:56
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$1640
RAM confirmation Number	E20190HC38010985
Deposit Account	061075
Authorized User	Maria Marley
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.16 (National application filing, search, and examination fees) 37 CFR 1.17 (Patent application and reexamination processing fees)	

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Extension of Time	104093-0002-118-EOT.pdf	130921 97c2eb4a404a45ecb2de1f923a2044c631be1110	no	1
Warnings:					
Information:					
2	Transmittal Letter	104093-0002-118-IDS.pdf	98763 1dc489da12a02de04c4bb71e7e69010b5da67e53	no	2
Warnings:					
Information:					
3	Information Disclosure Statement (IDS) Form (SB08)	104093-0002-118-SB08.pdf	152035 fc4ca8364f9ef63dce167a076d1abc5f63026b25	no	1
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
4		104093-0002-118-Reply.pdf	175484 2a53ae73eb1eed5fa9d37a9e98a146d1d350612a	yes	10

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Claims	2	6
Applicant Arguments/Remarks Made in an Amendment	7	10

Warnings:

Information:

5	Fee Worksheet (SB06)	fee-info.pdf	32454 9c687235b7c1077d895d685f5e6e482da04a2cac	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	589657	

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

PTO/AIA/22 (03-13)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)

Docket Number (Optional): 104093-0002-118

Application Number	15/977,748	Filed	May 11, 2018

For: SECURE DATA PARSER METHOD AND SYSTEM

Art Unit	2498	Examiner	Samson B. Lemma

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

		Fee	Small Entity Fee	Micro Entity Fee	
☐	One month (37 CFR 1.17(a)(1))	$200	$100	$50	$
☐	Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$
☒	Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$ 1,400.00
☐	Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐	Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☐ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 06-1075 .

☒ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant.

☒ attorney or agent of record. Registration number 67,675 .

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____ .

/Maxim Rapoport/ — Signature

October 18, 2019 — Date

Maxim Rapoport — Typed or printed name

646-973-2500 — Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☒ * Total of 1 forms are submitted.

Docket No.: 104093-0002-118

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	:	Security First Corp.	
Inventors	:	Mark S. O'Hare, et al.	
Application No.	:	15/977,748	Confirmation No.: 7200
Filed	:	May 11, 2018	
For	:	SECURE DATA PARSER METHOD AND SYSTEM	
Group Art Unit	:	2498	
Examiner	:	Samson B. Lemma	

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

INFORMATION DISCLOSURE STATEMENT

Sir:

Pursuant to 37 C.F.R. §§ 1.56, 1.97, and 1.98, applicant wishes to call the attention of the Examiner to the documents listed on the accompanying Form PTO/SB/08. It is respectfully requested that these documents be (1) fully considered by the United States Patent and Trademark Office during examination of this application and (2) printed on any patent which may issue on this application. Applicant requests that a copy of Form PTO/SB/08, as considered and initialed by the Examiner, be returned with the next communication.

In accordance with 37 C.F.R. § 1.98(a)(2)(ii), no copies of the listed U.S. patent documents are being submitted.

Applicant reserves the right to establish the patentability of the claimed invention over any of the information provided herewith, and/or to prove that this information may not be prior art, and/or to prove that this information may not be enabling for the teachings purportedly offered.

This Information Disclosure Statement is being filed after the mailing date of the first Office Action on the merits, but before the mailing date of either a final action under 37 C.F.R. § 1.113, or a notice of allowance under 37 C.F.R. § 1.311. Accordingly, a fee for filing this Statement is required. The Director is hereby authorized to charge payment of the fee and any additional fees required in connection with this Information Disclosure Statement to Deposit Account No. 06-1075, under Order No. 104093-0002-118.

Consideration of the foregoing in relation to this patent application is respectfully requested.

Respectfully submitted,

Date: October 18, 2019

/Maxim Rapoport/
Maxim Rapoport
Registration No. 67,675
HALEY GUILIANO LLP
Customer No. 15314
75 Broad Street
Suite 1000
New York, New York 10004
(646) 973-2500
Attorney for Applicant

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.
15/977,748	05/11/2018	Mark S. O'Hare	104093-0002-118	7200

15314 7590 04/18/2019

Haley Guiliano LLP
75 Broad Street
Suite 1000
New York, NY 10004

EXAMINER	
LEMMA, SAMSON B	

ART UNIT	PAPER NUMBER
2498	

NOTIFICATION DATE	DELIVERY MODE
04/18/2019	ELECTRONIC

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

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

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

haleyguiliano_PAIR@firsttofile.com
hgpatentdocket@hglaw.com

Office Action Summary	Application No. 15/977,748	Applicant(s) O'Hare et al.	
	Examiner SAMSON B LEMMA	Art Unit 2498	AIA (FITF) Status No

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

Period for Reply

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

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

Status

1)☑ Responsive to communication(s) filed on 05/11/2018.

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

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

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

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

Disposition of Claims*

5) ☑ Claim(s) 2-25 is/are pending in the application.

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

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 2-25 is/are rejected.

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

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

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

Application Papers

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

11)☑ The drawing(s) filed on 05/11/2018/ is/are: a)☑ accepted or b)☐ objected to by the Examiner.

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

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

Priority under 35 U.S.C. § 119

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

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

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

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

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

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

Attachment(s)

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

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

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

4) ☐ Other: _____.

DETAILED ACTION

1. This office action is in reply to an application No. 15/977,748 filed on 05/11/2018. Claims 2-25 are submitted/ presented for examination. Claims 2, 10, 16 and 22 are independent.

Notice of Pre-AIA or AIA Status

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

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

Preliminary Amendment

4. The preliminary amendment filed on 09/06/2018 is acknowledged. Accordingly claim 1 is cancelled and new claims 2-25 are submitted/ presented for examination. Claims 2, 10, 16 and 22 are independent.

Priority

5. This application filed 05/11/2018 is a continuation of 13915081, filed 06/11/2013 ,now U.S. Patent #9992170 and having 3 RCE-type filings therein 13915081 is a division of 13468383, filed 05/10/2012 ,now U.S. Patent #9338140 and having 2 RCE-type filings

therein 13468383 is a continuation of 11258839, filed 10/25/2005 ,now U.S. Patent #8266438 and having 1 RCE-type filing therein 11258839 Claims Priority from Provisional Application 60718185, filed 09/16/2005 11258839 Claims Priority from **Provisional Application 60622146, filed 10/25/2004.**

Information Disclosure Statement

6. The information disclosure statements (IDS) submitted on 05/11/2018 has been considered. The submission is in compliance with the provisions of 37 CFR 1.97. Form PTO-1449 is signed and attached hereto.

Drawings

7. The drawings filed on May 11, 2018 are accepted.

Specification

8. The specification filed on May 11, 2018 is also accepted.

Claim Rejections - 35 USC § 103

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

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject

matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 2-25 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Alexander Dickinson (hereinafter referred to as Dickinson) (International Publication No. WO 01/22322 A2. (March 29, 2001)(This reference is cited in the IDS and submitted in the parent application) in view of Shafi GoldWasser (herein after referred as GoldWasser) (US Patent No. 5,768,388, Date of Patent: Jun 16, 1998)

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

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

11. As per independent claim 2 Dickinson discloses as **method for securing a data set** *[See page 2, lines 25-30, "According to yet another aspect of the invention, the trust engine includes multiple depositories for storing portions of each cryptographic key and authentication data. The portions are created through a data splitting process that prohibits reconstruction without a predetermined portion from more than one depository. According to another embodiment, the multiple depositories are geographically remote such that a rogue employee or otherwise compromised system at one depository will not provide access to a user's key or authentication data."]***, the method comprising:**

distributing the data set into a plurality of data chunks, wherein none of the data chunks are, by themselves, sufficient to reconstruct the data set *[See figure 8, ref. 835, see at least page 20 lines 5-8, According to another embodiment of the invention, the depository system 700 comprises multiple geographically separated independent data storage systems. By distributing the sensitive data into distinct and independent storage facilities D1 through D4, some or all of which may be advantageously geographically separated, the depository system 700 provides redundancy along with additional security measures. For example, according to one embodiment, only data from two of the multiple data storage facilities, D1 through D4, are needed to decipher and reassemble the sensitive data. See also page 21, lines 10-14, Based on the foregoing, the data splitting process 800 advantageously places portions of the sensitive data in each of the four data storage facilities D1 through D4, such that no single data storage facility D1 through D4 includes sufficient encrypted data to recreate the original sensitive data S.]*;

encrypting each of the data chunks with a respective one of a plurality of encryption *keys [See page 20, lines 10-11, 'the data stored in each data storage facility is randomized and undecipherable, comprises of any individual data storage facility does not necessarily comprises the sensitive data. See page 21, lines 10-14, "Based on the foregoing, the data splitting process 800 advantageously places portions of the sensitive data in each of the four data storage facilities D1 through D4, such that no single data storage facility D1 through D4 includes sufficient encrypted data to recreate the original sensitive data S. As mentioned in the foregoing, such randomization of the data into individually unusable encrypted portions increases security and provides for maintained trust in the data even if one of the data storage facilities, D1 through D4, is*

compromised".See also figure 8, 825 and 830 wherein each chunk of data S is encrypted or XORed with the key such as a random numbers A and C]

obfuscating each of the plurality of different encryption keys [*See figure 8, 825 and 830 wherein each different keys such as random numbers A and B is obfuscated by the XOR operations***];**

and storing the plurality of data chunks with the plurality of obfuscated different encryption keys on a plurality of different storage devices [See figure 8, 835, and *See page 21, lines 10-14, "Based on the foregoing, the data splitting process 800 advantageously places/stores portions of the sensitive data in each of the four data storage facilities D1 through D4, such that no single data storage facility D1 through D4 includes sufficient encrypted data to recreate the original sensitive data S. As mentioned in the foregoing, such randomization of the data into individually unusable encrypted portions increases security and provides for maintained trust in the data even if one of the data storage facilities, D1 through D4, is compromised"]***.**

Dickinson substantially discloses all the limitation recited in the claim but even if it assumed that it does not explicitly disclose the limitation," **obfuscating each of the plurality of different encryption keys**"

GoldWasser discloses this particular limitation. For instance GoldWasser on column 4, lines 31-48 discloses the following that meets this broad claim limitation, "In preferred embodiments of the verifiable partial key escrow method, the first information (e.g., a portion of the secret key) provided to the first entity comprises information about a disclosed portion of the secret key, and there remains an undisclosed portion of the

secret key. The disclosed portion is divided into a plurality of portions separately escrowed with different trustees. The verification information is used to verify the size of the undisclosed portion and that the disclosed portion is a part of the secret key. The disclosed portion may comprise some of the bits of the secret key, and the verification information may be used to verify that the number of undisclosed bits is small enough to permit recovery to be within the predetermined level of computational difficulty, and that the disclosed bits are part of the secret key. The first entity must gain possession of a predetermined minimum number of the escrowed portions before the undisclosed portion of the secret key can be recovered within the predetermined level of computational difficulty"

Furthermore Goldwasser on column 4, lines 9-21 discloses the following that meets the rest of the claim limitation. "a method for securing a data set, the method comprising: distributing the data set into a plurality of data chunks, wherein none of the data chunks are, by themselves, sufficient to reconstruct the data set; encrypting each of the data chunks with a respective one of a plurality of encryption keys; obfuscating each of the plurality of different encryption keys; and storing the plurality of data chunks with the plurality of obfuscated different encryption keys on a plurality of different storage device"

"In preferred embodiments, the encrypted information is divided into a plurality of portions separately escrowed with different trustees of the first entity. The first entity is the government and the trustees are obligated under certain conditions to disclose the escrowed portions to the government, whereby the government can monitor the encrypted communications. At least a predetermined number of the escrowed portions must be combined to achieve recovery within the predetermined level of computational difficulty. The computational difficulty required to recover the encrypted communication

decreases with increasing numbers of escrowed portions combined to achieve recovery",[See at least column 4, lines 9-21]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to implement in the system of Dickinson, a mechanism such as "**obfuscating each of the plurality of different encryption keys**"" **as taught by** GoldWasser because this would enhance and strengthen the security of the system by keeping the secrecy of the encryption/decryption key by dividing and storing only portions of the encryption and decryption key in a pluralities of locations such in the secure Government agencies and when the decryption is required a certain number of the agencies which are location in a different locations could combine their portions of the key and able to decrypt and reconstruct the secret data. [GoldWasser, see at least column 4, lines 9-21 and column 2, lines 10-40]

12. **As per independent claim 10, independent claim 10 is rejected for the same reason/rational as that of the above independent claim 2.**

13. **As per independent claim 16, independent claim 16 is also rejected for the same reason/rational as that of the above independent claim 2.**

14. **As per independent claim 22, independent claim 22 is rejected for the same reason/rational as that of the above independent claim 2.**

15. **As per dependent claim 3 and 17 the combination of Dickinson and Goldwasser discloses a system/method as applied to claims above. Furthermore Dickinson discloses the method/system, wherein obfuscating each of the plurality of different encryption keys comprises performing a transform on data indicative of at least one of the plurality of different encryption keys. [***See figure 8, 825 and 830 wherein each different keys such as random numbers A and B is obfuscated by the XOR operations***]**

16. **As per dependent claim 4 and 18 the combination of Dickinson and Goldwasser discloses a system/method as applied to claims above. Furthermore Dickinson discloses the method/system, wherein performing a transform on data indicative of at least one of the plurality of different encryption keys comprises performing an all-or-nothing transform on the data indicative of at least one of the plurality of different encryption keys.** *[See figure 8, 825 and 830 wherein each different keys such as random numbers A and B is obfuscated by the XOR operations]*

17. **As per dependent claim 5 and 19 the combination of Dickinson and Goldwasser discloses a system/method as applied to claims above. Furthermore Goldwasser discloses the method/system, wherein obfuscating each of the plurality of different encryption keys comprises applying Shamir's Secret Sharing algorithm to data indicative of at least one of the plurality of different encryption keys [*See at least column 2, lines 60-column 3, lines 5 and also column 4, lines 9-21,* *Encrypt for each pair T_i ^{P}, the first member of the pair t.sub.f ^{1} using key K_i of "short" length (i.e that is feasible for the government to recover for individual wiretaps), using one of the encryption algorithms E discussed in the previous section . Let C_i =E(t_i ^{1}). Now the users "escrows" C_i for all i=1 . . . L. The escrow can be done as a split-key escrow by sharing C_i **using a shamir secret-sharing scheme among the trustees**, or any other secret sharing scheme, or simply sending the entire C_i for all i to the government (if there is only one trustee).*

18. **As per dependent claim 6 and 20 the combination of Dickinson and Goldwasser discloses a system/method as applied to claims above. Furthermore Dickinson discloses the method/system, wherein storing the plurality of data chunks together with the plurality of obfuscated different encryption keys comprises storing each of the plurality of data chunks together with a respective one of the plurality of obfuscated different encryption keys [See figure 8, 835, and** *See page 21, lines 10-14, "Based on the foregoing, the data splitting process 800 advantageously places/stores portions of the sensitive data in each of the four data storage facilities D1 through D4, such that no single data storage facility D1 through D4 includes sufficient encrypted data to recreate the original sensitive data S. As mentioned in the foregoing, such randomization of the data into individually unusable encrypted portions increases security and provides for maintained trust in the data even if one of the data storage*

facilities, D1 through D4, is compromised" and See Goldwasser column 4, lines 9-21 and lines 31-46, "In preferred embodiments, the encrypted information is divided into a plurality of portions separately escrowed with different trustees of the first entity. The first entity is the government and the trustees are obligated under certain conditions to disclose the escrowed portions to the government, whereby the government can monitor the encrypted communications. At least a predetermined number of the escrowed portions must be combined to achieve recovery within the predetermined level of computational difficulty. The computational difficulty required to recover the encrypted communication decreases with increasing numbers of escrowed portions combined to achieve recovery" and "In preferred embodiments of the verifiable partial key escrow method, the first information (e.g., a portion of the secret key) provided to the first entity comprises information about a disclosed portion of the secret key, and there remains an undisclosed portion of the secret key. The disclosed portion is divided into a plurality of portions separately escrowed with different trustees. The verification information is used to verify the size of the undisclosed portion and that the disclosed portion is a part of the secret key. The disclosed portion may comprise some of the bits of the secret key, and the verification information may be used to verify that the number of undisclosed bits is small enough to permit recovery to be within the predetermined level of computational difficulty, and that the disclosed bits are part of the secret key. The first entity must gain possession of a predetermined minimum number of the escrowed portions before the undisclosed portion of the secret key can be recovered within the predetermined level of computational difficulty"*]*.

19. As per dependent claim 7 and 21 the combination of Dickinson and Goldwasser discloses a system/method as applied to claims above. Furthermore Dickinson

discloses the method/system, wherein, storing the plurality of data chunks together with the plurality of obfuscated different encryption keys comprises including, with a data chunk of the plurality of data chunks, data indicative of an encryption key that was used to encrypt a different data chunk of the plurality of data chunks. [See figure 8, 835, and *See page 21, lines 10-14, "Based on the foregoing, the data splitting process 800 advantageously places/stores portions of the sensitive data in each of the four data storage facilities D1 through D4, such that no single data storage facility D1 through D4 includes sufficient encrypted data to recreate the original sensitive data S. As mentioned in the foregoing, such randomization of the data into individually unusable encrypted portions increases security and provides for maintained trust in the data even if one of the data storage facilities, D1 through D4, is compromised" and See Goldwasser column 4, lines 9-21 and lines 31-46,* "In preferred embodiments, the encrypted information is divided into a plurality of portions separately escrowed with different trustees of the first entity. The first entity is the government and the trustees are obligated under certain conditions to disclose the escrowed portions to the government, whereby the government can monitor the encrypted communications. At least a predetermined number of the escrowed portions must be combined to achieve recovery within the predetermined level of computational difficulty. The computational difficulty required to recover the encrypted communication decreases with increasing numbers of escrowed portions combined to achieve recovery" and "In preferred embodiments of the verifiable partial key escrow method, the first information (e.g., a portion of the secret key) provided to the first entity comprises information about a disclosed portion of the secret key, and there remains an undisclosed portion of the secret key. The disclosed portion is divided into a plurality of portions separately escrowed with different trustees. The verification information is used to verify the size of the undisclosed portion and that the disclosed portion is a part of the secret key. The

disclosed portion may comprise some of the bits of the secret key, and the verification information may be used to verify that the number of undisclosed bits is small enough to permit recovery to be within the predetermined level of computational difficulty, and that the disclosed bits are part of the secret key. The first entity must gain possession of a predetermined minimum number of the escrowed portions before the undisclosed portion of the secret key can be recovered within the predetermined level of computational difficulty"*]*.

20. **As per dependent claim 8 the combination of Dickinson and Goldwasser discloses a system/method as applied to claims above. Furthermore Dickinson discloses the method/system, wherein, distributing the data set into a plurality of data chunks comprises using a random technique or pseudorandom technique.** *[See page 20, lines 10-11, 'the data stored in each data storage facility is randomized and undecipherable, comprises of any individual data storage facility does not necessarily comprises the sensitive data. See page 21, lines 10-14, "Based on the foregoing, the data splitting process 800 advantageously places portions of the sensitive data in each of the four data storage facilities D1 through D4, such that no single data storage facility D1 through D4 includes sufficient encrypted data to recreate the original sensitive data S. As mentioned in the foregoing, such randomization of the data into individually unusable encrypted portions increases security and provides for maintained trust in the data even if one of the data storage facilities, D1 through D4, is compromised".See also figure 8, 825 and 830 wherein each chunk of data S is encrypted or XORed with the key such as a random numbers A and C]*

21. **As per dependent claim 9 the combination of Dickinson and Goldwasser discloses a system/method as applied to claims above. Furthermore Dickinson discloses the method/system, further comprising generating the data set by encrypting primary data** *[See page 20, lines 10-11, 'the data stored in each data storage facility is randomized and undecipherable, comprises of any individual data storage facility does not necessarily comprises the sensitive data. See page 21, lines 10-14, "Based on the foregoing, the data splitting process 800 advantageously places portions of the sensitive data in each of the four data storage facilities D1 through D4, such that no single data storage facility D1 through D4 includes sufficient encrypted data to recreate the original sensitive data S. As mentioned in the foregoing, such randomization of the data into individually unusable encrypted portions increases security and provides for maintained trust in the data even if one of the data storage facilities, D1 through D4, is compromised".See also figure 8, 825 and 830 wherein each chunk of data S is encrypted or XORed with the key such as a random numbers A and C. See also Goldwasser, see at least column 4, lines 9-21"* In preferred embodiments, the encrypted information is divided into a plurality of portions separately escrowed with different trustees of the first entity. The first entity is the government and the trustees are obligated under certain conditions to disclose the escrowed portions to the government, whereby the government can monitor the encrypted communications. At least a predetermined number of the escrowed portions must be combined to achieve recovery within the predetermined level of computational difficulty. The computational difficulty required to recover the encrypted communication decreases with increasing numbers of escrowed portions combined to achieve recovery*"]*

22. **As per dependent claim 11, dependent claim 11 is rejected for the same reason/rational as that of the above dependent claim 4.**

23. **As per dependent claim 12, dependent claim 12 is also rejected for the same reason/rational as that of the above independent claim 6.**

24. **As per dependent claim 13, dependent claim 13 is also rejected for the same reason/rational as that of the above independent claim 7.**

25. **As per dependent claim 14 the combination of Dickinson and Goldwasser discloses a system/method as applied to claims above. Furthermore Dickinson discloses the method/system, wherein, distributing the data set into a plurality of data chunks comprises using a random technique or pseudorandom technique.** *[See page 20, lines 10-11, 'the data stored in each data storage facility is randomized and undecipherable, comprises of any individual data storage facility does not necessarily comprises the sensitive data. See page 21, lines 10-14, "Based on the foregoing, the data splitting process 800 advantageously places portions of the sensitive data in each of the four data storage facilities D1 through D4, such that no single data storage facility D1 through D4 includes sufficient encrypted data to recreate the original sensitive data S. As mentioned in the foregoing, such randomization of the data into individually unusable encrypted portions increases security and provides for maintained trust in the data even if one of the data storage facilities, D1 through D4, is compromised".See also figure 8, 825 and 830 wherein each chunk of data S is encrypted or XORed with the key such as a random numbers A and C]*

26. **As per dependent claim 15 the combination of Dickinson and Goldwasser discloses a system/method as applied to claims above. Furthermore Dickinson discloses the method/system, further comprising generating the data set by encrypting primary data** *[See page 20, lines 10-11, 'the data stored in each data storage facility is randomized and undecipherable, comprises of any individual data storage facility does not necessarily comprises the sensitive data. See page 21, lines 10-14, "Based on the foregoing, the data splitting process 800 advantageously places portions of the sensitive data in each of the four data storage facilities D1 through D4, such that no single data storage facility D1 through D4 includes sufficient encrypted data to recreate the original sensitive data S. As mentioned in the foregoing, such randomization of the data into individually unusable encrypted portions increases security and provides for maintained trust in the data even if one of the data storage facilities, D1 through D4, is compromised".See also figure 8, 825 and 830 wherein each chunk of data S is encrypted or XORed with the key such as a random numbers A and C. See also Goldwasser, see at least column 4, lines 9-21"*In preferred embodiments, the encrypted information is divided into a plurality of portions separately escrowed with different trustees of the first entity. The first entity is the government and the trustees are obligated under certain conditions to disclose the escrowed portions to the government, whereby the government can monitor the encrypted communications. At least a predetermined number of the escrowed portions must be combined to achieve recovery within the predetermined level of computational difficulty. The computational difficulty required to recover the encrypted communication decreases with increasing numbers of escrowed portions combined to achieve recovery"*]*

27. **<u>As per dependent claim 23</u>, dependent claim 23 is rejected for the same reason/rational as that of the above dependent claim 4.**

28. **<u>As per dependent claim 24,</u> dependent claim 24 is also rejected for the same reason/rational as that of the above independent claim 6.**

29. **<u>As per independent claim 25,</u> dependent claim 25 is also rejected for the same reason/rational as that of the above independent claim 7.**

Conclusion

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

A. US Patent No. 6,088,454 to Nagashima on at least figure 2 discloses storing member keys K11, K12,… K1n to reconstruct/decrypt a data set/message in different apparatus/locations such as 11b, 11c,... 11d than the assigned receiving locations.FIG. 2 shows the arrangement of an encryption system in which the secret key K in the first embodiment is a decrypting key. The second embodiment is the same as

the first embodiment except that reference symbol K.sub.0 denotes a decrypting key of a group; and K.sub.11, K.sub.12, . . . , K.sub.1n, pieces of partial information of the decrypting key K.sub.0. The representative (member 0) can decrypt an encrypted sentence addressed to the group or encrypted message as data held by the group by himself/herself. However, a general member I.sub.i can decrypt an encrypted sentence addressed to the group only when a predetermined number t.sub.1 or more of members consent, each member then performs decrypting processing by using partial information K.sub.1i secretly held by each member, and the respective decrypting results are synthesized. The encrypted sentence cannot be decrypted by t.sub.1 -1 or less general members.

B. US Patent No. 8,788,803 to Irvine discloses a method of protecting data in a peer-to-peer network of a plurality of nodes, comprising: splitting the data into a plurality of data chunks of one or more sizes, wherein the one or more sizes are randomly calculated based on the data; obfuscating first, second and third data chunks of the plurality of data chunks by swapping a first byte of the first data chunk with a first byte of the second data chunk, a second byte of the second data chunk with a first byte of the third data chunk, and a second byte of the third chunk with the second byte of the first chunk till all bytes of the first, second and third data chunks are swapped, and repeating the swapping by same number of times as there are chunks, wherein obfuscating the data chunks leads to mixing UP of content of the data chunks, thereby ensuring that the data is rendered useless without presence of all the data chunks; and encrypting the plurality of obfuscated data chunks, wherein a hash value of a given data chunk of the plurality of obfuscated data chunks is used as an input to an encryption algorithm to encrypt a next given data chunk of the plurality of obfuscated data chunks; and naming the plurality of encrypted obfuscated data chunks using corresponding hash values of the data chunks.

C. See the other cited references.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SAMSON B LEMMA whose telephone number is 571-272-3806. The examiner can normally be reached on M-F 8am-10pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Shaw Yin Chen can be reached on 571-272-8593. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

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.

/SAMSON B LEMMA/
Primary Examiner, Art Unit 2498

Notice of References Cited	Application/Control No. 15/977,748	Applicant(s)/Patent Under Reexamination O'Hare et al.	
	Examiner SAMSON B LEMMA	Art Unit 2498	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-5768388-A	06-1998	Goldwasser; Shafi	H04L9/0894	380/286
*	B	US-7916871-B2	03-2011	Brookner; George M.	H04L9/085	380/279
*	C	US-20050111657-A1	05-2005	Lee, Kyung-hee	H04L9/085	380/28
*	D	US-6088454-A	07-2000	Nagashima; Takayuki	H04L9/0836	380/277
*	E	US-8788803-B2	07-2014	Irvine; David	G06F21/6218	713/150
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/977,748	O'Hare et al.
	Examiner	Art Unit
	SAMSON B LEMMA	2498

CPC - Searched*		
Symbol	Date	Examiner
H04L63/04;0428;08;0823;0876	04/05/2019	SL
G06F21/602;606;62;6218	04/05/2019	SL
H04L9/085;3226;3263	04/05/2019	SL
H04L2209/80	04/05/2019	SL

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner
726	5	04/05/2019	SL

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

Search Notes		
Search Notes	Date	Examiner
H04L63/$, G06F21/$, H04L9/$, H04L2209/$, 726/$ (With text Search)	04/05/2019	SL
East (See attachment)	04/05/2019	SL
NPL (IEEE, ACM DIGITAL LIBRARY, GOOGLE, GOOGLE PATENT, GOOGLE SCHOLAR, IP.COM...)	04/05/2019	SL
INVENTOR NAME SEARCH	04/05/2019	SL

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

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/977,748	O'Hare et al.
	Examiner	**Art Unit**
	SAMSON B LEMMA	2498

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

CLAIMS

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

CLAIM		DATE								
Final	Original	04/05/2019								
	1	-								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								
	22	✓								
	23	✓								
	24	✓								
	25	✓								

Discover | Pats & Apps | dividing splitting plurality ... | + 0 mods | 0 filters

Visuals | Query | Results | 0 Selected | Sort: Relevance | Cut-off: None | De-dup: None

1 - 50 12,487,211 results

1. **Block encryption**

A method of storing a file is provided. The method includes splitting the file into a plurality of file chunks and encrypting each file chunk of the plurality of file chunks. The method also includes generating a first security key that decrypts a first encrypted file chunk of the plurality of...

CURRENT ASSIGNEES: UNSENE INC
US20140281513 | US APPLICATIONS | 18-SEP-2014

2. **Block encryption**

A method of storing a file is provided. The method includes splitting the file into a plurality of file chunks and encrypting each file chunk of the plurality of file chunks. The method also includes generating a first security key that decrypts a first encrypted file chunk of the plurality of...

CURRENT ASSIGNEES: UNSENE INC
US9356782 | US PATENTS | 31-MAY-2016

3. **Systems and methods for efficiently and securely storing data in a distributed data storage system**

The present disclosure discloses a method of storing data in a distributed data storage system, the distributed data storage system including a plurality of server and client nodes. The method includes receiving unencrypted data from a client node for storing at a server node. The received data is...

CURRENT ASSIGNEES: XANADU BIG DATA LLC
US10158483 | US PATENTS | 18-DEC-2018

4. **Accelerating stream cipher operations using single and grid systems**

Systems and methods for accelerating stream cipher encryption operations are described. In one aspect, a computer-implemented method receives data. The method separates the data into multiple file chunks for compression. A respective compression-encryption instructions header is provided for each...

CURRENT ASSIGNEES: KING SAUD UNIV
US20120089829 | US APPLICATIONS | 12-APR-2012

5. **Encryption system for peer-to-peer networks in which data is divided into chunks and self-encryption is applied**

A file is divided into chunks 2 and small data elements, such as bytes, are permuted between the chunks 3. Each chunk is hashed 4 to form a chunk hash, and each chunk hash is encrypted using one or more other chunk hashes 5 in a self-encryption process. Self-encryption involves obfuscation using...

CURRENT ASSIGNEES: DAVID IRVINE
GB2444343A | GREAT BRITAIN APPLICATIONS | 04-JUN-2008

6. **Communication system, user equipment, content source and method for secure content delivery**

A communication system, a user device, a content source and a method for secure content delivery are provided. A user device configured to request and receive data divided into chunks from a content source over a network, the device comprising: means for establishing a secure path to the content...

Top 1500 results

Relevance VIEW

0 Results
38 Results
1462 Results
0 Results
0 Results

Publication Date VIEW

1991 2019

Cur Assignee by Relevance VIEW

UNSENE INC **(2)**
XANADU BIG DATA LLC **(1)**
KING SAUD UNIV **(2)**
DAVID IRVINE **(12)**
FUJITSU LTD **(5)**
MAIDSAFE FNDN **(15)**
MICROSOFT TECH LICENSI... **(34)**
NEC LAB EUR **(10)**

View More Visualizations

Result #1 PREV NEXT

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. 7200

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
15/977,748	05/11/2018 **RULE**	726	2498	104093-0002-118

APPLICANTS
Security First Corp., Rancho Santa Margarita, CA;

INVENTORS
Mark S. O'Hare, Coto De Caza, CA;
Rick L. Orsini, Flower Mound, TX;
Roger S. Davenport, Campbell, TX;
Steven Winick, Roslyn Heights, NY;

** **CONTINUING DATA** *************************
This application is a CON of 13/915,081 06/11/2013 PAT 9992170
which is a DIV of 13/468,383 05/10/2012 PAT 9338140
which is a CON of 11/258,839 10/25/2005 PAT 8266438
which claims benefit of 60/718,185 09/16/2005
and claims benefit of 60/622,146 10/25/2004

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

** **IF REQUIRED, FOREIGN FILING LICENSE GRANTED** **
06/04/2018

		STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /SAMSON B LEMMA/ Examiner's Signature	☐ Met after Allowance Initials	CA	68	24	4

ADDRESS

Haley Guiliano LLP
75 Broad Street
Suite 1000
New York, NY 10004
UNITED STATES

TITLE

SECURE DATA PARSER METHOD AND SYSTEM

FILING FEE RECEIVED 3540	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

BIB (Rev. 05/07).

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	2	"20180367509"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:25
L6	7369	(H04L63/04).CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:27
L7	57040	(H04L63/0428).CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:28
L8	68740	(H04L63/08).CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:28
L9	31394	(H04L63/0823).CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:28
L10	16784	(H04L63/0876).CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:28
L11	14793	(G06F21/602).CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:28
L12	10738	(G06F21/606).CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:28
L13	12862	(G06F21/62).CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:28
L14	35337	(G06F21/6218).CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:28

L15	24218	(H04L2209/80).CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:29
L16	5441	(H04L9/085).CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:29
L17	14791	(H04L9/3263).CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:29
L18	14791	(H04L9/3263).CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:29
L19	6580	(@pd @rlad @ptad @prad @ad) < "20041025" and (split$4 or divid$4) with (chunk$1 or portion$1) and encrypt$	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:40
L20	820	(@pd @rlad @ptad @prad @ad) < "20041025" and (split$4 or divid$4) with (chunk$1 or portion$1) same encrypt$	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:41
L21	44	(@pd @rlad @ptad @prad @ad) < "20041025" and (split$4 or divid$4) with (chunk$1 or portion$1) with encrypt$ same distribut$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:42
L22	45	(@pd @rlad @ptad @prad @ad) < "20042510" and (split$4 or divid$4) with (chunk$1 or portion$1) with encrypt$ same distribut$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:43
L23	13	6 and 20	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:44
L24	127	20 and 7	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:44
L25	19	20 and 8	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:44
L26	36	20 and 9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:44

L27	0	20 and 10	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:44
L28	32	20 and 11	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:44
L29	49	20 and 12	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:44
L30	20	20 and 13	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:44
L31	25	20 and 14	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:44
L32	22	20 and 15	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:44
L33	39	20 and 16	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:44
L34	46	20 and 17	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:44
L35	46	20 and 18	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:44
L36	155	(split$4 or divid$4) with (chunk$1 or portion$1) with encrypt$ same distribut$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:45
L37	106	(split$4 or divid$4) with (chunk$1 or portion$1) with encrypt$ with distribut$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:45
L38	48	(split$4 or divid$4) with (chunk$1 or portion$1) with encrypt$ with stor$4 with distribut$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:45

L39	3	((split$4 or divid$4) with (chunk$1 or portion$1) with encrypt$ with stor$4 with distribut$4).ab.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:46
L40	12	((split$4 or divid$4) with (chunk$1 or portion$1) with encrypt$ with stor$4 with distribut$4).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/14 21:46

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L41	12	((split$4 or divid$4) with (chunk$1 or portion$1) with encrypt$ with stor$4 with distribut$4).clm.	US-PGPUB; USPAT	OR	OFF	2019/04/14 21:46

4/ 14/ 2019 9:47:01 PM
C:\ Users\ slemma\ Documents\ EAST\ Workspaces\ 15675324.wsp

Splitting knowledge of a password

E Brickell, K Chan - US Patent 6,959,394, 2005 - Google Patents

... As an alternative to the example given above for **dividing** the password into N **pieces** by ... to the expected entropy of the password (expressed as an integer number of bits) **divide** by N ... For example, if the expected entropy of the user password **divided** by N equals eight bits, then ...

☆ 99 Cited by 136 Related articles All 2 versions »

Distributed split-key cryptosystem and applications

S Micali - US Patent 6,026,163, 2000 - Google Patents

... having an initial entity who (1) computes a public-secret **key** pair, and (2) **divides** the secret ... corresponding to the combined public **key** from the individual secret **keys** of the **plurality** of trustees ... Secure login using a multifactor **split** asymmetric crypto-**key** with persistent **key** security ...

☆ 99 Cited by 152 Related articles All 2 versions »

Data delivery method and data delivery system using sets of passkeys generated by **dividing** an **encryption key**

S Kamiya, M Yamashita - US Patent 7,421,082, 2008 - Google Patents

... the latter are referred to as passkeys, and **keys** generated by further **dividing** a passkey ... this example, the **encryption key** used to **encrypt** the digital data is **divided**, or parsed ... server 15 registers newly accepted content, searches for and retrieves desired content, **divides** files, and ...

☆ 99 Cited by 67 Related articles All 4 versions »

Cryptographic **key split** binder for use with tagged data elements

CJ Wack, EM Scheidt, JL Kolouch - US Patent 7,095,852, 2006 - Google Patents

... H04L9/085—Secret sharing or secret **splitting**, eg threshold schemes ... For example, an individual or computer can lack a random **key split** (or random value seed), the one or ... create the cryptographic **key** by a recipient, and can include, for example, one or more **key splits**, one or ...

☆ 99 Cited by 116 Related articles All 4 versions »

Distributed fault tolerant and secure storage

L Shu - US Patent App. 10/025,113, 2003 - Google Patents

... Details ; Arrangements for supplying electrical power along data transmission lines; H04L25/14—Channel **dividing** arrangements in which a single bit stream is **divided** between several ... a combination of an encoding scheme and a **splitting** mechanism for a file **split** into three ...

☆ 99 Cited by 897 Related articles All 3 versions »

Cryptographic **key split** binder for use with tagged data elements

CJ Wack, EM Scheidt, JL Kolouch - US Patent 7,817,800, 2010 - Google Patents

... H04L9/085—Secret sharing or secret **splitting**, eg threshold schemes ... For example, an individual or computer can lack a random **key split** (or random value seed), the one or ... create the cryptographic **key** by a recipient, and can include, for example, one or more **key splits**, one or ...

☆ 99 Cited by 34 Related articles All 5 versions »

Encryption load balancing and **distributed** policy enforcement

U Mattsson, Y Rozenberg - US Patent App. 11/644,106, 2008 - Google Patents

... For example, the method can further comprise **dividing** the request into one or more sub-requests ... The dispatcher is arranged to **divide** a request into at least a first and a second sub-request, and to delegate the ... 0050]. Upon receiving the query, the dispatcher 16 **divides** the query ...

☆ 99 Cited by 71 Related articles All 2 versions »

Cryptographic **key split** binder for use with tagged data elements

CJ Wack, EM Scheidt, JL Kolouch - US Patent 8,077,870, 2011 - Google Patents

... securing one or more respectively tagged data elements includes generating a **plurality** of cryptographic ... For example, an individual or computer can lack a random **key split** (or random value seed ... **key** by a recipient, and can include, for example, one or more **key splits**, one or ...

☆ 99 Cited by 20 Related articles All 5 versions »

Encryption using entropy-based **key** derivation

JL Tucker, T Cordella, JD Profumo - US Patent App. 10/013,363, 2018 - Google Patents

... In this way, **key** derivation module 10 may **divide key split** 16 into a **plurality** of **portions**, and **key** derivation ... In this way, an attacker of system 1 is not able to **break** down intermediate **key** 28 ... In some examples, **key split** 16 is unique to the instance of writing of the data to memory ...

☆ 99 Cited by 19 Related articles All 3 versions »

Cryptographic **key** backup and escrow system

Y Zheng, NK Kauer, DV Badia - US Patent 8,139,770, 2012 - Google Patents

... of this aspect, the method may further includes utilizing a mathematical algorithm to **split** the master ...
highest level of the **key** escrow system 30; another approach, which involves **splitting** the master ...
4 , application **keys** 20 may be **divided** into groups 21 according to **key** type or ...

☆ 99 Cited by 63 Related articles All 5 versions »

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 1 of 23	Attorney Docket Number	104093-0002-118

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-4,453,074	06-05-1984	Weinstein	
		US-4,802,220	01-31-1989	Marker, Jr.	
		US-4,924,513	05-08-1990	Herbison et al.	
		US-4,932,057	06-05-1990	Kolbert	
		US-5,010,572	04-23-1991	Bathrick et al.	
		US-5,016,274	05-14-1991	Micali et al.	
		US-5,051,745	09-24-1991	Katz	
		US-5,150,407	09-22-1992	Chan	
		US-5,163,096	11-10-1992	Clark et al.	
		US-5,239,659	08-24-1993	Rudeseal et al.	
		US-5,268,963	12-07-1993	Monroe et al.	
		US-5,375,244	12-20-1994	McNair	
		US-5,386,104	01-31-1995	Sime	
		US-5,450,099	09-12-1995	Stephenson et al.	
		US-5,485,474	01-16-1996	Rabin	
		US-5,524,073	06-04-1996	Stambler	
		US-5,603,003	02-11-1997	Akizawa et al.	
		US-5,615,269	03-25-1997	Micali	
		US-5,623,546	04-22-1997	Hardy et al.	
		US-5,623,549	04-22-1997	Ritter	
		US-5,642,508	06-24-1997	Miyazawa	
		US-5,666,414	09-09-1997	Micali	
		US-5,666,416	09-09-1997	Micali	
		US-5,666,514	09-09-1997	Cheriton	
		US-5,682,425	10-28-1997	Enari	
		US-5,703,907	12-30-1997	James	
		US-5,717,758	02-10-1998	Micall	
		US-5,748,735	05-05-1998	Ganesan	
		US-5,761,306	06-02-1998	Lewis	
		US-5,761,311	06-02-1998	Spelman et al.	
		US-5,768,382	06-16-1998	Schneier et al.	
		US-5,768,388	06-16-1998	Goldwasser et al.	

Examiner Signature	/SAMSON B LEMMA/	Date Considered	04/13/2019

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.

T^1 – Applicant is to place a check mark here if English language Translation is attached.

442734_1

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

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 2 of 23	Attorney Docket Number	104093-0002-118

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-5,768,519	06-16-1998	Swift et al.	
		US-5,790,677	08-04-1998	Fox et al.	
		US-5,823,948	10-20-1998	Ross, Jr. et al.	
		US-5,903,652	05-11-1999	Mital	
		US-5,903,882	05-11-1999	Asay et al.	
		US-5,910,987	06-08-1999	Ginter et al.	
		US-5,915,019	06-22-1999	Ginter et al.	
		US-5,915,024	06-22-1999	Kitaori et al.	
		US-5,917,913	06-29-1999	Wang	
		US-5,937,066	08-10-1999	Gennaro et al.	
		US-5,940,507	08-01-1999	Cane et al.	
		US-5,960,083	09-28-1999	Micali	
		US-5,966,444	10-12-1999	Yuan et al.	
		US-5,966,448	10-12-1999	Namba et al.	
		US-5,974,144	10-26-1999	Brandman	
		US-5,982,322	11-09-1999	Bickley et al.	
		US-5,987,232	11-16-1999	Tabuki	
		US-5,991,414	11-23-1999	Garay et al.	
		US-5,995,630	11-30-1999	Borza	
		US-6,009,173	12-28-1999	Sumner	
		US-6,009,177	12-28-1999	Sudia	
		US-6,023,508	02-08-2000	Bombard et al.	
		US-6,026,163	02-15-2000	Micali	
		US-6,058,188	05-02-2000	Chandersekaran et al.	
		US-6,061,790	05-09-2000	Bodnar	
		US-6,073,237	06-06-2000	Ellison	
		US-6,078,888	06-20-2000	Johnson, Jr.	
		US-6,084,968	07-04-2000	Kennedy et al.	
		US-6,088,454	07-11-2000	Nagashima et al.	
		US-6,092,201	07-18-2000	Turnbull et al.	
		US-6,094,485	07-25-2000	Weinstein et al.	
		US-6,118,874	09-12-2000	Okamoto et al.	

Examiner Signature	/SAMSON B LEMMA/	Date Considered	04/13/2019

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.

T^1 – Applicant is to place a check mark here if English language Translation is attached.

442734_1

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

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 3 of 23	Attorney Docket Number	104093-0002-118

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-6,134,550	10-17-2000	Van Oorschot et al.	
		US-6,182,214	01-30-2001	Hardjono	
		US-6,192,472	02-20-2001	Garay et al.	
		US-6,226,385	05-01-2001	Taguchi et al.	
		US-6,229,894	05-08-2001	Van Oorschot et al.	
		US-6,240,183	05-29-2001	Marchant	
		US-6,240,187	05-29-2001	Lewis	
		US-6,240,188	05-29-2001	Dondeti et al.	
		US-6,256,737	07-03-2001	Bianco et al.	
		US-6,260,125	07-10-2001	McDowell	
		US-6,266,413	07-24-2001	Shefi	
		US-6,269,432	07-31-2001	Smith	
		US-6,289,455	09-11-2001	Kocher et al.	
		US-6,289,509	09-11-2001	Kryloff	
		US-6,292,568	09-18-2001	Akins, III et al.	
		US-6,292,782	09-18-2001	Weideman	
		US-6,301,659	10-09-2001	Micali	
		US-6,307,940	10-23-2001	Yamamoto et al.	
		US-6,314,409	11-06-2001	Schneck et al.	
		US-6,324,650	11-27-2001	Ogilvie	
		US-6,336,186	01-01-2002	Dyksterhouse et al.	
		US-6,345,101	02-05-2002	Shukla	
		US-6,345,314	02-05-2002	Cole et al.	
		US-6,347,143	02-12-2002	Goff et al.	
		US-6,356,941	03-12-2002	Cohen	
		US-6,363,425	03-26-2002	Hook et al.	
		US-6,363,481	03-26-2002	Hardjono	
		US-6,381,331	04-30-2002	Kato	
		US-6,385,318	05-07-2002	Oishi	
		US-6,386,451	05-14-2002	Sehr	
		US-6,411,716	06-25-2002	Brickell	
		US-6,415,373	07-02-2002	Peters et al.	

Examiner Signature	/SAMSON B LEMMA/	Date Considered	04/13/2019

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.

T^1 – Applicant is to place a check mark here if English language Translation is attached.

442734_1

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

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 4 of 23	Attorney Docket Number	104093-0002-118

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-6,424,718	07-23-2002	Holloway	
		US-6,438,690	08-20-2002	Patel et al.	
		US-6,446,204	09-03-2002	Pang et al.	
		US-6,449,730	09-10-2002	Mann et al.	
		US-6,453,416	09-17-2002	Epstein	
		US-6,466,552	10-15-2002	Haumont	
		US-6,473,858	10-29-2002	Shimomura et al.	
		US-6,473,860	10-29-2002	Chan	
		US-6,483,921	11-19-2002	Harkins	
		US-6,505,216	01-07-2003	Schutzman et al.	
		US-6,519,262	02-11-2003	Stephens et al.	
		US-6,553,493	04-22-2003	Okumura et al.	
		US-6,557,123	04-29-2003	Wiencko, Jr. et. al.	
		US-6,615,347	09-02-2003	De Silva et al.	
		US-6,625,734	09-23-2003	Marvit et al.	
		US-6,631,201	10-07-2003	Dickinson et al.	
		US-6,684,330	01-27-2004	Wack et al.	
		US-6,687,375	02-03-2004	Matyas, Jr. et al.	
		US-6,701,303	03-02-2004	Dunn et al.	
		US-6,731,755	05-04-2004	Cocks	
		US-6,785,768	08-31-2004	Peters et al.	
		US-6,789,198	09-07-2004	Chan	
		US-6,807,649	10-19-2004	Murthy	
		US-6,816,970	11-09-2004	Morgan et al.	
		US-6,819,766	11-16-2004	Weidong	
		US-6,852,988	02-08-2005	Li	
		US-6,853,988	02-08-2005	Dickinson et al.	
		US-6,856,383	02-15-2005	Vachris et al.	
		US-6,898,285	05-24-2005	Hutchings et al.	
		US-6,915,436	07-05-2005	Booth, III et al.	
		US-6,931,549	08-16-2005	Ananda	
		US-6,947,557	09-20-2005	Megiddo et al.	

Examiner Signature	/SAMSON B LEMMA/	Date Considered	04/13/2019

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.

T^1 – Applicant is to place a check mark here if English language Translation is attached.

442734_1

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

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 5 of 23	Attorney Docket Number	104093-0002-118

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-6,952,684	10-04-2005	Toshikage et al.	
		US-6,959,383	10-25-2005	Terada et al.	
		US-6,965,993	11-15-2005	Baker	
		US-6,978,367	12-20-2005	Hind et al.	
		US-6,981,141	12-27-2005	Mahne et al.	
		US-7,003,531	02-21-2006	Holenstein et al.	
		US-7,003,668	02-21-2006	Berson et al.	
		US-7,035,405	04-25-2006	Schwenk	
		US-7,039,189	05-02-2006	Kienzle et al.	
		US-7,050,580	05-23-2006	Ferre Herrero	
		US-7,050,583	05-23-2006	Montgomery	
		US-7,058,605	06-06-2006	Gupta	
		US-7,069,451	06-27-2006	Ginter et al.	
		US-7,072,917	07-04-2006	Wong et al.	
		US-7,076,651	07-11-2006	Droge	
		US-7,085,854	08-01-2006	Corente	
		US-7,096,494	08-22-2006	Chen	
		US-7,107,385	09-12-2006	Rajan et al.	
		US-7,111,173	09-19-2006	Scheidt	
		US-7,111,303	09-19-2006	Macchiano et al.	
		US-7,117,365	10-03-2006	Rump et al.	
		US-7,133,845	11-07-2006	Ginter et al.	
		US-7,140,044	11-21-2006	Redlich et al.	
		US-7,143,289	11-28-2006	Denning et al.	
		US-7,171,685	01-30-2007	Batra et al.	
		US-7,174,385	02-06-2007	Li	
		US-7,187,771	03-06-2007	Dickinson et al.	
		US-7,188,203	03-06-2007	Mowry et al.	
		US-7,191,252	03-13-2007	Redlich et al.	
		US-7,191,410	03-13-2007	Kruempelmann et al.	
		US-7,203,844	04-10-2007	Oxford	
		US-7,203,871	04-10-2007	Turner et al.	

Examiner Signature	/SAMSON B LEMMA/	Date Considered	04/13/2019

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.

T^1 – Applicant is to place a check mark here if English language Translation is attached.

442734_1

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

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 6 of 23	Attorney Docket Number	104093-0002-118

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-7,206,250	04-17-2007	Groux	
		US-7,213,158	05-01-2007	Bantz et al.	
		US-7,218,736	05-15-2007	Nishimura et al.	
		US-7,222,062	05-22-2007	Goud et al.	
		US-7,225,158	05-29-2007	Toshikage et al.	
		US-7,228,337	06-05-2007	Bornstein et al.	
		US-7,234,063	06-19-2007	Baugher et al.	
		US-7,260,724	08-21-2007	Dickinson et al.	
		US-7,260,727	08-21-2007	Fougeroux et al.	
		US-7,277,958	10-02-2007	Chung et al.	
		US-7,302,583	11-27-2007	Forrest	
		US-7,304,990	12-04-2007	Rajwan	
		US-7,313,825	12-25-2007	Redlich et al.	
		US-7,322,047	01-22-2008	Redlich et al.	
		US-7,337,320	02-26-2008	Tada et al.	
		US-7,346,773	03-18-2008	Cam-Winget et al.	
		US-7,346,925	03-18-2008	Marcjan	
		US-7,349,539	03-25-2008	Wee et al.	
		US-7,349,987	03-25-2008	Redlich et al.	
		US-7,356,818	04-08-2008	Carollo et al.	
		US-7,363,361	04-22-2008	Tewari et al.	
		US-7,391,865	06-24-2008	Orsini et al.	
		US-7,392,403	06-24-2008	Munetoh	
		US-7,412,462	08-12-2008	Margolus et al.	
		US-7,428,751	09-23-2008	Oom Temudo de Castro et al.	
		US-7,428,754	09-23-2008	Neumann et al.	
		US-7,440,953	10-21-2008	Sidman	
		US-7,444,421	10-28-2008	Katayama	
		US-7,464,152	12-09-2008	Ishizaki et al.	
		US-7,469,340	12-23-2008	Karamchedu et al.	
		US-7,472,105	12-30-2008	Staddon et al.	

Examiner Signature	/SAMSON B LEMMA/	Date Considered	04/13/2019

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.

T^1 – Applicant is to place a check mark here if English language Translation is attached.

442734_1

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

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 7 of 23	Attorney Docket Number	104093-0002-118

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-7,478,427	01-13-2009	Mukherjee et al.	
		US-7,499,905	03-03-2009	Jaschek et al.	
		US-7,535,905	05-19-2009	Narayanan et al.	
		US-7,546,427	06-09-2009	Gladwin et al.	
		US-7,548,556	06-16-2009	Wittenschlaeger	
		US-7,549,061	06-16-2009	Nonaka et al.	
		US-7,552,482	06-23-2009	Redlich et al.	
		US-7,577,689	08-18-2009	Masinter et al.	
		US-7,584,285	09-01-2009	Hudson et al.	
		US-7,587,368	09-08-2009	Felsher	
		US-7,596,570	09-29-2009	Emigh et al.	
		US-7,596,741	09-29-2009	LaVigne et al.	
		US-7,609,687	10-27-2009	Kobayashi et al.	
		US-7,623,809	11-24-2009	Nakano et al.	
		US-7,627,125	12-01-2009	Lumsden et al.	
		US-7,649,992	01-19-2010	Raju et al.	
		US-7,657,760	02-02-2010	Teramoto et al.	
		US-7,669,051	02-23-2010	Redlich et al.	
		US-7,693,992	04-06-2010	Watson	
		US-7,721,150	05-18-2010	Belyakov et al.	
		US-7,721,344	05-18-2010	Redlich et al.	
		US-7,730,543	06-01-2010	Nath	
		US-7,743,261	06-22-2010	Nonaka et al.	
		US-7,752,482	07-06-2010	Gredone et al.	
		US-7,756,792	07-13-2010	Hughes	
		US-7,765,411	07-27-2010	Hennessey et al.	
		US-7,788,532	08-31-2010	Kawamura	
		US-7,801,781	09-21-2010	Olin et al.	
		US-7,831,995	11-09-2010	Futoransky et al.	
		US-7,865,741	01-04-2011	Wood et al.	
		US-7,869,597	01-11-2011	Nakai et al.	
		US-7,916,871	03-29-2011	Brookner et al.	

Examiner Signature	/SAMSON B LEMMA/	Date Considered	04/13/2019

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.

T^1 – Applicant is to place a check mark here if English language Translation is attached.

442734_1

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

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 8 of 23	Attorney Docket Number	104093-0002-118

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-7,921,288	04-05-2011	Hildebrand	
		US-7,926,090	04-12-2011	Blevins et al.	
		US-7,929,697	04-19-2011	McNeely et al.	
		US-7,934,100	04-26-2011	Fujimaki	
		US-7,940,932	05-10-2011	Paksoy et al.	
		US-7,983,994	07-19-2011	Hurry	
		US-8,009,830	08-30-2011	Orsini et al.	
		US-8,041,875	10-18-2011	Shah et al.	
		US-8,060,088	11-15-2011	Ihattula	
		US-8,060,832	11-15-2011	Kruempelmann et al.	
		US-8,095,800	01-10-2012	Creary et al.	
		US-8,112,622	02-07-2012	Qi	
		US-8,135,134	03-13-2012	Orsini et al.	
		US-8,135,980	03-13-2012	Dodgson et al.	
		US-8,151,333	04-03-2012	Zhu et al.	
		US-8,155,322	04-10-2012	Bellare et al.	
		US-8,189,769	05-29-2012	Ramasamy et al.	
		US-8,190,905	05-29-2012	Chang et al.	
		US-8,195,976	06-05-2012	Rao et al.	
		US-8,208,897	06-26-2012	Kaneko et al.	
		US-8,213,387	07-03-2012	Xia et al.	
		US-8,250,643	08-21-2012	Enomoto et al.	
		US-8,261,084	09-04-2012	Nonaka et al.	
		US-8,261,265	09-04-2012	Chen et al.	
		US-8,266,438	09-11-2012	Orsini et al.	
		US-8,271,802	09-18-2012	Orsini et al.	
		US-8,300,822	10-30-2012	Nakai et al.	
		US-8,307,443	11-06-2012	Wang et al.	
		US-8,332,638	12-11-2012	Orsini et al.	
		US-8,341,115	12-25-2012	Natanzon et al.	
		US-8,347,084	01-01-2013	Tavernier et al.	
		US-8,352,941	01-08-2013	Protopopov et al.	

Examiner Signature	/SAMSON B LEMMA/	Date Considered	04/13/2019

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.

T^1 – Applicant is to place a check mark here if English language Translation is attached.

442734_1

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

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 9 of 23	Attorney Docket Number	104093-0002-118

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-8,392,682	03-05-2013	Dodgson et al.	
		US-8,396,895	03-12-2013	Miloushev et al.	
		US-8,397,083	03-12-2013	Sussland et al.	
		US-8,397,084	03-12-2013	Ranade	
		US-8,397,288	03-12-2013	Melvin, Jr. et al.	
		US-8,473,757	06-25-2013	Gladstone et al.	
		US-8,578,076	11-05-2013	Van der Linden et al.	
		US-8,635,456	01-21-2014	Fascenda	
		US-8,755,322	06-17-2014	Miettinen et al.	
		US-8,761,401	06-24-2014	Sprunk et al.	
		US-8,959,199	02-17-2015	Peleg et al.	
		US-2001/0024502	09-27-2001	Ohkuma et al.	
		US-2001/0050990	12-13-2001	Sudia	
		US-2001/0051902	12-13-2001	Messner	
		US-2002/0016773	02-07-2002	Ohkuma et al.	
		US-2002/0016926	02-07-2002	Nguyen et al.	
		US-2002/0023210	02-21-2002	Tuomenoksa et al.	
		US-2002/0031230	03-14-2002	Sweet et al.	
		US-2002/0032663	03-14-2002	Messner	
		US-2002/0046359	04-18-2002	Boden	
		US-2002/0071566	06-13-2002	Kurn	
		US-2002/0075844	06-20-2002	Hagen	
		US-2002/0080888	06-27-2002	Shu et al.	
		US-2002/0087866	07-04-2002	Berson et al.	
		US-2002/0129235	09-12-2002	Okamoto et al.	
		US-2002/0129245	09-12-2002	Cassagnol et al.	
		US-2002/0157007	10-24-2002	Sashihara	
		US-2002/0162047	10-31-2002	Peters et al.	
		US-2002/0172358	11-21-2002	Hurich	
		US-2002/0178355	11-28-2002	D'Sa et al.	
		US-2002/0178361	11-28-2002	Genty et al.	
		US-2002/0184444	12-05-2002	Shandony	

Examiner Signature	/SAMSON B LEMMA/	Date Considered	04/13/2019

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.

T^1 – Applicant is to place a check mark here if English language Translation is attached.

442734_1

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

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 10 of 23	Attorney Docket Number	104093-0002-118

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-2002/0191796	12-19-2002	Muschenborn	
		US-2003/0005094	01-02-2003	YUAN et al.	
		US-2003/0023958	01-30-2003	Patel et al.	
		US-2003/0051159	03-13-2003	McCown et al.	
		US-2003/0055905	03-20-2003	Nishiyama et al.	
		US-2003/0058274	03-27-2003	Hill et al.	
		US-2003/0061481	03-27-2003	Levine et al.	
		US-2003/0084020	05-01-2003	Shu	
		US-2003/0084290	05-01-2003	Murty et al.	
		US-2003/0084397	05-01-2003	Peleg	
		US-2003/0110188	06-12-2003	Howard et al.	
		US-2003/0126434	07-03-2003	Lim et al.	
		US-2003/0167408	09-04-2003	Fitzpatrick et al.	
		US-2003/0182435-A1	09-25-2003	Redlich et al.	
		US-2003/0188153	10-02-2003	Demoff et al.	
		US-2003/0204605	10-30-2003	Hudson et al.	
		US-2003/0236943	12-25-2003	Delaney	
		US-2004/0022390	02-05-2004	McDonald et al.	
		US-2004/0049687	03-11-2004	Orsini et al.	
		US-2004/0078542	04-22-2004	Fuller et al.	
		US-2004/0122960	06-24-2004	Hall et al.	
		US-2004/0193878	09-30-2004	Dillinger et al.	
		US-2004/0208170	10-21-2004	Miyazaki et al.	
		US-2004/0215955	10-28-2004	Tamai et al.	
		US-2004/0268148	12-30-2004	Karjala et al.	
		US-2005/0050004	03-03-2005	Sheu et al.	
		US-2005/0071631	03-31-2005	Langer	
		US-2005/0111657-A1	05-26-2005	Lee et al.	
		US-2005/0132060	06-16-2005	Mo et al.	
		US-2005/0160290	07-21-2005	Moon et al.	
		US-2005/0198306	09-08-2005	Palojarvi et al.	
		US-2005/0210243	09-22-2005	Archard et al.	

Examiner Signature	/SAMSON B LEMMA/	Date Considered	04/13/2019

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.

T^1 – Applicant is to place a check mark here if English language Translation is attached.

442734_1

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

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 11 of 23	Attorney Docket Number	104093-0002-118

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-2005/0289218	12-29-2005	Rothman et al.	
		US-2006/0020646	01-26-2006	Tee et al.	
		US-2006/0046728	03-02-2006	Jung et al.	
		US-2006/0075222	04-06-2006	Moloney et al.	
		US-2006/0075225	04-06-2006	Flynn et al.	
		US-2006/0078127	04-13-2006	Cacayorin	
		US-2006/0090200	04-27-2006	Oie	
		US-2006/0165060	07-27-2006	Dua	
		US-2006/0282681	12-14-2006	Scheidt et al.	
		US-2007/0006015	01-04-2007	Rao et al.	
		US-2007/0033644	02-08-2007	Thomas et al.	
		US-2007/0064704	03-22-2007	Balay et al.	
		US-2007/0071234	03-29-2007	Lagrange et al.	
		US-2007/0094272	04-26-2007	Yeh	
		US-2007/0097885	05-03-2007	Traversat et al.	
		US-2007/0122111	05-31-2007	Yamamoto et al.	
		US-2007/0124584	05-31-2007	Gupta	
		US-2007/0157025	07-05-2007	Sastry et al.	
		US-2007/0160198	07-12-2007	Orsini et al.	
		US-2007/0162744	07-12-2007	Hoshino et al.	
		US-2007/0165865	07-19-2007	Talvitie	
		US-2008/0016334	01-17-2008	Kurapati et al.	
		US-2008/0037557	02-14-2008	Fujita et al.	
		US-2008/0046752	02-21-2008	Berger et al.	
		US-2008/0072035	03-20-2008	Johnson et al.	
		US-2008/0126614	05-29-2008	Ooi et al.	
		US-2008/0147821	06-19-2008	Dietrich et al.	
		US-2008/0155252	06-26-2008	Nambiar	
		US-2008/0170693	07-17-2008	Spies et al.	
		US-2008/0183975	07-31-2008	Foster et al.	
		US-2008/0183992	07-31-2008	Martin et al.	
		US-2008/0232592	09-25-2008	Lee et al.	

Examiner Signature	/SAMSON B LEMMA/	Date Considered	04/13/2019

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.

T^1 – Applicant is to place a check mark here if English language Translation is attached.

442734_1

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

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 12 of 23	Attorney Docket Number	104093-0002-118

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-2008/0240441	10-02-2008	Kawakami	
		US-2008/0244277	10-02-2008	Orsini et al.	
		US-2008/0270603	10-30-2008	Berger et al.	
		US-2008/0294646	11-27-2008	Chang et al.	
		US-2008/0297326	12-04-2008	Chakraborty et al.	
		US-2009/0077379	03-19-2009	Geyzel et al.	
		US-2009/0092252	04-09-2009	Noll et al.	
		US-2009/0097657	04-16-2009	Scheidt et al.	
		US-2009/0113203	04-30-2009	Tsuge et al.	
		US-2009/0144202	06-04-2009	Hurry	
		US-2009/0172417	07-02-2009	Mikami et al.	
		US-2009/0177894	07-09-2009	Orsini et al.	
		US-2009/0209232	08-20-2009	Cha et al.	
		US-2009/0254572	10-08-2009	Redlich et al.	
		US-2009/0254750	10-08-2009	Bono et al.	
		US-2009/0288167	11-19-2009	Freericks et al.	
		US-2009/0292919	11-26-2009	England	
		US-2009/0292930	11-26-2009	Marano et al.	
		US-2009/0300284	12-03-2009	Murotani et al.	
		US-2009/0304004	12-10-2009	Huynh Van et al.	
		US-2009/0305900	12-10-2009	Belouchi et al.	
		US-2010/0005028	01-07-2010	Hartley et al.	
		US-2010/0046750	02-25-2010	Asfour	
		US-2010/0054474	03-04-2010	Schneider	
		US-2010/0077252	03-25-2010	Siewert et al.	
		US-2010/0095354	04-15-2010	Uchida et al.	
		US-2010/0125730	05-20-2010	Dodgson et al.	
		US-2010/0150341	06-17-2010	Dodgson et al.	
		US-2010/0153703	06-17-2010	Dodgson et al.	
		US-2010/0154053	06-17-2010	Dodgson et al.	
		US-2010/0162001 A1	06-24-2010	Dodgson; David	
		US-2010/0162004	06-24-2010	Dodgson et al.	

Examiner Signature	/SAMSON B LEMMA/	Date Considered	04/13/2019

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.

T^1 – Applicant is to place a check mark here if English language Translation is attached.

442734_1

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

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 13 of 23	Attorney Docket Number	104093-0002-118

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-2010/0191958	07-29-2010	Chen	
		US-2010/0223613	09-02-2010	Schneider	
		US-2010/0268966	10-21-2010	Leggette et al.	
		US-2010/0283734	11-11-2010	Hallbauer et al.	
		US-2010/0293380	11-18-2010	Wiseman et al.	
		US-2010/0299313	11-25-2010	ORSINI et al.	
		US-2010/0306578	12-02-2010	THORNTON et al.	
		US-2010/0318812	12-16-2010	Auradkar et al.	
		US-2010/0332617	12-30-2010	Goodwin et al.	
		US-2011/0085667	04-14-2011	BERRIOS et al.	
		US-2011/0093113	04-21-2011	Sager et al.	
		US-2011/0125849	05-26-2011	Boyd et al.	
		US-2011/0135094	06-09-2011	Muto et al.	
		US-2011/0145413	06-16-2011	Dawson et al.	
		US-2011/0179214	07-21-2011	Goggin et al.	
		US-2011/0179271	07-21-2011	Orsini et al.	
		US-2011/0179287	07-21-2011	Orsini et al.	
		US-2011/0246766	10-06-2011	Orsini et al.	
		US-2011/0246817	10-06-2011	Orsini et al.	
		US-2012/0042034	02-16-2012	Goggin et al.	
		US-2012/0072723	03-22-2012	Orsini et al.	
		US-2012/0166576	06-28-2012	Orsini et al.	
		US-2012/0166818	06-28-2012	Orsini et al.	
		US-2012/0179916	07-12-2012	Staker et al.	
		US-2012/0198338	08-02-2012	Flint et al.	
		US-2012/0221854	08-30-2012	Orsini et al.	
		US-2012/0221855	08-30-2012	Orsini et al.	
		US-2012/0221856	08-30-2012	Orsini et al.	
		US-2012/0222134	08-30-2012	Orsini et al.	
		US-2012/0226904	09-06-2012	Orsini et al.	
		US-2012/0255034	10-04-2012	Orsini et al.	
		US-2012/0255035	10-04-2012	Orsini et al.	

Examiner Signature	/SAMSON B LEMMA/	Date Considered	04/13/2019

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.

T^1 – Applicant is to place a check mark here if English language Translation is attached.

442734_1

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

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 14 of 23	Attorney Docket Number	104093-0002-118

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-2012/0266231	10-18-2012	Spiers et al.	
		US-2013/0042105	02-14-2013	Orsini et al.	

FOREIGN PATENT PUBLICATIONS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T^1
		AU-2004248616	06-04-2009	Security First Corporation		
		CN-101375284-A	02-25-2009	Orsini Rick L		
		CN-1329417A	01-02-2002	IBM		
		CN-1347225A	05-01-2002	Yang Gaoxiong		
		CN-1607762A	04-20-2005	Microsoft Corp.		
		CN-1613111A	05-04-2005	Sony Music Entertainment Inc.		
		EP-0485090-A2	05-13-1992	Visa Int Service Ass		
		EP-0798892 A2	10-01-1997	IBM		
		EP-0821504	01-28-1998	Nippon Telegraph and Telephone Corporation		
		EP-0851629-A2	07-01-1998	Canon Kk		
		EP-0862301	09-02-1998	Fujitsu Limited		
		EP-1011222	06-21-2000	Fujitsu Limited		
		EP-1239384-A2	09-11-2002	Pkware Inc		
		EP-2309700-A1	04-13-2011	Alcatel Lucent		
		EP-346180	12-13-1989	France Telecom		
		EP-354774	02-14-1990	International Business Machines Corporation		
		EP-636259	02-01-1995	Secure Computing Corporation		
		EP-793367	09-03-1997	Oki Electric Industry Co., Ltd.		
		FR-2632469	12-08-1989	Pailles Jean Claude		
		GB-2237670-A	05-08-1991	De La Rue Syst et al.		

Examiner Signature	/SAMSON B LEMMA/	Date Considered	04/13/2019

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.

T^1 – Applicant is to place a check mark here if English language Translation is attached.

442734_1

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

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 15 of 23	Attorney Docket Number	104093-0002-118

FOREIGN PATENT PUBLICATIONS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[1]
		JP-04297157-A	10-21-1992	Mitsubishi Electric Corp		
		JP-2003/132234	05-09-2003	Global Friendship Inc.		
		JP-2004-185573	07-02-2004	Nec Infrontia Corp		
		JP-2005/136739	05-26-2005	Furukawa Electric Co Ltd.		
		JP-2005-244379-A	09-08-2005	Nec Communication Syst		
		JP-2005-267520	09-29-2005	Ntt Comware Corp		
		JP-2006-174152-A	06-29-2006	Matsushita Electric Works Ltd.		
		JP-2007-334836	12-27-2007	Canon Kk		
		JP-2008/250369	10-16-2008	Sorun Corp.		
		JP-2008-103936	05-01-2008	Toshiba Corp		
		JP-2008-250931	10-16-2008	Toshiba Corp		
		RU-2124814	01-10-1999	A.A. Moldovjan		
		WO-00/36786-A1	06-22-2000	Philips Electronics Na		
		WO-00/49766 A1	08-24-2000	Sonera Smarttrust Oy		
		WO-00/76118-A1	12-14-2000	Gen Instrument Corp		
		WO-00/79367-A1	12-28-2000	Brodia Group		
		WO-01/22201-A1	03-29-2001	Ethentica Inc		
		WO-01/22319-A1	03-29-2001	Ethentica Inc		
		WO-01/22322-A2	03-29-2001	Ethentica Inc		
		WO-01/22650-A2	03-29-2001	Ethentica Inc		
		WO-01/22651-A2	03-29-2001	Ethentica Inc		
		WO-02/062032	08-08-2002	The Charles Stark Draper Laboratory, Inc.		
		WO-02/21283-A1	03-14-2002	Sanctuary Systems Pty Ltd.		
		WO-02/21761-A2	03-14-2002	Widevine Technologies Inc		
		WO-03/036538	05-01-2003	Yasukura Yutaka		
		WO-04/111791-A2	12-23-2004	Security First Corp.		
		WO-06/047694-A1	05-04-2006	Orsini Rick L et al.		

Examiner Signature	/SAMSON B LEMMA/	Date Considered	04/13/2019

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.

T[1] – Applicant is to place a check mark here if English language Translation is attached.

442734_1

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

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 16 of 23	Attorney Docket Number	104093-0002-118

FOREIGN PATENT PUBLICATIONS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[1]
		WO-08/054406-A2	05-08-2008	Orsini Rick L et al.		
		WO-08/070167-A1	06-12-2008	Martin Don et al.		
		WO-08/127309-A2	10-23-2008	Bellare Mihir et al.		
		WO-08/142440-A1	11-27-2008	Surf-Control On-Demand Limited		
		WO-09/035674-A1	03-19-2009	Security First Corp.		
		WO-09/089015-A1	07-16-2009	Security First Corp.		
		WO-09/105280-A2	08-27-2009	Security First Corp.		
		WO-2001/054370	07-26-2001	The University of Manitoba		
		WO-2004/001561-A2	12-31-2003	Armoursoft Ltd		
		WO-2007/078846	07-12-2007	United Video Properties Inc.		
		WO-2010/057181-A2	05-20-2010	Unisys Corp		
		WO-2010/135412-A2	11-25-2010	Security First Corp.		
		WO-2011/068738-A2	06-09-2011	Orsini Rick L et al.		
		WO-2011/123692-A2	10-06-2011	Orsini et al.		
		WO-2011/123699-A2	10-06-2011	Orsini et al.		
		WO-98/47091-A1	10-22-1998	Transactor Networks Inc		
		WO-99/19845-A1	04-22-1999	At & T Corp		
		WO-99/46720-A1	09-16-1999	Cha Tech Serv Inc		
		WO-99/65207-A1	12-16-1999	Microsoft Corp		

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.	T[1]
		Barlas, "RSA's Security Showcase", Line56.com - The E-Business Executive Daily, 15 April 2003.	
		Brainard, "A New Two-Server Approach for Authentication with Short Secrets" RSA Laboratories, Bedford, MA (13 pages)	
		Cachin, "On-Line secret Sharing," Cryptography and Coding. IMA Conference, Proceedings, December 18, 1995, pages 190-198, XP002137681.	

Examiner Signature	/SAMSON B LEMMA/	Date Considered	04/13/2019

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.

T[1] – Applicant is to place a check mark here if English language Translation is attached.

442734_1

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

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 17 of 23	Attorney Docket Number	104093-0002-118

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.	T[1]
		Chan et. al., "Distributed Server Networks for Secure Multicast", GLOBCOM'01: IEEE Global Telecommunications Conference (IEEE, Piscataway, NJ) 3:1974-1978 (2001).	
		Chan et. al., "Distributed Servers Approach for Large-Scale Multicast", IEEE Journal on Selected Areas in Communications (IEEE, Piscataway, NJ) October 2002, 20(8):1500-1510.	
		Crescenzo et al., "Non-Interactive and Non-Malleable Commitment," Proceedings of the 30th Annual ACM Symposium on Theory of Computing. Dallas, TX, May 23-26, 1998, [Proceedings of the 30th Annual ACM Symposium on Theory of Computing], New York, NY: ACM, US, PAGES 141-150; XP000970902; ISBN: 978-0-89791-962-3.	
		Damgard et. al., "Non-interactive and Reusable Non-malleable Commitment Schemes," ACM STOC '03; pgs. 427-428; June 9-11, 2003.	
		Decru Unveils Security Appliances for Storage Networks; Decru DataFort (TM) Security Alliances Protect SAN and NAS Environments with Wire-Speed Encryption and Transparent Deployment", PR Newswire (PR Newswire Association. Inc.), 14 October 2002.	
		Dierks, "The Transport Layer Security Protocol," RFC 4346m Version 1.1, April 2006, 86 pages	
		Doyle, "RSA Splits Data to Stop Hackers", vnunet.com, 16 April 2003.	
		Easter et al. "S/390 parallel enterprise server CMOS cryptographic coprocessor," IBM Journal of Research and Development, International Business Machines Corporation, New York, NY, US, vol. 43, no. 5, 1 January 1999, pgs. 761-776, XP002335589, ISSN: 0018-8646.	
		Fisher, "RSA Looks to Lock Down Personal Data", eWeek - Enterprise News & Reviews, 14 April 2003.	
		Ganger et al., "PASIS: A Distributed Framework for Perpetually Available and Secure Information Systems, Final Technical rept. June 1999-Dec 2003," (7-1-2005),pgs 1-302, XP55011444, Retrieved from the Internet: URL:http://www.dtic/mil/cgi-bin/GetTRDoc?AD=ADA436245&Location-U2&doc=GetTRDoc.pdf (retrieved 0n 2011-11-07]	
		Ganger et al., "Survivable storage systems," DARPA Information Survivability Conference & Exposition II, 2001. DISC EX '01. Proc. 12-14 June 2001, Piscataway, NJ, USA, IEEE, vo. 2, pgs. 184-195, XP010548746	
		Garay et. al., "Secure distributed storage and retrieval," Theoretical Comput. Sci., 243(1-2):363-389, July 2000	

Examiner Signature	/SAMSON B LEMMA/	Date Considered	04/13/2019

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.

T[1] – Applicant is to place a check mark here if English language Translation is attached.

442734_1

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

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 18 of 23	Attorney Docket Number	104093-0002-118

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.	T[1]
		Gibson, "Opinion", eWeek - Enterprise News & Reviews, 14 April 2003.	
		Grant et. al., "Secret Sharing and Splitting", (White Paper) Notre Dame, Indiana, 16 December 2002.	
		Hand et al., Spread Spectrum Storage with Mnemosyne, 2003, Retrieved from the Internet <URL: springerlink.com/content/9vdp5b40ep2pjvba/>, pp 1-5 as printed	
		Haniotakis et al., "Security Enhancement Through Multiple Path Transmission in Ad Hoc Networks," IEEE Intl. Conference on Communications, 20-24 June 2004, 5 pgs.	
		Horne et al., Escrow services and incentives in Peer-to-Peer Networks, 2001, Retrieved from the Internet URL:dl.acm.org.citation.cfm?id=501168, pp 1-10 as printed	
		Hunter, "Simplifying PKI Usage Through a Client-Server Architecture and Dynamic Propagation of Certificate Paths and Repository Addresses", Proceedings 13th International Workshop on Database and Expert Systems Applications (IEEE Computer Soc., Los Alamitos, CA), 2-6 September 2002, pg. 505-510.	
		Johnson, "MLS-Net and Secure Parser: A New Method for Securing and Segregating Network Data" [Online] 8-July 2007"XP002582437 5th International Symposium on Risk Management and Informatic: WMS12007, Orlando Florida, USA	
		Kent, "Security Architecture for the Internet Protocol," RFC 2401, November 1998, 67 pages.	
		Klensin, J., "Simple Mail Transfer Protocol; rfs5321.txt," Simple Mail Transfer Protocol; RFC5321.TXT, Internet Engineering Task Force, IETF; Standard, Internet Society (ISOC) 4, Rue Des Falaises CH- 1205 Geneva, Switzerland, XP015060297 (October 2008)	
		Krawczyk, "Distributed Fingerprints and Secure Information Dispersal," 12th ACM, Symposium on Principles on Distributed Computing, Ithaca, NY, ACM 0-89191-613-1/93/0008/0207, 1993, pages 207-218	
		Krawczyk, "Secret sharing made Short," IBM T.J. Watson Research Center, [Online] 1998, retrieved from the Internet: URL:http://www.cs.cornell.edu/courses/cs754/2001fa/secretshort.pdf> [retrieved on 11-24-2008]	
		Kroç, Erol, "Access Control in Peer-to-Peer Storage Systems," 1 Oct 2006, XP55036196, Retrieved from the Internet: URL:ftp://ftp.tik.ee.ethz.ch/pub/studfents/2006-So/MA-2006-10.pdf [retrieved on 2012-08-23] page. 61-62	
		Kubiatowicz et al., OceanStore: an architecture for global-scale persistent storage, Retrieved from the Internet <URL: dl.acm.org/citation.cfm?id=356989.357007>, pp 1-12 as printed	

Examiner Signature	/SAMSON B LEMMA/	Date Considered	04/13/2019

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.

T[1] – Applicant is to place a check mark here if English language Translation is attached.

442734_1

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

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 19 of 23	Attorney Docket Number	104093-0002-118

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.	T[1]
		Lancope Announces Stealthwatch 3.0 for Enhanced Enterprise-Wide Security and Improved Manageability", Business Wire (Newswire Association, Inc.), 14 April 2003.	
		Loutrel et. al. "An EAP-BT Smartcard for Authentication in the Next Generation of Wireless Communications", Conference on Network Control and Engineering for QoS Security and Mobility (Kluwer Academic Publishers, Norwell, MA) October 23-25, 2002, pgs. 1-4-114.	
		Mayer et. al., "Generalized Secret Sharing and Group-Key Distribution Using Short Keys," Compression and Complexity of Sequences 1997, Proceedings Salerno, Italy, June 11-13, 1997, Los Alamitos, CA, USA, IEEE Comput,. SOC, US, June 11, 1997, pages 30-44, XP010274905, ISBN: 978-0-8186-8132-5.	
		McNamara, "Strong Crypto Freeware" (Secret Sharer Version 1.0) July 11, 1995.	
		Menezes, "Handbook of Applied Cryptography, Ch. 7 Block Ciphers" 1997, pgs. 223-271 CRC Press LLC, XP001525007	
		Mitchell, "Making Serial Number Based Authentication Robust Against Loss of State", Operating Systems Review, 34:3, pgs. 1-5, November 24, 1999	
		Myers et. al., "A secure, publisher-centric Web caching infrastructure" In: INFOCOM 2001 Proceedings. IEEE Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies [online], vol. 3 p. 1235-1243. Published 04/22/2001. [retrieved on 7-8-2008]. Retrieved from the internet <URL: http://people.ischool.berkeley.edu/-chuang/pubs/gemini.pdf>	
		Nightingale, The New Secret-Splitting Technology from RSA... NGBK DS 0403 http://developer.rsasecurity.com/labs/nightingale/developer.rsasecurity.com/labs/nightingale/files/nightingale-brochure.pdf	
		Pattam, "Enhancing Security in 802.11 and 802.1X Networks with Intrusion Detection," Jan. 20, 2006, Univ. of New Orleans Theses and Dissertations, Paper 1034, 111 pages	
		Rabin, "Efficient Dispersal of Information for Security, Load Balancing and Fault Tolerance," Journal of the Association for Computing Machinery, Vol. 36, No. 2, pp. 335-348, April 1989	
		Rivest, "All-Or-Nothing Encryption and The Package Transform," Proc. Of the 4th Intl. Workshop on Fast Software Encryption (1997), 9 pgs.	
		RSA SureFile: Software Powered by PKZIP...BSSF DS 0103 Authorized Reseller: Technical Specifications Platforms Microsoft ® Windows ® 98 Second Edition ME NT 4.0 Workstation SP6A 2000 Professional SP2... www.rsasecurity.com/products/bsafe/datasheets/BSSF_DS_103.pdf	

Examiner Signature	/SAMSON B LEMMA/	Date Considered	04/13/2019

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.

T[1] – Applicant is to place a check mark here if English language Translation is attached.

442734_1

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

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 20 of 23	Attorney Docket Number	104093-0002-118

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.	T[1]
		Savage, "RSA Unveils Nightingale Technology", CRN.com, 14 April 2003.	
		Sengar et al., "MTPSec: Customizable Secure MTP3 Tunnels in the SS7 Network," Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium, 8 pages (2005)	
		Shamir, "How to Share a Secret," Communications of the Association for Computing Machinery, ACM, New York, NY, US, Vol. 22, No. 11, November 1, 1979, pages 1-4, XP002241399; ISSN: 0001-0782.	
		Shin et. al., "Design a Working Model of Secure Data Transfer Using a Data Mart", Proceedings of the ISCA 14th International Conference Computer Applications in Industry and Engineering (ISCA, Cary, NC) 27-29 November 2001, pg. 66-69.	
		Tactilesense TM White Paper - A Breakthrough in Fingerprint Authentication", Ethentica, Inc. by Security First Corporation, January, 2003.	
		Trustengine TM White Paper - Enthentication Services, Secure Storage and Authentication Solutions", Ethentica, Inc. by Security First Corporation, June 2002.	
		Vijayan, "RSA unveils Management, Encryption Products", Computerworld, 15 April 2003.	
		Waldman et al., "Publius: A robust, tamper-evident, censorship-resistant web publishing sytem," Proceedings of the 9th USENIX Security Symposum, August 2000	
		Waters, "RSA Integrates ID Management; discloses 'Nightingale' ", ADTmag.com, 21 April 2003.	
		Copy of Office Actions and Replies issued for U.S. Patent Application No. 13/468,383 (104093-0002-107)	
		Copy of Office Actions and Replies issued for U.S. Patent Application No. 13/468,428 (104093-0002-108)	
		Copy of Office Actions and Replies issued for U.S. Patent Application No. 13/468,450 (104093-0002-109)	
		Copy of Office Actions and Replies issued for U.S. Patent Application No. 13/468,523 (104093-0002-110)	
		Copy of Office Actions and Replies issued for U.S. Patent Application No. 13/468,605 (104093-0002-111)	
		Copy of Office Actions and Replies issued for U.S. Patent Application No. 13/468,562 (104093-0002-112)	
		Copy of Office Actions and Replies issued for U.S. Patent Application No. 13/468,584 (104093-0002-113)	

Examiner Signature	/SAMSON B LEMMA/	Date Considered	04/13/2019

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.

T[1] – Applicant is to place a check mark here if English language Translation is attached.

442734_1

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

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 21 of 23	Attorney Docket Number	104093-0002-118

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.	T[1]
		Xu, "Locality Driven Key Management Architecture for Mobile Ad-hoc Networks," 2004 IEEE International Conference on Mobile Ad-hoc and Sensor Systems," pgs. 436-446.	
		Nacht, "The Spectrum of Modern Firewalls," Computers & Security, 16 (1997), pp. 54-56.	
		Shaw et al (eds.), "Handbook on Electronic Commerce, Conway, Chapter 31, Springer-Verlag, Berlin Heidelbert, pp. 649-690 (2000)	
		Mondal, "Mobile IP," Chapter 7, Fluwer Academic/Plenum Publishers, New York, pp. 173-202 (2003)	
		Rosen, "BGP/MPLS VPNs," Network Working Group, RFC 2547, March 1999, 25 pages.	
		Tewari et al.; "High Availability in Clustered Multimedia Servers; 1996; Retrieved from the Internet <URL:ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=492215>; pp. 1-10 as printed.	
		Wells; The OceanStore Archive: Goals, Structures, and Self-Repair; 2001; Retrieved from the Internet <URL: oceanstore.org/publications/papers/pdf/>; pp. 1-20 as printed.	
		Wylie et al.; Selecting the right data distribution scheme for a survivable storage system; 2001; Retrieved from the Internet <URL: repository.cmu./edu/compsci/2164/?utm_source=repository.cmu.edu%2Fcompsci%2F2164&utm_medium=PDF&utm_campaign=PDFCoverPages.; pp. 1-25 as printed.	
		Buckhard et al., "MDP Disk Array Storage System Reliability; 1992; Retrieved from the Internet <URL:ieexplore.ieee.org/xpls/abs_all.jsp?arnumber=627346&tag=1>; pp. 1-26 as printed.	
		Kim et al., "Secure Group Key Management for Storage Area Networks," IEEE Communications Magazine, August 2003, pp. 92-99.	
		Bendix, "RAID and Informix Databases," White Paper, Advanced Technology Group, June 1995; Retrieved from the Internet <URL: informix.com.ua/articles/raid/raid.htm>; retrieved from the internet on December 3, 2014, pp. 1-15 as printed.	
		D'Arco et al.: "Fault Tolerant and distributed Broadcast Encryption"; 2003: Retrieved from the Internet<URL:link.springer.com/chapter/10.1007/3-540-36563-x18#page-1>; pp. 1-18 as printed.	
		Schwartz, Richard; "Using field encryption in applications"; 2001; Retrieved from the Internet<URL:ibm.com/developerworks/lotus/library/IS-filed_encryption/>; pp. 1-16 as printed.	

Examiner Signature	/SAMSON B LEMMA/	Date Considered	04/13/2019

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.

T[1] – Applicant is to place a check mark here if English language Translation is attached.

442734_1

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

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 22 of 23	Attorney Docket Number	104093-0002-118

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.	T[1]
		Goodson et al., "Efficient consistency for erasure-coded data via versioning servers," Retrieved from the Internet<URL:oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA461126> pgs. 1-25, March 2003.	
		Long et al., "Swift/RAID: A Distributed RAID System," Retrieved from the Internet<URL:http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.53.7183>pgs. 1-20 (1994)	
		Guo et al. "Design and implementation of the KioskNet System", Information and Communication Technologies and Development, 2007. ICTD 2007. International Conference on, 31 December 2007 (2007-12-31) pages 264-281 [retrieved on 2015-11-26]	
		CHEN, et al., "RAID: High-Performance, Reliable Secondary Storage" Retrieved from the internet, <URL:https://web.archive.org/web/20040721062927/http://meseec.ce.rit.edu/eecc722-fall2002/papers/io/3/chen94raid.pdf> 26:145-184 (1994)	
		PLANK, JAMES A., "A Tutorial on Reed-Solomon Coding for Fault-Tolerance in RAID-like Systems," Retrieved from the Internet <URL: citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.160.4742&rep=rep1&type=pdf>; pp. 1-18 as printed (1997).	
		Office Actions and Replies for U.S. Application No. 11/258,839.	
		Office Actions and Replies for U.S. Application No. 12/148,365.	
		Office Actions and Replies for U.S. Application No. 12/272,012.	
		Office Actions and Replies for U.S. Application No. 12/336,558.	
		Restriction Requirement issued September 29, 2011 for U.S. Application No. 12/336,559.	
		Office Action issued November 28, 2011 for U.S. Application No. 12/336,562.	
		Office Action issued September 27, 2011 for U.S. Application No. 12/336,568.	
		Office Action issued November 8, 2011 for U.S. Application No. 12/342,379.	
		Office Action issued September 14, 2011 for U.S. Application No. 12/342,500.	
		Office Action issued October 7, 2011 for U.S. Application No. 12/342,523.	
		Office Actions issued October 6, 2011 for U.S. Application No. 12/342,547.	
		Office Action issued November 10, 2011 for U.S. Application No. 12/342,575.	
		Office Actions and Replies for U.S. Application No. 12/342,610.	
		Office Action issued November 23, 2011 for U.S. Application No. 12/342,636.	

Examiner Signature	/SAMSON B LEMMA/	Date Considered	04/13/2019

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.

T[1] – Applicant is to place a check mark here if English language Translation is attached.

442734_1

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

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 23 of 23	Attorney Docket Number	104093-0002-118

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.	T[1]
		Office Actions and Replies for U.S. Application No. 12/346,578.	
		Office Actions and Replies for U.S. Application No. 13/024,791.	
		Office Action issued June 11, 2012 for U.S. Application No. 13/371,361.	
		Office Actions and Replies for U.S. Application No. 13/371,363.	
		Office Actions and Replies for U.S. Application No. 13/371,364.	

Examiner Signature	/SAMSON B LEMMA/	Date Considered	04/13/2019

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.

T[1] – Applicant is to place a check mark here if English language Translation is attached.

442734_1

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

Patents dividing splitting plurality chunks portions encrypt distri Sign In

dividing; splitting; plurality; chunks; portions; encrypt; distribute; keys;

About 4,696 results Download Side-by-side

Sort by · Relevance Grouped by · None Results / page · 10

Splitting knowledge of a password



~~US~~ · US6959394B1 · Emie Brickell · Intel Corporation

Priority 2000-09-29 · Filing 2000-09-29 · Grant 2005-10-25 · Publication 2005-10-25

... for registering the user's **distributed** cryptographic **key**. In brief, a cryptographic **key** is **split** into **pieces** and **distributed** among a **plurality** of ... **divides** the password into N **pieces** using the same method used during registration. (Act 302). The password **pieces** may then be **encrypted** for each ...

Cloud file system

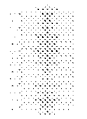


WO EP US CN JP KR · US9252164B2 · Anthony Francois Gauda · Bitcasa, Inc

Priority 2011-05-14 · Filing 2012-05-14 · Grant 2016-02-02 · Publication 2016-02-02

... least a **portion** of one or more of the **plurality** of files stored in the cloud storage system, wherein each of the **plurality** of **encrypted** file **chunks** ... **splitting** that file into a **plurality** of **chunks**, for each of the **plurality** of **chunks**, performing the following: generating an **encryption key** based on ...

Method and system for data delivery and reproduction



WO US AU · US7447907B2 · John J. Hart, III · Ecd Systems, Inc.

Priority 2000-04-04 · Filing 2001-04-04 · Grant 2008-11-04 · Publication 2008-11-04

... the title data into a **plurality** of **chunks** of data, and providing an decryption **key** for each **chunk**. The step of **encrypting** can also include **dividing** ... A system and method for **distributing** title data, such as songs, videos or computer games. The title data is provided from a central location to a ...

Information-centric security



WO US · US7715565B2 · Gerald D. Kimmel · Infoassure, Inc.

Priority 2004-07-29 · Filing 2005-07-29 · Grant 2010-05-11 · Publication 2010-05-11

wherein the **key** management module is configured to **encrypt** the data **encryption key** for each of a **plurality** of public **key portions** received associated ... to communicate with the interface and the memory and configured to: **split** public and private **portions** of **encryption keys** into asymmetric **pieces**;

Apparatus and method for processing **encrypted** data



WO EP US CN JP KR AU IL MX · KR100917487B1 · 다비 프랑리니 · 톰슨 라이센싱

Priority 2001-12-12 · Filing 2002-12-12 · Grant 2009-09-16 · Publication 2009-09-16

A data processing device includes a virtual smart card, virtual manager, and a virtual smart card, and / or virtual manager according to the invention is disclosed.

Secure data parser method and system

WO EP US CN AU BR CA · CN102609636B · 里奇·L·奥尔德尼 · 安全第一公司

Priority 2004-10-25 · Filing 2005-10-25 · Grant 2015-07-15 · Publication 2015-07-15

16. A computer-implemented method for protecting a data set-implemented method comprising: determining a **plurality** of data **portions** to be **distributed** ... engine 220 to disrupt at least the private **key** to **encrypt** the data and **divides**, thereby storing only the scrambled data is **divided**. Similar **split** ...

Data **distribution** system and method



WO EP ~~US~~ AT ~~DE~~ ES ~~GB~~ · EP1730934B1 · Ian David Parr · Siemens IT Solutions and Services Limited

Priority 2004-03-16 · Filing 2005-03-15 · Grant 2008-05-07 · Publication 2008-05-07

Preferably rights management is effected by supplying a licence containing playback conditions and decryption **keys** to enable decryption of **encrypted** ... of **distributing** validated data in a network comprising: **dividing** the data into a **plurality** of data **chunks**; deriving a hash value for each data **chunk**;

Efficient transmission of cryptographic information in secure real time ...

WO EP US ~~CN~~ JP ~~KR~~ AU ~~BR~~ ~~CA~~ IL MX ~~RU~~ · JP2007529947A · シュ、レイモンド・クーンシェン・クアルコム・インコーポレイテッドQualcomm Incorporated

Priority 2004-03-18 • Filing 2005-03-17 • Publication 2007-10-25

... from the received **portions** of the MKI information. For example, assume that the MKI information is **divided** into smaller **portions** or **chunks** (**chunk**), ... And to derive the session **key** from the bit stream, And **encrypting** the data with the session **key**, And **dividing** the information into a **plurality** of ...

Secure cloud storage **distribution** and aggregation

US • US9836103B2 • David A. Redberg • Fortinet, Inc.

Priority 2013-12-02 • Filing 2015-06-17 • Grant 2017-01-03 • Publication 2017-01-03

... of the file using cryptographic **key** information defined by the first file storage policy, including (a) **dividing** the file into a **plurality** of **chunks**, ... and (ii) the searchable **encrypted** data is **distributed** among the third-party cloud storage platforms based on the storage diversity requirements ...

Encrypting segmented data in a **distributed** computing system



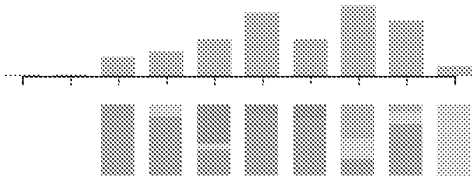
US • US20170139843A1 • Jason K. Resch • International Business Machines Corporation

Priority 2011-12-12 • Filing 2017-01-27 • Publication 2017-05-18

appending the masked **key** to the **encrypted** data to produce the **encrypted** data segment; or **distributing**, in accordance with a pattern, **portions** of the ... **divides** the data segment into the set of data sub-segments 558 . The sub-segmenting module 548 may **divide** the data segment into the set of data sub- ...

Next › » About 4,696 results

Top 1000 results by filing date



Relative count of top 5 values

Assignees	Inventors	CPCs
Digimarc Corporation G06T1/005 G06T2201/00 H04N2201/3225 G06T2201		11%
Amazon Technologies, Inc. G06N99/005 G06N G06N20/00 G06N5/025		3.8%
International Business Machines Corporation G06F3/067 H04L67/1097 G06F3/0638 G06F11/1076		3.8%
Digital Doors, Inc. H04L63/10 G06F21/62 G06F21/6209 G06F21/60		3%
Fusion-Io, Inc. G06F3/0688 G06F12/02 G06F3/0683 G06F12		2.6%

Expand

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
15/977,748	05/11/2018	Mark S. O'Hare	104093-0002-118

CONFIRMATION NO. 7200

15314
Haley Guiliano LLP
75 Broad Street
Suite 1000
New York, NY 10004

PUBLICATION NOTICE



Title:SECURE DATA PARSER METHOD AND SYSTEM

Publication No.US-2018-0367509-A1
Publication Date:12/20/2018

NOTICE OF PUBLICATION OF APPLICATION

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

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

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

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently https://portal.uspto.gov/pair/PublicPair. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
15/977,748	05/11/2018	2827	3540	104093-0002-118	24	4

CONFIRMATION NO. 7200

UPDATED FILING RECEIPT

15314
Haley Guiliano LLP
75 Broad Street
Suite 1000
New York, NY 10004

OC000000102179762

Date Mailed: 09/11/2018

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)

Mark S. O'Hare, Coto De Caza, CA;
Rick L. Orsini, Flower Mound, TX;
Roger S. Davenport, Campbell, TX;
Steven Winick, Roslyn Heights, NY;

Applicant(s)

Security First Corp., Rancho Santa Margarita, CA;

Power of Attorney: The patent practitioners associated with Customer Number 15314

Domestic Priority data as claimed by applicant

This application is a CON of 13/915,081 06/11/2013 PAT 9992170
which is a DIV of 13/468,383 05/10/2012 PAT 9338140
which is a CON of 11/258,839 10/25/2005 PAT 8266438
which claims benefit of 60/718,185 09/16/2005
and claims benefit of 60/622,146 10/25/2004

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: 06/04/2018

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 15/977,748**

Projected Publication Date: 12/20/2018

Non-Publication Request: No

Early Publication Request: No

Title

SECURE DATA PARSER METHOD AND SYSTEM

Preliminary Class

365

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

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

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

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

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

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

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific

countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

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

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

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

NOT GRANTED

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

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop

technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 15/977,748

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	300
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	660
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	760
TOTAL CLAIMS (37 CFR 1.16(i))	24 minus 20 =	* 4			OR	x 100 =	400
INDEPENDENT CLAIMS (37 CFR 1.16(h))	4 minus 3 =	* 1				x 460 =	460
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).						800
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	3380

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

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

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

Docket No.: 104093-0002-118
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of: Mark S. O'Hare, et al.	
Application No.: 15/977,748	Confirmation No.: 7200
Filed: May 11, 2018	Art Unit: 2827
For: SECURE DATA PARSER METHOD AND SYSTEM	Examiner: Not Yet Assigned

FIRST PRELIMINARY AMENDMENT

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

Dear Sir:

Prior to substantive examination, please amend the above-identified patent application as follows:

Amendments of the Claims are reflected on page 2 of this Preliminary Amendment.

Remarks/Arguments begin on page 7 of this Preliminary Amendment.

AMENDMENTS TO THE CLAIMS

This listing will replace all prior version and listings of claims in the above-identified patent application.

Listing of the Claims

1. (Canceled)

2. (New) A method for securing a data set, the method comprising:

distributing the data set into a plurality of data chunks, wherein none of the data chunks are, by themselves, sufficient to reconstruct the data set;

encrypting each of the data chunks with a respective one of a plurality of encryption keys;

obfuscating each of the plurality of different encryption keys; and

storing the plurality of data chunks with the plurality of obfuscated different encryption keys on a plurality of different storage devices.

3. (New) The method of claim 2, wherein obfuscating each of the plurality of different encryption keys comprises performing a transform on data indicative of at least one of the plurality of different encryption keys.

4. (New) The method of claim 3, wherein performing a transform on data indicative of at least one of the plurality of different encryption keys comprises performing an all-or-nothing transform on the data indicative of at least one of the plurality of different encryption keys.

5. (New) The method of claim 2, wherein obfuscating each of the plurality of different encryption keys comprises applying Shamir's Secret Sharing algorithm to data indicative of at least one of the plurality of different encryption keys.

6. (New) The method of claim 2, wherein storing the plurality of data chunks together with the plurality of obfuscated different encryption keys comprises storing each of the plurality of data chunks together with a respective one of the plurality of obfuscated different encryption keys.

7. (New) The method of claim 2, wherein storing the plurality of data chunks together with the plurality of obfuscated different encryption keys comprises including, with a data chunk of the plurality of data chunks, data indicative of an encryption key that was used to encrypt a different data chunk of the plurality of data chunks.

8. (New) The method of claim 2, wherein distributing the data set into a plurality of data chunks comprises using a random technique or pseudorandom technique.

9. (New) The method of claim 2, further comprising generating the data set by encrypting primary data.

10. (New) A method for securing a data set, the method comprising:

distributing the data set into a plurality of data chunks, wherein none of the data chunks are, by themselves, sufficient to reconstruct the data set;

encrypting each of the data chunks with a respective one of a plurality of encryption keys;

transforming each of the plurality of different encryption keys; and

storing the plurality of data chunks with the plurality of transformed different encryption keys on a plurality of different storage devices.

11. (New) The method of claim 10, wherein transforming each of the plurality of different encryption keys comprises performing an all-or-nothing transform on data indicative of at least one of the plurality of different encryption keys.

12. (New) The method of claim 10, wherein storing the plurality of data chunks with the plurality of transformed different encryption keys comprises storing each of the plurality of data chunks with a respective one of the plurality of transformed different encryption keys.

13. (New) The method of claim 10, wherein storing the plurality of data chunks with the plurality of transformed different encryption keys comprises including, with a data chunk of the plurality of data chunks, data indicative of an encryption key of the plurality of encryption keys that was used to encrypt a different data chunk of the plurality of data chunks.

14. (New) The method of claim 10, wherein distributing the data set into a plurality of data chunks comprises using a random technique or pseudorandom technique.

15. (New) The method of claim 10, further comprising generating the data by encrypting primary data.

16. (New) A computer system for securing a data set, the system comprising:

at least one hardware processor, configured to:

access the data set;

distribute the data set into a plurality of data chunks, wherein none of the data chunks are, by themselves, sufficient to reconstruct the data set;

encrypt each of the data chunks with a respective one of a plurality of encryption keys;

obfuscate each of the plurality of different encryption keys; and

storing the plurality of data chunks together with the plurality of obfuscated different encryption keys;

store the plurality of data chunks together with the plurality of obfuscated different encryption keys, wherein the plurality of data chunks is stored on a plurality of different storage devices.

17. (New) The computer system of claim 16, wherein, when obfuscating each of the plurality of different encryption keys, the at least one hardware processor is configured to perform a transform on data indicative of at least one of the plurality of different encryption keys.

18. (New) The computer system of claim 17, wherein, when performing a transform on data indicative of at least one of the plurality of different encryption keys, the at least one hardware processor is configured to perform an all-or-nothing transform on the data indicative of at least one of the plurality of different encryption keys.

19. (New) The computer system of claim 16, wherein, when obfuscating each of the plurality of different encryption keys, the at least one hardware processor is configured to apply Shamir's Secret Sharing algorithm to data indicative of at least one of the plurality of different encryption keys.

20. (New) The computer system of claim 16, wherein, when storing the plurality of data chunks together with the plurality of obfuscated different encryption keys, the at least one hardware processor is configured to store each of the plurality of data chunks together with a respective one of the plurality of obfuscated different encryption keys.

21. (New) The computer system of claim 16, wherein, when storing the plurality of data chunks together with the plurality of obfuscated different encryption keys, the at least one hardware processor is configured to include, with a data chunk of the plurality of data chunks, data indicative of an encryption key that was used to encrypt a different data chunk of the plurality of data chunks.

22. (New) A computer system for securing a data set, the system comprising:

at least one hardware processor, configured to:

access the data set;

distribute the data set into a plurality of data chunks, wherein none of the data chunks are, by themselves, sufficient to reconstruct the data set;

encrypt each of the data chunks with a respective one of a plurality of encryption keys;

transform each of the plurality of different encryption keys; and

storing the plurality of data chunks together with the plurality of transformed different encryption keys;

store the plurality of data chunks together with the plurality of transformed different encryption keys, wherein the plurality of data chunks is stored on a plurality of different storage devices.

23. (New) The computer system of claim 22, wherein, when transforming each of the plurality of different encryption keys, the at least one hardware processor is configured to perform an all-or-nothing transform on data indicative of at least one of the plurality of different encryption keys.

24. (New) The computer system of claim 22, wherein, when storing the plurality of data chunks with the plurality of transformed different encryption keys, the at least one hardware processor is configured to store each of the plurality of data chunks with a respective one of the plurality of transformed different encryption keys.

25. (New) The computer system of claim 22, wherein, when storing the plurality of data chunks with the plurality of transformed different encryption keys, the at least one hardware processor is configured to include, with a data chunk of the plurality of data chunks, data indicative of an encryption key of the plurality of encryption keys that was used to encrypt a different data chunk of the plurality of data chunks.

REMARKS

Claim 1 was pending in this application. Claim 1 is canceled. In addition, new claims 2-25 have been added. The new claims are fully supported by the originally filed specification.

An early and favorable action is respectfully requested.

Applicant believes no fee is due with this paper other than as set forth in the accompanying fee statement. However, if any additional fee is due, the Director is hereby authorized to charge Deposit Account No. 06-1075, under Order No. 104093-0002-118.

Dated: September 6, 2018

Respectfully submitted,

By: /Maxim Rapoport/
Maxim Rapoport
Registration No.: 67,675
HALEY GUILIANO LLP
Customer No. 15314
75 Broad Street, Suite 1000
New York, New York 10004
646-973-2500
Attorney for Applicant

PTO/AIA/22 (03-13)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)	Docket Number (Optional) 104093-0002-118
Application Number 15/977,748	Filed May 11, 2018
For SECURE DATA PARSER METHOD AND SYSTEM	
Art Unit 2827	Examiner Not Yet Assigned

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

		Fee	Small Entity Fee	Micro Entity Fee	
☑	One month (37 CFR 1.17(a)(1))	$200	$100	$50	$ 200
☐	Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$
☐	Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$
☐	Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐	Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☐ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 06-1075.

☑ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant.

☑ attorney or agent of record. Registration number 67,675.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/Maxim Rapoport/	September 6, 2018
Signature	Date
Maxim Rapoport	646-973-2500
Typed or printed name	Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☑ * Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.136(a). 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 6 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: Mail Stop PCT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Electronic Patent Application Fee Transmittal

Application Number:	15977748
Filing Date:	11-May-2018
Title of Invention:	SECURE DATA PARSER METHOD AND SYSTEM
First Named Inventor/Applicant Name:	Mark S. O'Hare
Filer:	Maxim Rapoport/Juanita Alvarez
Attorney Docket Number:	104093-0002-118

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
UTILITY APPLICATION FILING	1011	1	300	300
UTILITY SEARCH FEE	1111	1	660	660
UTILITY EXAMINATION FEE	1311	1	760	760
Pages:				
UTILITY APPL SIZE FEE PER 50 SHEETS >100	1081	2	400	800
Claims:				
CLAIMS IN EXCESS OF 20	1202	4	100	400
INDEPENDENT CLAIMS IN EXCESS OF 3	1201	1	460	460

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous-Filing:				
LATE FILING FEE FOR OATH OR DECLARATION	1051	1	160	160
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 1 month with $0 paid	1251	1	200	200
Miscellaneous:				
		Total in USD ($)		**3740**

Electronic Acknowledgement Receipt	
EFS ID:	33651255
Application Number:	15977748
International Application Number:	
Confirmation Number:	7200
Title of Invention:	SECURE DATA PARSER METHOD AND SYSTEM
First Named Inventor/Applicant Name:	Mark S. O'Hare
Customer Number:	15314
Filer:	Maxim Rapoport/Juanita Alvarez
Filer Authorized By:	Maxim Rapoport
Attorney Docket Number:	104093-0002-118
Receipt Date:	06-SEP-2018
Filing Date:	11-MAY-2018
Time Stamp:	20:21:37
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$3740
RAM confirmation Number	090718INTEFSW00006192061075
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	Applicant Response to Pre-Exam Formalities Notice	104093_0002_118_Reply_to_Missing_Parts.pdf	97390 9b49368176c98df262c574dc0c6471e63176d8f9	no	1
Warnings:					
Information:					
2		104093_0002_118_Preliminary_Amendment.pdf	117180 3d4723c9bca2bca64fc55141072d55040db0e5bf	yes	7

Multipart Description/PDF files in .zip description

Document Description	Start	End
Preliminary Amendment	1	1
Claims	2	6
Applicant Arguments/Remarks Made in an Amendment	7	7

Warnings:					
Information:					
3	Extension of Time	104093_0002_118_1_MO_EOT.pdf	734928 f07178421ba104ca2f475aff189dda46719af2a9	no	1
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	43695 69e29e2336d637c09f57c2a25de24bb9f17d5eda	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	993193		

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.

Docket No.: 104093-0002-118
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of: Mark S. O'Hare, et al.	
Application No.: 15/977,748	Confirmation No.: 7200
Filed: May 11, 2018	Art Unit: 2827
For: SECURE DATA PARSER METHOD AND SYSTEM	Examiner: Not Yet Assigned

RESPONSE TO NOTICE TO FILE MISSING PARTS OF APPLICATION

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

Dear Sir:

In response to the Notice to File Missing Parts of Application mailed June 6, 2018, Applicant respectfully submits the Filing Fee for the Application (as shown on accompanying Fee Transmittal) an Extension of Time and a Preliminary Amendment.

Please charge our Deposit Account No. 06-1075 in the amount of $3740 covering the fees set forth in 37 C.F.R. § 1.16(a), 1.16(f), 1.16(h), 1.16(i), 1.16(k), 1.16(o), 1.16(s), and 1.17(a)(1). The Director is hereby authorized to charge any deficiency in the fees filed, asserted to be filed or which should have been filed herewith (or with any paper hereafter filed in this application by this firm) to our Deposit Account No. 06-1075.

Dated: September 6, 2018

Respectfully submitted,

By: /Maxim Rapoport/
Maxim Rapoport
Registration No.: 67,675
HALEY GUILIANO LLP
Customer No. 15314
75 Broad Street, Suite 1000
New York, New York 10004
646-973-2500
Attorney for Applicant

742420_1

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 15/977,748	Filing Date 05/11/2018	☐ To be Mailed

ENTITY: ☑ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $100 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $460 =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

AMENDMENT	09/06/2018	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 24	Minus	** 24	= 0		x $100 =	0
	Independent (37 CFR 1.16(h))	* 4	Minus	*** 4	= 0		x $460 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

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

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.	LDRC
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/eva gillis/
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".	
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.	

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

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

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 15/977,748

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	300
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	660
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	760
TOTAL CLAIMS (37 CFR 1.16(i))	1 minus 20 =	*			OR	x 100 =	0.00
INDEPENDENT CLAIMS (37 CFR 1.16(h))	1 minus 3 =	*				x 460 =	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).						800
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	2520

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

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

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
15/977,748	05/11/2018	Mark S. O'Hare	104093-0002-118

CONFIRMATION NO. 7200

15314
Haley Guiliano LLP
75 Broad Street
Suite 1000
New York, NY 10004

FORMALITIES LETTER

OC000000100008852

Date Mailed: 06/06/2018

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The statutory basic filing fee is missing.
- The application search fee must be submitted.
- The application examination fee must be submitted.
- Surcharge as set forth in 37 CFR 1.16(f) must be submitted.
  The surcharge is due for any one of:
  - late submission of the basic filing fee, search fee, or examination fee,
  - late submission of inventor's oath or declaration,
  - filing an application that does not contain at least one claim on filing, or
  - submission of an application filed by reference to a previously filed application.

SUMMARY OF FEES DUE:

The fee(s) required within **TWO MONTHS** from the date of this Notice to avoid abandonment is/are itemized below. No entity status discount is in effect. If applicant is qualified for small entity status, a written assertion of small entity status must be submitted to establish small entity status. (See 37 CFR 1.27). If applicant is qualified for micro entity status, an acceptable Certification of Micro Entity Status must be submitted to establish micro entity status. (See 37 CFR 1.29 and forms PTO/SB/15A and 15B.)

- $ **300** basic filing fee.
- $ **800** for **70** electronically equivalent pages in excess of **100** application size fee.
- $ **160** surcharge.
- $ **660** search fee.
- $ **760** examination fee.
- $(**0**) previous unapplied payment amount.
- $ **2680** TOTAL FEE BALANCE DUE.

Replies must be received in the USPTO within the set time period or must include a proper Certificate of Mailing or Transmission under 37 CFR 1.8 with a mailing or transmission date within the set time period. For more information and a suggested format, see Form PTO/SB/92 and MPEP 512.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web, including a copy of this Notice and selecting the document description "Applicant response to Pre-Exam Formalities Notice". https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at 1-866-217-9197 or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/hchin/

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
15/977,748	05/11/2018	2827	0.00	104093-0002-118	1	1

CONFIRMATION NO. 7200

15314
Haley Guiliano LLP
75 Broad Street
Suite 1000
New York, NY 10004

FILING RECEIPT

OC000000100008851

Date Mailed: 06/06/2018

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)

Mark S. O'Hare, Coto De Caza, CA;
Rick L. Orsini, Flower Mound, TX;
Roger S. Davenport, Campbell, TX;
Steven Winick, Roslyn Heights, NY;

Applicant(s)

Security First Corp., Rancho Santa Margarita, CA;

Power of Attorney: The patent practitioners associated with Customer Number 15314

Domestic Priority data as claimed by applicant

This application is a CON of 13/915,081 06/11/2013 PAT 9992170
which is a DIV of 13/468,383 05/10/2012 PAT 9338140
which is a CON of 11/258,839 10/25/2005 PAT 8266438
which claims benefit of 60/718,185 09/16/2005
and claims benefit of 60/622,146 10/25/2004

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: 06/04/2018

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 15/977,748**

Projected Publication Date: To Be Determined - pending completion of Missing Parts

Non-Publication Request: No

Early Publication Request: No

Title

SECURE DATA PARSER METHOD AND SYSTEM

Preliminary Class

365

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

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

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

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

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

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

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific

countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

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

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

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

NOT GRANTED

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

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop

technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 1 of 23	Attorney Docket Number	104093-0002-118

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-4,453,074	06-05-1984	Weinstein	
		US-4,802,220	01-31-1989	Marker, Jr.	
		US-4,924,513	05-08-1990	Herbison et al.	
		US-4,932,057	06-05-1990	Kolbert	
		US-5,010,572	04-23-1991	Bathrick et al.	
		US-5,016,274	05-14-1991	Micali et al.	
		US-5,051,745	09-24-1991	Katz	
		US-5,150,407	09-22-1992	Chan	
		US-5,163,096	11-10-1992	Clark et al.	
		US-5,239,659	08-24-1993	Rudeseal et al.	
		US-5,268,963	12-07-1993	Monroe et al.	
		US-5,375,244	12-20-1994	McNair	
		US-5,386,104	01-31-1995	Sime	
		US-5,450,099	09-12-1995	Stephenson et al.	
		US-5,485,474	01-16-1996	Rabin	
		US-5,524,073	06-04-1996	Stambler	
		US-5,603,003	02-11-1997	Akizawa et al.	
		US-5,615,269	03-25-1997	Micali	
		US-5,623,546	04-22-1997	Hardy et al.	
		US-5,623,549	04-22-1997	Ritter	
		US-5,642,508	06-24-1997	Miyazawa	
		US-5,666,414	09-09-1997	Micali	
		US-5,666,416	09-09-1997	Micali	
		US-5,666,514	09-09-1997	Cheriton	
		US-5,682,425	10-28-1997	Enari	
		US-5,703,907	12-30-1997	James	
		US-5,717,758	02-10-1998	Micall	
		US-5,748,735	05-05-1998	Ganesan	
		US-5,761,306	06-02-1998	Lewis	
		US-5,761,311	06-02-1998	Spelman et al.	
		US-5,768,382	06-16-1998	Schneier et al.	
		US-5,768,388	06-16-1998	Goldwasser 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.

T^1 – Applicant is to place a check mark here if English language Translation is attached.

442734_1

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 2 of 23	Attorney Docket Number	104093-0002-118

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-5,768,519	06-16-1998	Swift et al.	
		US-5,790,677	08-04-1998	Fox et al.	
		US-5,823,948	10-20-1998	Ross, Jr. et al.	
		US-5,903,652	05-11-1999	Mital	
		US-5,903,882	05-11-1999	Asay et al.	
		US-5,910,987	06-08-1999	Ginter et al.	
		US-5,915,019	06-22-1999	Ginter et al.	
		US-5,915,024	06-22-1999	Kitaori et al.	
		US-5,917,913	06-29-1999	Wang	
		US-5,937,066	08-10-1999	Gennaro et al.	
		US-5,940,507	08-01-1999	Cane et al.	
		US-5,960,083	09-28-1999	Micali	
		US-5,966,444	10-12-1999	Yuan et al.	
		US-5,966,448	10-12-1999	Namba et al.	
		US-5,974,144	10-26-1999	Brandman	
		US-5,982,322	11-09-1999	Bickley et al.	
		US-5,987,232	11-16-1999	Tabuki	
		US-5,991,414	11-23-1999	Garay et al.	
		US-5,995,630	11-30-1999	Borza	
		US-6,009,173	12-28-1999	Sumner	
		US-6,009,177	12-28-1999	Sudia	
		US-6,023,508	02-08-2000	Bombard et al.	
		US-6,026,163	02-15-2000	Micali	
		US-6,058,188	05-02-2000	Chandersekaran et al.	
		US-6,061,790	05-09-2000	Bodnar	
		US-6,073,237	06-06-2000	Ellison	
		US-6,078,888	06-20-2000	Johnson, Jr.	
		US-6,084,968	07-04-2000	Kennedy et al.	
		US-6,088,454	07-11-2000	Nagashima et al.	
		US-6,092,201	07-18-2000	Turnbull et al.	
		US-6,094,485	07-25-2000	Weinstein et al.	
		US-6,118,874	09-12-2000	Okamoto 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.

T^1 – Applicant is to place a check mark here if English language Translation is attached.

442734_1

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 3 of 23	Attorney Docket Number	104093-0002-118

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-6,134,550	10-17-2000	Van Oorschot et al.	
		US-6,182,214	01-30-2001	Hardjono	
		US-6,192,472	02-20-2001	Garay et al.	
		US-6,226,385	05-01-2001	Taguchi et al.	
		US-6,229,894	05-08-2001	Van Oorschot et al.	
		US-6,240,183	05-29-2001	Marchant	
		US-6,240,187	05-29-2001	Lewis	
		US-6,240,188	05-29-2001	Dondeti et al.	
		US-6,256,737	07-03-2001	Bianco et al.	
		US-6,260,125	07-10-2001	McDowell	
		US-6,266,413	07-24-2001	Shefi	
		US-6,269,432	07-31-2001	Smith	
		US-6,289,455	09-11-2001	Kocher et al.	
		US-6,289,509	09-11-2001	Kryloff	
		US-6,292,568	09-18-2001	Akins, III et al.	
		US-6,292,782	09-18-2001	Weideman	
		US-6,301,659	10-09-2001	Micali	
		US-6,307,940	10-23-2001	Yamamoto et al.	
		US-6,314,409	11-06-2001	Schneck et al.	
		US-6,324,650	11-27-2001	Ogilvie	
		US-6,336,186	01-01-2002	Dyksterhouse et al.	
		US-6,345,101	02-05-2002	Shukla	
		US-6,345,314	02-05-2002	Cole et al.	
		US-6,347,143	02-12-2002	Goff et al.	
		US-6,356,941	03-12-2002	Cohen	
		US-6,363,425	03-26-2002	Hook et al.	
		US-6,363,481	03-26-2002	Hardjono	
		US-6,381,331	04-30-2002	Kato	
		US-6,385,318	05-07-2002	Oishi	
		US-6,386,451	05-14-2002	Sehr	
		US-6,411,716	06-25-2002	Brickell	
		US-6,415,373	07-02-2002	Peters 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.

T^1 – Applicant is to place a check mark here if English language Translation is attached.

442734_1

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 4 of 23	Attorney Docket Number	104093-0002-118

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-6,424,718	07-23-2002	Holloway	
		US-6,438,690	08-20-2002	Patel et al.	
		US-6,446,204	09-03-2002	Pang et al.	
		US-6,449,730	09-10-2002	Mann et al.	
		US-6,453,416	09-17-2002	Epstein	
		US-6,466,552	10-15-2002	Haumont	
		US-6,473,858	10-29-2002	Shimomura et al.	
		US-6,473,860	10-29-2002	Chan	
		US-6,483,921	11-19-2002	Harkins	
		US-6,505,216	01-07-2003	Schutzman et al.	
		US-6,519,262	02-11-2003	Stephens et al.	
		US-6,553,493	04-22-2003	Okumura et al.	
		US-6,557,123	04-29-2003	Wiencko, Jr. et. al.	
		US-6,615,347	09-02-2003	De Silva et al.	
		US-6,625,734	09-23-2003	Marvit et al.	
		US-6,631,201	10-07-2003	Dickinson et al.	
		US-6,684,330	01-27-2004	Wack et al.	
		US-6,687,375	02-03-2004	Matyas, Jr. et al.	
		US-6,701,303	03-02-2004	Dunn et al.	
		US-6,731,755	05-04-2004	Cocks	
		US-6,785,768	08-31-2004	Peters et al.	
		US-6,789,198	09-07-2004	Chan	
		US-6,807,649	10-19-2004	Murthy	
		US-6,816,970	11-09-2004	Morgan et al.	
		US-6,819,766	11-16-2004	Weidong	
		US-6,852,988	02-08-2005	Li	
		US-6,853,988	02-08-2005	Dickinson et al.	
		US-6,856,383	02-15-2005	Vachris et al.	
		US-6,898,285	05-24-2005	Hutchings et al.	
		US-6,915,436	07-05-2005	Booth, III et al.	
		US-6,931,549	08-16-2005	Ananda	
		US-6,947,557	09-20-2005	Megiddo 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.

T^1 – Applicant is to place a check mark here if English language Translation is attached.

442734_1

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 5 of 23	Attorney Docket Number	104093-0002-118

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-6,952,684	10-04-2005	Toshikage et al.	
		US-6,959,383	10-25-2005	Terada et al.	
		US-6,965,993	11-15-2005	Baker	
		US-6,978,367	12-20-2005	Hind et al.	
		US-6,981,141	12-27-2005	Mahne et al.	
		US-7,003,531	02-21-2006	Holenstein et al.	
		US-7,003,668	02-21-2006	Berson et al.	
		US-7,035,405	04-25-2006	Schwenk	
		US-7,039,189	05-02-2006	Kienzle et al.	
		US-7,050,580	05-23-2006	Ferre Herrero	
		US-7,050,583	05-23-2006	Montgomery	
		US-7,058,605	06-06-2006	Gupta	
		US-7,069,451	06-27-2006	Ginter et al.	
		US-7,072,917	07-04-2006	Wong et al.	
		US-7,076,651	07-11-2006	Droge	
		US-7,085,854	08-01-2006	Corente	
		US-7,096,494	08-22-2006	Chen	
		US-7,107,385	09-12-2006	Rajan et al.	
		US-7,111,173	09-19-2006	Scheidt	
		US-7,111,303	09-19-2006	Macchiano et al.	
		US-7,117,365	10-03-2006	Rump et al.	
		US-7,133,845	11-07-2006	Ginter et al.	
		US-7,140,044	11-21-2006	Redlich et al.	
		US-7,143,289	11-28-2006	Denning et al.	
		US-7,171,685	01-30-2007	Batra et al.	
		US-7,174,385	02-06-2007	Li	
		US-7,187,771	03-06-2007	Dickinson et al.	
		US-7,188,203	03-06-2007	Mowry et al.	
		US-7,191,252	03-13-2007	Redlich et al.	
		US-7,191,410	03-13-2007	Kruempelmann et al.	
		US-7,203,844	04-10-2007	Oxford	
		US-7,203,871	04-10-2007	Turner 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.

T^1 – Applicant is to place a check mark here if English language Translation is attached.

442734_1

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 6 of 23	Attorney Docket Number	104093-0002-118

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-7,206,250	04-17-2007	Groux	
		US-7,213,158	05-01-2007	Bantz et al.	
		US-7,218,736	05-15-2007	Nishimura et al.	
		US-7,222,062	05-22-2007	Goud et al.	
		US-7,225,158	05-29-2007	Toshikage et al.	
		US-7,228,337	06-05-2007	Bornstein et al.	
		US-7,234,063	06-19-2007	Baugher et al.	
		US-7,260,724	08-21-2007	Dickinson et al.	
		US-7,260,727	08-21-2007	Fougeroux et al.	
		US-7,277,958	10-02-2007	Chung et al.	
		US-7,302,583	11-27-2007	Forrest	
		US-7,304,990	12-04-2007	Rajwan	
		US-7,313,825	12-25-2007	Redlich et al.	
		US-7,322,047	01-22-2008	Redlich et al.	
		US-7,337,320	02-26-2008	Tada et al.	
		US-7,346,773	03-18-2008	Cam-Winget et al.	
		US-7,346,925	03-18-2008	Marcjan	
		US-7,349,539	03-25-2008	Wee et al.	
		US-7,349,987	03-25-2008	Redlich et al.	
		US-7,356,818	04-08-2008	Carollo et al.	
		US-7,363,361	04-22-2008	Tewari et al.	
		US-7,391,865	06-24-2008	Orsini et al.	
		US-7,392,403	06-24-2008	Munetoh	
		US-7,412,462	08-12-2008	Margolus et al.	
		US-7,428,751	09-23-2008	Oom Temudo de Castro et al.	
		US-7,428,754	09-23-2008	Neumann et al.	
		US-7,440,953	10-21-2008	Sidman	
		US-7,444,421	10-28-2008	Katayama	
		US-7,464,152	12-09-2008	Ishizaki et al.	
		US-7,469,340	12-23-2008	Karamchedu et al.	
		US-7,472,105	12-30-2008	Staddon 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.

T^1 – Applicant is to place a check mark here if English language Translation is attached.

442734_1

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 7 of 23	Attorney Docket Number	104093-0002-118

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-7,478,427	01-13-2009	Mukherjee et al.	
		US-7,499,905	03-03-2009	Jaschek et al.	
		US-7,535,905	05-19-2009	Narayanan et al.	
		US-7,546,427	06-09-2009	Gladwin et al.	
		US-7,548,556	06-16-2009	Wittenschlaeger	
		US-7,549,061	06-16-2009	Nonaka et al.	
		US-7,552,482	06-23-2009	Redlich et al.	
		US-7,577,689	08-18-2009	Masinter et al.	
		US-7,584,285	09-01-2009	Hudson et al.	
		US-7,587,368	09-08-2009	Felsher	
		US-7,596,570	09-29-2009	Emigh et al.	
		US-7,596,741	09-29-2009	LaVigne et al.	
		US-7,609,687	10-27-2009	Kobayashi et al.	
		US-7,623,809	11-24-2009	Nakano et al.	
		US-7,627,125	12-01-2009	Lumsden et al.	
		US-7,649,992	01-19-2010	Raju et al.	
		US-7,657,760	02-02-2010	Teramoto et al.	
		US-7,669,051	02-23-2010	Redlich et al.	
		US-7,693,992	04-06-2010	Watson	
		US-7,721,150	05-18-2010	Belyakov et al.	
		US-7,721,344	05-18-2010	Redlich et al.	
		US-7,730,543	06-01-2010	Nath	
		US-7,743,261	06-22-2010	Nonaka et al.	
		US-7,752,482	07-06-2010	Gredone et al.	
		US-7,756,792	07-13-2010	Hughes	
		US-7,765,411	07-27-2010	Hennessey et al.	
		US-7,788,532	08-31-2010	Kawamura	
		US-7,801,781	09-21-2010	Olin et al.	
		US-7,831,995	11-09-2010	Futoransky et al.	
		US-7,865,741	01-04-2011	Wood et al.	
		US-7,869,597	01-11-2011	Nakai et al.	
		US-7,916,871	03-29-2011	Brookner 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.

T^1 – Applicant is to place a check mark here if English language Translation is attached.

442734_1

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 8 of 23	Attorney Docket Number	104093-0002-118

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-7,921,288	04-05-2011	Hildebrand	
		US-7,926,090	04-12-2011	Blevins et al.	
		US-7,929,697	04-19-2011	McNeely et al.	
		US-7,934,100	04-26-2011	Fujimaki	
		US-7,940,932	05-10-2011	Paksoy et al.	
		US-7,983,994	07-19-2011	Hurry	
		US-8,009,830	08-30-2011	Orsini et al.	
		US-8,041,875	10-18-2011	Shah et al.	
		US-8,060,088	11-15-2011	Ihattula	
		US-8,060,832	11-15-2011	Kruempelmann et al.	
		US-8,095,800	01-10-2012	Creary et al.	
		US-8,112,622	02-07-2012	Qi	
		US-8,135,134	03-13-2012	Orsini et al.	
		US-8,135,980	03-13-2012	Dodgson et al.	
		US-8,151,333	04-03-2012	Zhu et al.	
		US-8,155,322	04-10-2012	Bellare et al.	
		US-8,189,769	05-29-2012	Ramasamy et al.	
		US-8,190,905	05-29-2012	Chang et al.	
		US-8,195,976	06-05-2012	Rao et al.	
		US-8,208,897	06-26-2012	Kaneko et al.	
		US-8,213,387	07-03-2012	Xia et al.	
		US-8,250,643	08-21-2012	Enomoto et al.	
		US-8,261,084	09-04-2012	Nonaka et al.	
		US-8,261,265	09-04-2012	Chen et al.	
		US-8,266,438	09-11-2012	Orsini et al.	
		US-8,271,802	09-18-2012	Orsini et al.	
		US-8,300,822	10-30-2012	Nakai et al.	
		US-8,307,443	11-06-2012	Wang et al.	
		US-8,332,638	12-11-2012	Orsini et al.	
		US-8,341,115	12-25-2012	Natanzon et al.	
		US-8,347,084	01-01-2013	Tavernier et al.	
		US-8,352,941	01-08-2013	Protopopov 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.

T^1 – Applicant is to place a check mark here if English language Translation is attached.

442734_1

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 9 of 23	Attorney Docket Number	104093-0002-118

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-8,392,682	03-05-2013	Dodgson et al.	
		US-8,396,895	03-12-2013	Miloushev et al.	
		US-8,397,083	03-12-2013	Sussland et al.	
		US-8,397,084	03-12-2013	Ranade	
		US-8,397,288	03-12-2013	Melvin, Jr. et al.	
		US-8,473,757	06-25-2013	Gladstone et al.	
		US-8,578,076	11-05-2013	Van der Linden et al.	
		US-8,635,456	01-21-2014	Fascenda	
		US-8,755,322	06-17-2014	Miettinen et al.	
		US-8,761,401	06-24-2014	Sprunk et al.	
		US-8,959,199	02-17-2015	Peleg et al.	
		US-2001/0024502	09-27-2001	Ohkuma et al.	
		US-2001/0050990	12-13-2001	Sudia	
		US-2001/0051902	12-13-2001	Messner	
		US-2002/0016773	02-07-2002	Ohkuma et al.	
		US-2002/0016926	02-07-2002	Nguyen et al.	
		US-2002/0023210	02-21-2002	Tuomenoksa et al.	
		US-2002/0031230	03-14-2002	Sweet et al.	
		US-2002/0032663	03-14-2002	Messner	
		US-2002/0046359	04-18-2002	Boden	
		US-2002/0071566	06-13-2002	Kurn	
		US-2002/0075844	06-20-2002	Hagen	
		US-2002/0080888	06-27-2002	Shu et al.	
		US-2002/0087866	07-04-2002	Berson et al.	
		US-2002/0129235	09-12-2002	Okamoto et al.	
		US-2002/0129245	09-12-2002	Cassagnol et al.	
		US-2002/0157007	10-24-2002	Sashihara	
		US-2002/0162047	10-31-2002	Peters et al.	
		US-2002/0172358	11-21-2002	Hurich	
		US-2002/0178355	11-28-2002	D'Sa et al.	
		US-2002/0178361	11-28-2002	Genty et al.	
		US-2002/0184444	12-05-2002	Shandony	

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.

T^1 – Applicant is to place a check mark here if English language Translation is attached.

442734_1

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 10 of 23	Attorney Docket Number	104093-0002-118

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-2002/0191796	12-19-2002	Muschenborn	
		US-2003/0005094	01-02-2003	YUAN et al.	
		US-2003/0023958	01-30-2003	Patel et al.	
		US-2003/0051159	03-13-2003	McCown et al.	
		US-2003/0055905	03-20-2003	Nishiyama et al.	
		US-2003/0058274	03-27-2003	Hill et al.	
		US-2003/0061481	03-27-2003	Levine et al.	
		US-2003/0084020	05-01-2003	Shu	
		US-2003/0084290	05-01-2003	Murty et al.	
		US-2003/0084397	05-01-2003	Peleg	
		US-2003/0110188	06-12-2003	Howard et al.	
		US-2003/0126434	07-03-2003	Lim et al.	
		US-2003/0167408	09-04-2003	Fitzpatrick et al.	
		US-2003/0182435-A1	09-25-2003	Redlich et al.	
		US-2003/0188153	10-02-2003	Demoff et al.	
		US-2003/0204605	10-30-2003	Hudson et al.	
		US-2003/0236943	12-25-2003	Delaney	
		US-2004/0022390	02-05-2004	McDonald et al.	
		US-2004/0049687	03-11-2004	Orsini et al.	
		US-2004/0078542	04-22-2004	Fuller et al.	
		US-2004/0122960	06-24-2004	Hall et al.	
		US-2004/0193878	09-30-2004	Dillinger et al.	
		US-2004/0208170	10-21-2004	Miyazaki et al.	
		US-2004/0215955	10-28-2004	Tamai et al.	
		US-2004/0268148	12-30-2004	Karjala et al.	
		US-2005/0050004	03-03-2005	Sheu et al.	
		US-2005/0071631	03-31-2005	Langer	
		US-2005/0111657-A1	05-26-2005	Lee et al.	
		US-2005/0132060	06-16-2005	Mo et al.	
		US-2005/0160290	07-21-2005	Moon et al.	
		US-2005/0198306	09-08-2005	Palojarvi et al.	
		US-2005/0210243	09-22-2005	Archard 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.

T^1 – Applicant is to place a check mark here if English language Translation is attached.

442734_1

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 11 of 23	Attorney Docket Number	104093-0002-118

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-2005/0289218	12-29-2005	Rothman et al.	
		US-2006/0020646	01-26-2006	Tee et al.	
		US-2006/0046728	03-02-2006	Jung et al.	
		US-2006/0075222	04-06-2006	Moloney et al.	
		US-2006/0075225	04-06-2006	Flynn et al.	
		US-2006/0078127	04-13-2006	Cacayorin	
		US-2006/0090200	04-27-2006	Oie	
		US-2006/0165060	07-27-2006	Dua	
		US-2006/0282681	12-14-2006	Scheidt et al.	
		US-2007/0006015	01-04-2007	Rao et al.	
		US-2007/0033644	02-08-2007	Thomas et al.	
		US-2007/0064704	03-22-2007	Balay et al.	
		US-2007/0071234	03-29-2007	Lagrange et al.	
		US-2007/0094272	04-26-2007	Yeh	
		US-2007/0097885	05-03-2007	Traversat et al.	
		US-2007/0122111	05-31-2007	Yamamoto et al.	
		US-2007/0124584	05-31-2007	Gupta	
		US-2007/0157025	07-05-2007	Sastry et al.	
		US-2007/0160198	07-12-2007	Orsini et al.	
		US-2007/0162744	07-12-2007	Hoshino et al.	
		US-2007/0165865	07-19-2007	Talvitie	
		US-2008/0016334	01-17-2008	Kurapati et al.	
		US-2008/0037557	02-14-2008	Fujita et al.	
		US-2008/0046752	02-21-2008	Berger et al.	
		US-2008/0072035	03-20-2008	Johnson et al.	
		US-2008/0126614	05-29-2008	Ooi et al.	
		US-2008/0147821	06-19-2008	Dietrich et al.	
		US-2008/0155252	06-26-2008	Nambiar	
		US-2008/0170693	07-17-2008	Spies et al.	
		US-2008/0183975	07-31-2008	Foster et al.	
		US-2008/0183992	07-31-2008	Martin et al.	
		US-2008/0232592	09-25-2008	Lee 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.

T^1 – Applicant is to place a check mark here if English language Translation is attached.

442734_1

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 12 of 23	Attorney Docket Number	104093-0002-118

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-2008/0240441	10-02-2008	Kawakami	
		US-2008/0244277	10-02-2008	Orsini et al.	
		US-2008/0270603	10-30-2008	Berger et al.	
		US-2008/0294646	11-27-2008	Chang et al.	
		US-2008/0297326	12-04-2008	Chakraborty et al.	
		US-2009/0077379	03-19-2009	Geyzel et al.	
		US-2009/0092252	04-09-2009	Noll et al.	
		US-2009/0097657	04-16-2009	Scheidt et al.	
		US-2009/0113203	04-30-2009	Tsuge et al.	
		US-2009/0144202	06-04-2009	Hurry	
		US-2009/0172417	07-02-2009	Mikami et al.	
		US-2009/0177894	07-09-2009	Orsini et al.	
		US-2009/0209232	08-20-2009	Cha et al.	
		US-2009/0254572	10-08-2009	Redlich et al.	
		US-2009/0254750	10-08-2009	Bono et al.	
		US-2009/0288167	11-19-2009	Freericks et al.	
		US-2009/0292919	11-26-2009	England	
		US-2009/0292930	11-26-2009	Marano et al.	
		US-2009/0300284	12-03-2009	Murotani et al.	
		US-2009/0304004	12-10-2009	Huynh Van et al.	
		US-2009/0305900	12-10-2009	Belouchi et al.	
		US-2010/0005028	01-07-2010	Hartley et al.	
		US-2010/0046750	02-25-2010	Asfour	
		US-2010/0054474	03-04-2010	Schneider	
		US-2010/0077252	03-25-2010	Siewert et al.	
		US-2010/0095354	04-15-2010	Uchida et al.	
		US-2010/0125730	05-20-2010	Dodgson et al.	
		US-2010/0150341	06-17-2010	Dodgson et al.	
		US-2010/0153703	06-17-2010	Dodgson et al.	
		US-2010/0154053	06-17-2010	Dodgson et al.	
		US-2010/0162001 A1	06-24-2010	Dodgson; David	
		US-2010/0162004	06-24-2010	Dodgson 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.

T^1 – Applicant is to place a check mark here if English language Translation is attached.

442734_1

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 13 of 23	Attorney Docket Number	104093-0002-118

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-2010/0191958	07-29-2010	Chen	
		US-2010/0223613	09-02-2010	Schneider	
		US-2010/0268966	10-21-2010	Leggette et al.	
		US-2010/0283734	11-11-2010	Hallbauer et al.	
		US-2010/0293380	11-18-2010	Wiseman et al.	
		US-2010/0299313	11-25-2010	ORSINI et al.	
		US-2010/0306578	12-02-2010	THORNTON et al.	
		US-2010/0318812	12-16-2010	Auradkar et al.	
		US-2010/0332617	12-30-2010	Goodwin et al.	
		US-2011/0085667	04-14-2011	BERRIOS et al.	
		US-2011/0093113	04-21-2011	Sager et al.	
		US-2011/0125849	05-26-2011	Boyd et al.	
		US-2011/0135094	06-09-2011	Muto et al.	
		US-2011/0145413	06-16-2011	Dawson et al.	
		US-2011/0179214	07-21-2011	Goggin et al.	
		US-2011/0179271	07-21-2011	Orsini et al.	
		US-2011/0179287	07-21-2011	Orsini et al.	
		US-2011/0246766	10-06-2011	Orsini et al.	
		US-2011/0246817	10-06-2011	Orsini et al.	
		US-2012/0042034	02-16-2012	Goggin et al.	
		US-2012/0072723	03-22-2012	Orsini et al.	
		US-2012/0166576	06-28-2012	Orsini et al.	
		US-2012/0166818	06-28-2012	Orsini et al.	
		US-2012/0179916	07-12-2012	Staker et al.	
		US-2012/0198338	08-02-2012	Flint et al.	
		US-2012/0221854	08-30-2012	Orsini et al.	
		US-2012/0221855	08-30-2012	Orsini et al.	
		US-2012/0221856	08-30-2012	Orsini et al.	
		US-2012/0222134	08-30-2012	Orsini et al.	
		US-2012/0226904	09-06-2012	Orsini et al.	
		US-2012/0255034	10-04-2012	Orsini et al.	
		US-2012/0255035	10-04-2012	Orsini 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.

T^1 – Applicant is to place a check mark here if English language Translation is attached.

442734_1

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 14 of 23	Attorney Docket Number	104093-0002-118

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-2012/0266231	10-18-2012	Spiers et al.	
		US-2013/0042105	02-14-2013	Orsini et al.	

FOREIGN PATENT PUBLICATIONS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[1]
		AU-2004248616	06-04-2009	Security First Corporation		
		CN-101375284-A	02-25-2009	Orsini Rick L		
		CN-1329417A	01-02-2002	IBM		
		CN-1347225A	05-01-2002	Yang Gaoxiong		
		CN-1607762A	04-20-2005	Microsoft Corp.		
		CN-1613111A	05-04-2005	Sony Music Entertainment Inc.		
		EP-0485090-A2	05-13-1992	Visa Int Service Ass		
		EP-0798892 A2	10-01-1997	IBM		
		EP-0821504	01-28-1998	Nippon Telegraph and Telephone Corporation		
		EP-0851629-A2	07-01-1998	Canon Kk		
		EP-0862301	09-02-1998	Fujitsu Limited		
		EP-1011222	06-21-2000	Fujitsu Limited		
		EP-1239384-A2	09-11-2002	Pkware Inc		
		EP-2309700-A1	04-13-2011	Alcatel Lucent		
		EP-346180	12-13-1989	France Telecom		
		EP-354774	02-14-1990	International Business Machines Corporation		
		EP-636259	02-01-1995	Secure Computing Corporation		
		EP-793367	09-03-1997	Oki Electric Industry Co., Ltd.		
		FR-2632469	12-08-1989	Pailles Jean Claude		
		GB-2237670-A	05-08-1991	De La Rue Syst 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.

T[1] – Applicant is to place a check mark here if English language Translation is attached.

442734_1

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 15 of 23	Attorney Docket Number	104093-0002-118

FOREIGN PATENT PUBLICATIONS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T^1
		JP-04297157-A	10-21-1992	Mitsubishi Electric Corp		
		JP-2003/132234	05-09-2003	Global Friendship Inc.		
		JP-2004-185573	07-02-2004	Nec Infrontia Corp		
		JP-2005/136739	05-26-2005	Furukawa Electric Co Ltd.		
		JP-2005-244379-A	09-08-2005	Nec Communication Syst		
		JP-2005-267520	09-29-2005	Ntt Comware Corp		
		JP-2006-174152-A	06-29-2006	Matsushita Electric Works Ltd.		
		JP-2007-334836	12-27-2007	Canon Kk		
		JP-2008/250369	10-16-2008	Sorun Corp.		
		JP-2008-103936	05-01-2008	Toshiba Corp		
		JP-2008-250931	10-16-2008	Toshiba Corp		
		RU-2124814	01-10-1999	A.A. Moldovjan		
		WO-00/36786-A1	06-22-2000	Philips Electronics Na		
		WO-00/49766 A1	08-24-2000	Sonera Smarttrust Oy		
		WO-00/76118-A1	12-14-2000	Gen Instrument Corp		
		WO-00/79367-A1	12-28-2000	Brodia Group		
		WO-01/22201-A1	03-29-2001	Ethentica Inc		
		WO-01/22319-A1	03-29-2001	Ethentica Inc		
		WO-01/22322-A2	03-29-2001	Ethentica Inc		
		WO-01/22650-A2	03-29-2001	Ethentica Inc		
		WO-01/22651-A2	03-29-2001	Ethentica Inc		
		WO-02/062032	08-08-2002	The Charles Stark Draper Laboratory, Inc.		
		WO-02/21283-A1	03-14-2002	Sanctuary Systems Pty Ltd.		
		WO-02/21761-A2	03-14-2002	Widevine Technologies Inc		
		WO-03/036538	05-01-2003	Yasukura Yutaka		
		WO-04/111791-A2	12-23-2004	Security First Corp.		
		WO-06/047694-A1	05-04-2006	Orsini Rick L 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.

T^1 – Applicant is to place a check mark here if English language Translation is attached.

442734_1

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 16 of 23	Attorney Docket Number	104093-0002-118

FOREIGN PATENT PUBLICATIONS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[1]
		WO-08/054406-A2	05-08-2008	Orsini Rick L et al.		
		WO-08/070167-A1	06-12-2008	Martin Don et al.		
		WO-08/127309-A2	10-23-2008	Bellare Mihir et al.		
		WO-08/142440-A1	11-27-2008	Surf-Control On-Demand Limited		
		WO-09/035674-A1	03-19-2009	Security First Corp.		
		WO-09/089015-A1	07-16-2009	Security First Corp.		
		WO-09/105280-A2	08-27-2009	Security First Corp.		
		WO-2001/054370	07-26-2001	The University of Manitoba		
		WO-2004/001561-A2	12-31-2003	Armoursoft Ltd		
		WO-2007/078846	07-12-2007	United Video Properties Inc.		
		WO-2010/057181-A2	05-20-2010	Unisys Corp		
		WO-2010/135412-A2	11-25-2010	Security First Corp.		
		WO-2011/068738-A2	06-09-2011	Orsini Rick L et al.		
		WO-2011/123692-A2	10-06-2011	Orsini et al.		
		WO-2011/123699-A2	10-06-2011	Orsini et al.		
		WO-98/47091-A1	10-22-1998	Transactor Networks Inc		
		WO-99/19845-A1	04-22-1999	At & T Corp		
		WO-99/46720-A1	09-16-1999	Cha Tech Serv Inc		
		WO-99/65207-A1	12-16-1999	Microsoft Corp		

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.	T[1]
		Barlas, "RSA's Security Showcase", Line56.com - The E-Business Executive Daily, 15 April 2003.	
		Brainard, "A New Two-Server Approach for Authentication with Short Secrets" RSA Laboratories, Bedford, MA (13 pages)	
		Cachin, "On-Line secret Sharing," Cryptography and Coding. IMA Conference, Proceedings, December 18, 1995, pages 190-198, XP002137681.	

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.

T[1] – Applicant is to place a check mark here if English language Translation is attached.

442734_1

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 17 of 23	Attorney Docket Number	104093-0002-118

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.	T[1]
		Chan et. al., "Distributed Server Networks for Secure Multicast", GLOBCOM'01: IEEE Global Telecommunications Conference (IEEE, Piscataway, NJ) 3:1974-1978 (2001).	
		Chan et. al., "Distributed Servers Approach for Large-Scale Multicast", IEEE Journal on Selected Areas in Communications (IEEE, Piscataway, NJ) October 2002, 20(8):1500-1510.	
		Crescenzo et al., "Non-Interactive and Non-Malleable Commitment," Proceedings of the 30th Annual ACM Symposium on Theory of Computing. Dallas, TX, May 23-26, 1998, [Proceedings of the 30th Annual ACM Symposium on Theory of Computing], New York, NY: ACM, US, PAGES 141-150; XP000970902; ISBN: 978-0-89791-962-3.	
		Damgard et. al., "Non-interactive and Reusable Non-malleable Commitment Schemes," ACM STOC '03; pgs. 427-428; June 9-11, 2003.	
		Decru Unveils Security Appliances for Storage Networks; Decru DataFort (TM) Security Alliances Protect SAN and NAS Environments with Wire-Speed Encryption and Transparent Deployment", PR Newswire (PR Newswire Association. Inc.), 14 October 2002.	
		Dierks, "The Transport Layer Security Protocol," RFC 4346m Version 1.1, April 2006, 86 pages	
		Doyle, "RSA Splits Data to Stop Hackers", vnunet.com, 16 April 2003.	
		Easter et al. "S/390 parallel enterprise server CMOS cryptographic coprocessor," IBM Journal of Research and Development, International Business Machines Corporation, New York, NY, US, vol. 43, no. 5, 1 January 1999, pgs. 761-776, XP002335589, ISSN: 0018-8646.	
		Fisher, "RSA Looks to Lock Down Personal Data", eWeek - Enterprise News & Reviews, 14 April 2003.	
		Ganger et al., "PASIS: A Distributed Framework for Perpetually Available and Secure Information Systems, Final Technical rept. June 1999-Dec 2003," (7-1-2005),pgs 1-302, XP55011444, Retrieved from the Internet: URL:http://www.dtic/mil/cgi-bin/GetTRDoc?AD=ADA436245&Location-U2&doc=GetTRDoc.pdf (retrieved 0n 2011-11-07]	
		Ganger et al., "Survivable storage systems," DARPA Information Survivability Conference & Exposition II, 2001. DISC EX '01. Proc. 12-14 June 2001, Piscataway, NJ, USA, IEEE, vo. 2, pgs. 184-195, XP010548746	
		Garay et. al., "Secure distributed storage and retrieval," Theoretical Comput. Sci., 243(1-2):363-389, July 2000	

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.

T[1] – Applicant is to place a check mark here if English language Translation is attached.

442734_1

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 18 of 23	Attorney Docket Number	104093-0002-118

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.	T[1]
		Gibson, "Opinion", eWeek - Enterprise News & Reviews, 14 April 2003.	
		Grant et. al., "Secret Sharing and Splitting", (White Paper) Notre Dame, Indiana, 16 December 2002.	
		Hand et al., Spread Spectrum Storage with Mnemosyne, 2003, Retrieved from the Internet <URL: springerlink.com/content/9vdp5b40ep2pjvba/>, pp 1-5 as printed	
		Haniotakis et al., "Security Enhancement Through Multiple Path Transmission in Ad Hoc Networks," IEEE Intl. Conference on Communications, 20-24 June 2004, 5 pgs.	
		Horne et al., Escrow services and incentives in Peer-to-Peer Networks, 2001, Retrieved from the Internet URL:dl.acm.org.citation.cfm?id=501168, pp 1-10 as printed	
		Hunter, "Simplifying PKI Usage Through a Client-Server Architecture and Dynamic Propagation of Certificate Paths and Repository Addresses", Proceedings 13th International Workshop on Database and Expert Systems Applications (IEEE Computer Soc., Los Alamitos, CA), 2-6 September 2002, pg. 505-510.	
		Johnson, "MLS-Net and Secure Parser: A New Method for Securing and Segregating Network Data" [Online] 8-July 2007"XP002582437 5th International Symposium on Risk Management and Informatic: WMS12007, Orlando Florida, USA	
		Kent, "Security Architecture for the Internet Protocol," RFC 2401, November 1998, 67 pages.	
		Klensin, J., "Simple Mail Transfer Protocol; rfs5321.txt," Simple Mail Transfer Protocol; RFC5321.TXT, Internet Engineering Task Force, IETF; Standard, Internet Society (ISOC) 4, Rue Des Falaises CH- 1205 Geneva, Switzerland, XP015060297 (October 2008)	
		Krawczyk, "Distributed Fingerprints and Secure Information Dispersal," 12th ACM, Symposium on Principles on Distributed Computing, Ithaca, NY, ACM 0-89191-613-1/93/0008/0207, 1993, pages 207-218	
		Krawczyk, "Secret sharing made Short," IBM T.J. Watson Research Center, [Online] 1998, retrieved from the Internet: URL:http://www.cs.cornell.edu/courses/cs754/2001fa/secretshort.pdf> [retrieved on 11-24-2008]	
		Kroç, Erol, "Access Control in Peer-to-Peer Storage Systems," 1 Oct 2006, XP55036196, Retrieved from the Internet: URL:ftp://ftp.tik.ee.ethz.ch/pub/studfents/2006-So/MA-2006-10.pdf [retrieved on 2012-08-23] page. 61-62	
		Kubiatowicz et al., OceanStore: an architecture for global-scale persistent storage, Retrieved from the Internet <URL: dl.acm.org/citation.cfm?id=356989.357007>, pp 1-12 as printed	

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.

T[1] – Applicant is to place a check mark here if English language Translation is attached.

442734_1

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 19 of 23	Attorney Docket Number	104093-0002-118

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.	T[1]
		Lancope Announces Stealthwatch 3.0 for Enhanced Enterprise-Wide Security and Improved Manageability", Business Wire (Newswire Association, Inc.), 14 April 2003.	
		Loutrel et. al. "An EAP-BT Smartcard for Authentication in the Next Generation of Wireless Communications", Conference on Network Control and Engineering for QoS Security and Mobility (Kluwer Academic Publishers, Norwell, MA) October 23-25, 2002, pgs. 1-4-114.	
		Mayer et. al., "Generalized Secret Sharing and Group-Key Distribution Using Short Keys," Compression and Complexity of Sequences 1997, Proceedings Salerno, Italy, June 11-13, 1997, Los Alamitos, CA, USA, IEEE Comput,. SOC, US, June 11, 1997, pages 30-44, XP010274905, ISBN: 978-0-8186-8132-5.	
		McNamara, "Strong Crypto Freeware" (Secret Sharer Version 1.0) July 11, 1995.	
		Menezes, "Handbook of Applied Cryptography, Ch. 7 Block Ciphers" 1997, pgs. 223-271 CRC Press LLC, XP001525007	
		Mitchell, "Making Serial Number Based Authentication Robust Against Loss of State", Operating Systems Review, 34:3, pgs. 1-5, November 24, 1999	
		Myers et. al., "A secure, publisher-centric Web caching infrastructure" In: INFOCOM 2001 Proceedings. IEEE Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies [online], vol. 3 p. 1235-1243. Published 04/22/2001. [retrieved on 7-8-2008]. Retrieved from the internet <URL: http://people.ischool.berkeley.edu/-chuang/pubs/gemini.pdf>	
		Nightingale, The New Secret-Splitting Technology from RSA... NGBK DS 0403 http://developer.rsasecurity.com/labs/nightingale/developer.rsasecurity.com/labs/nightingale/files/nightingale-brochure.pdf	
		Pattam, "Enhancing Security in 802.11 and 802.1X Networks with Intrusion Detection," Jan. 20, 2006, Univ. of New Orleans Theses and Dissertations, Paper 1034, 111 pages	
		Rabin, "Efficient Dispersal of Information for Security, Load Balancing and Fault Tolerance," Journal of the Association for Computing Machinery, Vol. 36, No. 2, pp. 335-348, April 1989	
		Rivest, "All-Or-Nothing Encryption and The Package Transform," Proc. Of the 4th Intl. Workshop on Fast Software Encryption (1997), 9 pgs.	
		RSA SureFile: Software Powered by PKZIP...BSSF DS 0103 Authorized Reseller: Technical Specifications Platforms Microsoft ® Windows ® 98 Second Edition ME NT 4.0 Workstation SP6A 2000 Professional SP2... www.rsasecurity.com/products/bsafe/datasheets/BSSF_DS_103.pdf	

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.

T[1] – Applicant is to place a check mark here if English language Translation is attached.

442734_1

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 20 of 23	Attorney Docket Number	104093-0002-118

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.	T^1
		Savage, "RSA Unveils Nightingale Technology", CRN.com, 14 April 2003.	
		Sengar et al., "MTPSec: Customizable Secure MTP3 Tunnels in the SS7 Network," Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium, 8 pages (2005)	
		Shamir, "How to Share a Secret," Communications of the Association for Computing Machinery, ACM, New York, NY, US, Vol. 22, No. 11, November 1, 1979, pages 1-4, XP002241399; ISSN: 0001-0782.	
		Shin et. al., "Design a Working Model of Secure Data Transfer Using a Data Mart", Proceedings of the ISCA 14th International Conference Computer Applications in Industry and Engineering (ISCA, Cary, NC) 27-29 November 2001, pg. 66-69.	
		Tactilesense TM White Paper - A Breakthrough in Fingerprint Authentication", Ethentica, Inc. by Security First Corporation, January, 2003.	
		Trustengine TM White Paper - Enthentication Services, Secure Storage and Authentication Solutions", Ethentica, Inc. by Security First Corporation, June 2002.	
		Vijayan, "RSA unveils Management, Encryption Products", Computerworld, 15 April 2003.	
		Waldman et al., "Publius: A robust, tamper-evident, censorship-resistant web publishing sytem," Proceedings of the 9th USENIX Security Symposum, August 2000	
		Waters, "RSA Integrates ID Management; discloses 'Nightingale' ", ADTmag.com, 21 April 2003.	
		Copy of Office Actions and Replies issued for U.S. Patent Application No. 13/468,383 (104093-0002-107)	
		Copy of Office Actions and Replies issued for U.S. Patent Application No. 13/468,428 (104093-0002-108)	
		Copy of Office Actions and Replies issued for U.S. Patent Application No. 13/468,450 (104093-0002-109)	
		Copy of Office Actions and Replies issued for U.S. Patent Application No. 13/468,523 (104093-0002-110)	
		Copy of Office Actions and Replies issued for U.S. Patent Application No. 13/468,605 (104093-0002-111)	
		Copy of Office Actions and Replies issued for U.S. Patent Application No. 13/468,562 (104093-0002-112)	
		Copy of Office Actions and Replies issued for U.S. Patent Application No. 13/468,584 (104093-0002-113)	

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.

T^1 – Applicant is to place a check mark here if English language Translation is attached.

442734_1

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 21 of 23	Attorney Docket Number	104093-0002-118

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.	T[1]
		Xu, "Locality Driven Key Management Architecture for Mobile Ad-hoc Networks," 2004 IEEE International Conference on Mobile Ad-hoc and Sensor Systems," pgs. 436-446.	
		Nacht, "The Spectrum of Modern Firewalls," Computers & Security, 16 (1997), pp. 54-56.	
		Shaw et al (eds.), "Handbook on Electronic Commerce, Conway, Chapter 31, Springer-Verlag, Berlin Heidelbert, pp. 649-690 (2000)	
		Mondal, "Mobile IP," Chapter 7, Fluwer Academic/Plenum Publishers, New York, pp. 173-202 (2003)	
		Rosen, "BGP/MPLS VPNs," Network Working Group, RFC 2547, March 1999, 25 pages.	
		Tewari et al.; "High Availability in Clustered Multimedia Servers; 1996; Retrieved from the Internet <URL:ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=492215>; pp. 1-10 as printed.	
		Wells; The OceanStore Archive: Goals, Structures, and Self-Repair; 2001; Retrieved from the Internet <URL: oceanstore.org/publications/papers/pdf/>; pp. 1-20 as printed.	
		Wylie et al.; Selecting the right data distribution scheme for a survivable storage system; 2001; Retrieved from the Internet <URL: repository.cmu./edu/compsci/2164/?utm_source=repository.cmu.edu%2Fcompsci%2F2164&utm_medium=PDF&utm_campaign=PDFCoverPages.; pp. 1-25 as printed.	
		Buckhard et al., "MDP Disk Array Storage System Reliability; 1992; Retrieved from the Internet <URL:ieexplore.ieee.org/xpls/abs_all.jsp?arnumber=627346&tag=1>; pp. 1-26 as printed.	
		Kim et al., "Secure Group Key Management for Storage Area Networks," IEEE Communications Magazine, August 2003, pp. 92-99.	
		Bendix, "RAID and Informix Databases," White Paper, Advanced Technology Group, June 1995; Retrieved from the Internet <URL: informix.com.ua/articles/raid/raid.htm>; retrieved from the internet on December 3, 2014, pp. 1-15 as printed.	
		D'Arco et al.: "Fault Tolerant and distributed Broadcast Encryption"; 2003: Retrieved from the Internet<URL:link.springer.com/chapter/10.1007/3-540-36563-x18#page-1>; pp. 1-18 as printed.	
		Schwartz, Richard; "Using field encryption in applications"; 2001; Retrieved from the Internet<URL:ibm.com/developerworks/lotus/library/IS-filed_encryption/>; pp. 1-16 as printed.	

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.

T[1] – Applicant is to place a check mark here if English language Translation is attached.

442734_1

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 22 of 23	Attorney Docket Number	104093-0002-118

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.	T[1]
		Goodson et al., "Efficient consistency for erasure-coded data via versioning servers," Retrieved from the Internet<URL:oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA461126> pgs. 1-25, March 2003.	
		Long et al., "Swift/RAID: A Distributed RAID System," Retrieved from the Internet<URL:http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.53.7183>pgs. 1-20 (1994)	
		Guo et al. "Design and implementation of the KioskNet System", Information and Communication Technologies and Development, 2007. ICTD 2007. International Conference on, 31 December 2007 (2007-12-31) pages 264-281 [retrieved on 2015-11-26]	
		CHEN, et al., "RAID: High-Performance, Reliable Secondary Storage" Retrieved from the internet, <URL:https://web.archive.org/web/20040721062927/http://meseec.ce.rit.edu/eecc722-fall2002/papers/io/3/chen94raid.pdf> 26:145-184 (1994)	
		PLANK, JAMES A., "A Tutorial on Reed-Solomon Coding for Fault-Tolerance in RAID-like Systems," Retrieved from the Internet <URL: citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.160.4742&rep=rep1&type=pdf>; pp. 1-18 as printed (1997).	
		Office Actions and Replies for U.S. Application No. 11/258,839.	
		Office Actions and Replies for U.S. Application No. 12/148,365.	
		Office Actions and Replies for U.S. Application No. 12/272,012.	
		Office Actions and Replies for U.S. Application No. 12/336,558.	
		Restriction Requirement issued September 29, 2011 for U.S. Application No. 12/336,559.	
		Office Action issued November 28, 2011 for U.S. Application No. 12/336,562.	
		Office Action issued September 27, 2011 for U.S. Application No. 12/336,568.	
		Office Action issued November 8, 2011 for U.S. Application No. 12/342,379.	
		Office Action issued September 14, 2011 for U.S. Application No. 12/342,500.	
		Office Action issued October 7, 2011 for U.S. Application No. 12/342,523.	
		Office Actions issued October 6, 2011 for U.S. Application No. 12/342,547.	
		Office Action issued November 10, 2011 for U.S. Application No. 12/342,575.	
		Office Actions and Replies for U.S. Application No. 12/342,610.	
		Office Action issued November 23, 2011 for U.S. Application No. 12/342,636.	

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.

T[1] – Applicant is to place a check mark here if English language Translation is attached.

442734_1

PTO/SB/08 Equivalent

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	*Complete if Known*	
	Application Number	Not Yet Assigned
	Filing Date	Herewith
	First Named Inventor	Mark S. O'Hare
	Art Unit	Not Yet Assigned
	Examiner Name	Not Yet Assigned
Sheet 23 of 23	Attorney Docket Number	104093-0002-118

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.	T[1]
		Office Actions and Replies for U.S. Application No. 12/346,578.	
		Office Actions and Replies for U.S. Application No. 13/024,791.	
		Office Action issued June 11, 2012 for U.S. Application No. 13/371,361.	
		Office Actions and Replies for U.S. Application No. 13/371,363.	
		Office Actions and Replies for U.S. Application No. 13/371,364.	

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.

T[1] – Applicant is to place a check mark here if English language Translation is attached.

442734_1

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82A (07-13)
Approved for use through 01/31/2018. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	Not Yet Assigned
Filing Date	Herewith
First Named Inventor	Mark S. O'Hare
Title	SECURE DATA PARSER METHOD AND SYSTEM
Art Unit	Not Yet Assigned
Examiner Name	Not Yet Assigned
Attorney Docket Number	104093-0002-118

SIGNATURE of Applicant or Patent Practitioner

Signature	/Maxim Rapoport/	Date (Optional)	May 11, 2018
Name	Maxim Rapoport	Registration Number	67,675
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)			

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☑ *Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82B (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☑ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: 15314

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):

☐ 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	James Varner		
Title	President & CEO, Security First Corp.		

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.

Docket No.: 104093-0002-118

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	:	Security First Corp.	
Inventors	:	Mark S. O'Hare et al.	
Application No.	:	Not Yet Assigned	Confirmation No.: Not Yet Assigned
Filed	:	Herewith	
For	:	SECURE DATA PARSER METHOD AND SYSTEM	
Group Art Unit	:	Not Yet Assigned	
Examiner	:	Not Yet Assigned	

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

INFORMATION DISCLOSURE STATEMENT

Sir:

Pursuant to 37 C.F.R. §§ 1.56, 1.97, and 1.98, applicant wishes to call the attention of the Examiner to the documents listed on the accompanying Form PTO/SB/08. It is respectfully requested that these documents be (1) fully considered by the United States Patent and Trademark Office during examination of this application and (2) printed on any patent which may issue on this application. Applicant requests that a copy of Form PTO/SB/08, as considered and initialed by the Examiner, be returned with the next communication.

In accordance with 37 C.F.R. § 1.98(a)(2)(ii), no copies of the listed U.S. patent documents are being submitted.

The documents listed on the accompanying Form PTO/SB/08 are of record in parent U.S. Patent Application No. 13/915,081, filed June 11, 2013, which is relied on for an earlier effective

filing date under 35 U.S.C. § 120. In accordance with 37 C.F.R. § 1.98(d), no copies of these documents are being submitted.

Applicant reserves the right to establish the patentability of the claimed invention over any of the information provided herewith, and/or to prove that this information may not be prior art, and/or to prove that this information may not be enabling for the teachings purportedly offered.

This Information Disclosure Statement is being filed within three months of the application filing date. Therefore, in accordance with 37 C.F.R. § 1.97(b)(1), submission of this Statement requires no fee.

Consideration of the foregoing in relation to this patent application is respectfully requested.

Respectfully submitted,

Date: May 11, 2018

/Maxim Rapoport/
Maxim Rapoport
Registration No. 67,675
HALEY GUILIANO LLP
Customer No. 15314
75 Broad Street
Suite 1000
New York, New York 10004
(646) 973-2511
Attorney for Applicant

SECURE DATA PARSER METHOD AND SYSTEM

Cross-reference to Related Applications

[0001] This application is a continuation of U.S. Patent Application No. 13/915,081, filed June 11, 2013, which is a divisional of U.S. Patent Application No. 13/468,383, filed on May 10, 2012, now U.S. Patent No. 9,338,140, which is a continuation of U.S. Patent Application No. 11/258,839, filed on October 25, 2005, now U.S. Patent No. 8,266,438, which claims priority benefit from U.S. provisional application No. 60/622,146, filed on October 25, 2004, and U.S. provisional application No. 60/718,185, filed September 16, 2005. The aforementioned, earlier-filed applications are hereby incorporated by reference herein in their entireties.

Field of the Invention

[0002] The present invention relates in general to a system for securing data from unauthorized access or use.

Background of the Invention

[0003] In today's society, individuals and businesses conduct an ever-increasing amount of activities on and over computer systems. These computer systems, including proprietary and non-proprietary computer networks, are often storing, archiving, and transmitting all types of sensitive information. Thus, an ever-increasing need exists for ensuring data stored and transmitted over these systems cannot be read or otherwise compromised.

[0004] One common solution for securing computer systems is to provide login and password functionality. However, password management has proven to be

quite costly with a large percentage of help desk calls relating to password issues. Moreover, passwords provide little security in that they are generally stored in a file susceptible to inappropriate access, through, for example, brute-force attacks.

[0005] Another solution for securing computer systems is to provide cryptographic infrastructures. Cryptography, in general, refers to protecting data by transforming, or encrypting, it into an unreadable format. Only those who possess the key(s) to the encryption can decrypt the data into a useable format. Cryptography is used to identify users, e.g., authentication, to allow access privileges, e.g., authorization, to create digital certificates and signatures, and the like. One popular cryptography system is a public key system that uses two keys, a public key known to everyone and a private key known only to the individual or business owner thereof. Generally, the data encrypted with one key is decrypted with the other and neither key is recreatable from the other.

[0006] Unfortunately, even the foregoing typical public-key cryptographic systems are still highly reliant on the user for security. For example, cryptographic systems issue the private key to the user, for example, through the user's browser. Unsophisticated users then generally store the private key on a hard drive accessible to others through an open computer system, such as, for example, the Internet. On the other hand, users may choose poor names for files containing their private key, such as, for example, "key." The result of the foregoing and other acts is to allow the key or keys to be susceptible to compromise.

[0007] In addition to the foregoing compromises, a user may save his or her private key on a computer system configured with an archiving or backup system, potentially resulting in copies of the private key traveling through multiple computer storage devices or other systems. This security breach is often referred to as "key migration." Similar to key migration, many applications provide access to a user's private key through, at most, simple login and password access. As mentioned in the foregoing, login and password access often does not provide adequate security.

[0008] One solution for increasing the security of the foregoing cryptographic systems is to include biometrics as part of the authentication or authorization. Biometrics generally include measurable physical characteristics, such as, for

example, finger prints or speech that can be checked by an automated system, such as, for example, pattern matching or recognition of finger print patterns or speech patterns. In such systems, a user's biometric and/or keys may be stored on mobile computing devices, such as, for example, a smartcard, laptop, personal digital assistant, or mobile phone, thereby allowing the biometric or keys to be usable in a mobile environment.

[0009] The foregoing mobile biometric cryptographic system still suffers from a variety of drawbacks. For example, the mobile user may lose or break the smartcard or portable computing device, thereby having his or her access to potentially important data entirely cut-off. Alternatively, a malicious person may steal the mobile user's smartcard or portable computing device and use it to effectively steal the mobile user's digital credentials. On the other hand, the portable-computing device may be connected to an open system, such as the Internet, and, like passwords, the file where the biometric is stored may be susceptible to compromise through user inattentiveness to security or malicious intruders.

Summary of the Invention

[0010] Based on the foregoing, a need exists to provide a cryptographic system whose security is user-independent while still supporting mobile users.

[0011] Accordingly, one aspect of the present invention is to provide a method for securing virtually any type of data from unauthorized access or use. The method comprises one or more steps of parsing, splitting and/or separating the data to be secured into two or more parts or portions. The method also comprises encrypting the data to be secured. Encryption of the data may be performed prior to or after the first parsing, splitting and/or separating of the data. In addition, the encrypting step may be repeated for one or more portions of the data. Similarly, the parsing, splitting and/or separating steps may be repeated for one or more portions of the data. The method also optionally comprises storing the parsed, split and/or separated data that has been encrypted in one location or in multiple locations. This method also optionally comprises reconstituting or re-assembling the secured data into its original form for authorized access or use. This method

may be incorporated into the operations of any computer, server, engine or the like, that is capable of executing the desired steps of the method.

[0012] Another aspect of the present invention provides a system for securing virtually any type of data from unauthorized access or use. This system comprises a data splitting module, a cryptographic handling module, and, optionally, a data assembly module. The system may, in one embodiment, further comprise one or more data storage facilities where secure data may be stored.

[0013] Accordingly, one aspect of the invention is to provide a secure server, or trust engine, having server-centric keys, or in other words, storing cryptographic keys and user authentication data on a server. According to this embodiment, a user accesses the trust engine in order to perform authentication and cryptographic functions, such as, but not limited to, for example, authentication, authorization, digital signing and generation, storage, and retrieval of certificates, encryption, notary-like and power-of-attorney-like actions, and the like.

[0014] Another aspect of the invention is to provide a reliable, or trusted, authentication process. Moreover, subsequent to a trustworthy positive authentication, a wide number of differing actions may be taken, from providing cryptographic technology, to system or device authorization and access, to permitting use or control of one or a wide number of electronic devices.

[0015] Another aspect of the invention is to provide cryptographic keys and authentication data in an environment where they are not lost, stolen, or compromised, thereby advantageously avoiding a need to continually reissue and manage new keys and authentication data. According to another aspect of the invention, the trust engine allows a user to use one key pair for multiple activities, vendors, and/or authentication requests. According to yet another aspect of the invention, the trust engine performs at least one step of cryptographic processing, such as, but not limited to, encrypting, authenticating, or signing, on the server side, thereby allowing clients or users to possess only minimal computing resources.

[0016] According to yet another aspect of the invention, the trust engine includes one or multiple depositories for storing portions of each cryptographic key and authentication data. The portions are created through a data splitting process that

prohibits reconstruction without a predetermined portion from more than one location in one depository or from multiple depositories. According to another embodiment, the multiple depositories may be geographically remote such that a rogue employee or otherwise compromised system at one depository will not provide access to a user's key or authentication data.

[0017] According to yet another embodiment, the authentication process advantageously allows the trust engine to process multiple authentication activities in parallel. According to yet another embodiment, the trust engine may advantageously track failed access attempts and thereby limit the number of times malicious intruders may attempt to subvert the system.

[0018] According to yet another embodiment, the trust engine may include multiple instantiations where each trust engine may predict and share processing loads with the others. According to yet another embodiment, the trust engine may include a redundancy module for polling a plurality of authentication results to ensure that more than one system authenticates the user.

[0019] Therefore, one aspect of the invention includes a secure cryptographic system, which may be remotely accessible, for storing data of any type, including, but not limited to, a plurality of private cryptographic keys to be associated with a plurality of users. The cryptographic system associates each of the plurality of users with one or more different keys from the plurality of private cryptographic keys and performs cryptographic functions for each user using the associated one or more different keys without releasing the plurality of private cryptographic keys to the users. The cryptographic system comprises a depository system having at least one server which stores the data to be secured, such as a plurality of private cryptographic keys and a plurality of enrollment authentication data. Each enrollment authentication data identifies one of multiple users and each of the multiple users is associated with one or more different keys from the plurality of private cryptographic keys. The cryptographic system also may comprise an authentication engine which compares authentication data received by one of the multiple users to enrollment authentication data corresponding to the one of multiple users and received from the depository system, thereby producing an authentication result. The cryptographic system also may comprise a

cryptographic engine which, when the authentication result indicates proper identification of the one of the multiple users, performs cryptographic functions on behalf of the one of the multiple users using the associated one or more different keys received from the depository system. The cryptographic system also may comprise a transaction engine connected to route data from the multiple users to the depository server system, the authentication engine, and the cryptographic engine.

[0020] Another aspect of the invention includes a secure cryptographic system that is optionally remotely accessible. The cryptographic system comprises a depository system having at least one server which stores at least one private key and any other data, such as, but not limited to, a plurality of enrollment authentication data, wherein each enrollment authentication data identifies one of possibly multiple users. The cryptographic system may also optionally comprise an authentication engine which compares authentication data received by users to enrollment authentication data corresponding to the user and received from the depository system, thereby producing an authentication result. The cryptographic system also comprises a cryptographic engine which, when the authentication result indicates proper identification of the user, performs cryptographic functions on behalf of the user using at least said private key, which may be received from the depository system. The cryptographic system may also optionally comprise a transaction engine connected to route data from the users to other engines or systems such as, but not limited to, the depository server system, the authentication engine, and the cryptographic engine.

[0021] Another aspect of the invention includes a method of facilitating cryptographic functions. The method comprises associating a user from multiple users with one or more keys from a plurality of private cryptographic keys stored on a secure location, such as a secure server. The method also comprises receiving authentication data from the user, and comparing the authentication data to authentication data corresponding to the user, thereby verifying the identity of the user. The method also comprises utilizing the one or more keys to perform cryptographic functions without releasing the one or more keys to the user.

[0022] Another aspect of the invention includes an authentication system for uniquely identifying a user through secure storage of the user's enrollment authentication data. The authentication system comprises one or more data storage facilities, wherein each data storage facility includes a computer accessible storage medium which stores at least one of portions of enrollment authentication data. The authentication system also comprises an authentication engine which communicates with the data storage facility or facilities. The authentication engine comprises a data splitting module which operates on the enrollment authentication data to create portions, a data assembling module which processes the portions from at least one of the data storage facilities to assemble the enrollment authentication data, and a data comparator module which receives current authentication data from a user and compares the current authentication data with the assembled enrollment authentication data to determine whether the user has been uniquely identified.

[0023] Another aspect of the invention includes a cryptographic system. The cryptographic system comprises one or more data storage facilities, wherein each data storage facility includes a computer accessible storage medium which stores at least one portion of one ore more cryptographic keys. The cryptographic system also comprises a cryptographic engine which communicates with the data storage facilities. The cryptographic engine also comprises a data splitting module which operate on the cryptographic keys to create portions, a data assembling module which processes the portions from at least one of the data storage facilities to assemble the cryptographic keys, and a cryptographic handling module which receives the assembled cryptographic keys and performs cryptographic functions therewith.

[0024] Another aspect of the invention includes a method of storing any type of data, including, but not limited to, authentication data in geographically remote secure data storage facilities thereby protecting the data against composition of any individual data storage facility. The method comprises receiving data at a trust engine, combining at the trust engine the data with a first substantially random value to form a first combined value, and combining the data with a second substantially random value to form a second combined value. The method

comprises creating a first pairing of the first substantially random value with the second combined value, creating a second pairing of the first substantially random value with the second substantially random value, and storing the first pairing in a first secure data storage facility. The method comprises storing the second pairing in a second secure data storage facility remote from the first secure data storage facility.

[0025] Another aspect of the invention includes a method of storing any type of data, including, but not limited to, authentication data comprising receiving data, combining the data with a first set of bits to form a second set of bits, and combining the data with a third set of bits to form a fourth set of bits. The method also comprises creating a first pairing of the first set of bits with the third set of bits. The method also comprises creating a second pairing of the first set of bits with the fourth set of bits, and storing one of the first and second pairings in a first computer accessible storage medium. The method also comprises storing the other of the first and second pairings in a second computer accessible storage medium.

[0026] Another aspect of the invention includes a method of storing cryptographic data in geographically remote secure data storage facilities thereby protecting the cryptographic data against comprise of any individual data storage facility. The method comprises receiving cryptographic data at a trust engine, combining at the trust engine the cryptographic data with a first substantially random value to form a first combined value, and combining the cryptographic data with a second substantially random value to form a second combined value. The method also comprises creating a first pairing of the first substantially random value with the second combined value, creating a second pairing of the first substantially random value with the second substantially random value, and storing the first pairing in a first secure data storage facility. The method also comprises storing the second pairing in a secure second data storage facility remote from the first secure data storage facility.

[0027] Another aspect of the invention includes a method of storing cryptographic data comprising receiving authentication data and combining the cryptographic data with a first set of bits to form a second set of bits. The method also comprises combining the cryptographic data with a third set of bits to form a

fourth set of bits, creating a first pairing of the first set of bits with the third set of bits, and creating a second pairing of the first set of bits with the fourth set of bits. The method also comprises storing one of the first and second pairings in a first computer accessible storage medium, and storing the other of the first and second pairings in a second computer accessible storage medium.

[0028] Another aspect of the invention includes a method of handling sensitive data of any type or form in a cryptographic system, wherein the sensitive data exists in a useable form only during actions by authorized users, employing the sensitive data. The method also comprises receiving in a software module, substantially randomized or encrypted sensitive data from a first computer accessible storage medium, and receiving in the software module, substantially randomized or encrypted data which may or may not be sensitive data, from one or more other computer accessible storage medium. The method also comprises processing the substantially randomized pre-encrypted sensitive data and the substantially randomized or encrypted data which may or may not be sensitive data, in the software module to assemble the sensitive data and employing the sensitive data in a software engine to perform an action. The action includes, but is not limited to, one of authenticating a user and performing a cryptographic function.

[0029] Another aspect of the invention includes a secure authentication system. The secure authentication system comprises a plurality of authentication engines. Each authentication engine receives enrollment authentication data designed to uniquely identify a user to a degree of certainty. Each authentication engine receives current authentication data to compare to the enrollment authentication data, and each authentication engine determines an authentication result. The secure authentication system also comprises a redundancy system which receives the authentication result of at least two of the authentication engines and determines whether the user has been uniquely identified.

[0030] Another aspect of the invention includes a secure data in motion system whereby data may be transmitted in different portions that are secured in accordance with the present invention such that any one portion becoming compromised shall not provide sufficient data to restore the original data. This

may be applied to any transmission of data, whether it be wired, wireless, or physical.

[0031] Another aspect of the invention includes integration of the secure data parser of the present invention into any suitable system where data is stored or communicated. For example, email system, RAID systems, video broadcasting systems, database systems, or any other suitable system may have the secure data parser integrated at any suitable level.

[0032] Another aspect of the invention includes using any suitable parsing and splitting algorithm to generate shares of data. Either random, pseudo-random, deterministic, or any combination thereof may be employed for parsing and splitting data.

Brief Description of the Drawings

[0033] The present invention is described in more detail below in connection with the attached drawings, which are meant to illustrate and not to limit the invention, and in which:

[0034] FIGURE 1 illustrates a block diagram of a cryptographic system, according to aspects of an embodiment of the invention;

[0035] FIGURE 2 illustrates a block diagram of the trust engine of FIGURE 1, according to aspects of an embodiment of the invention;

[0036] FIGURE 3 illustrates a block diagram of the transaction engine of FIGURE 2, according to aspects of an embodiment of the invention;

[0037] FIGURE 4 illustrates a block diagram of the depository of FIGURE 2, according to aspects of an embodiment of the invention;

[0038] FIGURE 5 illustrates a block diagram of the authentication engine of FIGURE 2, according to aspects of an embodiment of the invention;

[0039] FIGURE 6 illustrates a block diagram of the cryptographic engine of FIGURE 2, according to aspects of an embodiment of the invention;

[0040] FIGURE 7 illustrates a block diagram of a depository system, according to aspects of another embodiment of the invention;

[0041] FIGURE 8 illustrates a flow chart of a data splitting process according to aspects of an embodiment of the invention;

[0042] FIGURE 9, Panel A illustrates a data flow of an enrollment process according to aspects of an embodiment of the invention;

[0043] FIGURE 9, Panel B illustrates a flow chart of an interoperability process according to aspects of an embodiment of the invention;

[0044] FIGURE 10 illustrates a data flow of an authentication process according to aspects of an embodiment of the invention;

[0045] FIGURE 11 illustrates a data flow of a signing process according to aspects of an embodiment of the invention;

[0046] FIGURE 12 illustrates a data flow and an encryption/decryption process according to aspects and yet another embodiment of the invention;

[0047] FIGURE 13 illustrates a simplified block diagram of a trust engine system according to aspects of another embodiment of the invention;

[0048] FIGURE 14 illustrates a simplified block diagram of a trust engine system according to aspects of another embodiment of the invention;

[0049] FIGURE 15 illustrates a block diagram of the redundancy module of FIGURE 14, according to aspects of an embodiment of the invention;

[0050] FIGURE 16 illustrates a process for evaluating authentications according to one aspect of the invention;

[0051] FIGURE 17 illustrates a process for assigning a value to an authentication according to one aspect as shown in FIGURE 16 of the invention;

[0052] FIGURE 18 illustrates a process for performing trust arbitrage in an aspect of the invention as shown in FIGURE 17; and

[0053] FIGURE 19 illustrates a sample transaction between a user and a vendor according to aspects of an embodiment of the invention where an initial web based contact leads to a sales contract signed by both parties.

[0054] FIGURE 20 illustrates a sample user system with a cryptographic service provider module which provides security functions to a user system.

[0055] FIGURE 21 illustrates a process for parsing, splitting and/or separating data with encryption and storage of the encryption master key with the data.

[0056] FIGURE 22 illustrates a process for parsing, splitting and/or separating data with encryption and storing the encryption master key separately from the data.

[0057] FIGURE 23 illustrates the intermediary key process for parsing, splitting and/or separating data with encryption and storage of the encryption master key with the data.

[0058] FIGURE 24 illustrates the intermediary key process for parsing, splitting and/or separating data with encryption and storing the encryption master key separately from the data.

[0059] FIGURE 25 illustrates utilization of the cryptographic methods and systems of the present invention with a small working group.

[0060] FIGURE 26 is a block diagram of an illustrative physical token security system employing the secure data parser in accordance with one embodiment of the present invention.

[0061] FIGURE 27 is a block diagram of an illustrative arrangement in which the secure data parser is integrated into a system in accordance with one embodiment of the present invention.

[0062] FIGURE 28 is a block diagram of an illustrative data in motion system in accordance with one embodiment of the present invention.

[0063] FIGURE 29 is a block diagram of another illustrative data in motion system in accordance with one embodiment of the present invention.

[0064] FIGURE 30-32 are block diagrams of an illustrative system having the secure data parser integrated in accordance with one embodiment of the present invention.

[0065] FIGURE 33 is a process flow diagram of an illustrative process for parsing and splitting data in accordance with one embodiment of the present invention.

[0066] FIGURE 34 is a process flow diagram of an illustrative process for restoring portions of data into original data in accordance with one embodiment of the present invention.

[0067] FIGURE 35 is a process flow diagram of an illustrative process for splitting data at the bit level in accordance with one embodiment of the present invention.

[0068] FIGURE 36 depicts an exemplary bit-splitting technique in accordance with one embodiment of the present invention.

[0069] FIGURE 37 depicts a data flow for distributing the output of a bit-splitting process into one or more shares in accordance with one embodiment of the present invention.

[0070] FIGURE 38 depicts an exemplary bit scatter technique for the distribution of data into shares in accordance with one embodiment of the present invention.

[0071] FIGURE 39 depicts an exemplary technique for restoring data that was distributed to a share using the bit scatter technique.

[0072] FIGURE 40 illustrates example of such an allocation for a 2 of 4 key split with a ratio of 75% in accordance with one embodiment of the present invention.

[0073] FIGURE 41 is an illustrative overview process for using the secure data parser of the present invention.

[0074] FIGURE 42 depicts an exemplary secure parser system in accordance with one embodiment of the present invention.

[0075] FIGURE 43 depicts an exemplary integration of a secure parser into a system utilizing an Application Programming Interface (API).

[0076] FIGURE 44 depicts an example configuration of a share fault tolerance system in accordance with one embodiment of the present invention.

[0077] FIGURE 45 depicts an example configuration of a share fault tolerance system with a mandatory share in accordance with one embodiment of the present invention.

[0078] FIGURE 46 depicts an illustrative process for parsing and distributing data into shares in accordance with one embodiment of the present invention.

[0079] FIGURE 47 depicts an illustrative process for recovering data from shares in accordance with one embodiment of the present invention.

[0080] FIGURE 48 Panels A and B depict various parameters used in parsing operations in accordance with one embodiment of the present invention.

[0081] FIGURE 49 Panels A and B depict data structures for the parser, keys, and shares in accordance with one embodiment of the present invention.

[0082] FIGURE 50 Panels A and B depict data structures relating to encryption, authentication, and hashing functionality in accordance with one embodiment of the present invention.

[0083] FIGURE 51 Panels A and B depict data formats in accordance with one embodiment of the present invention.

[0084] FIGURE 52A Panels A and B and FIGURE 52B Panels A and B depict a function library in accordance with one embodiment of the present invention.

[0085] FIGURE 53 depicts an exemplary implementation of a secure parser within a hardware system in accordance with one embodiment of the present invention.

[0086] FIGURE 54 depicts an exemplary implementation of a secure parser for data masking in accordance with one embodiment of the present invention.

[0087] FIGURE 55 depicts an exemplary data record in a data masking implementation in accordance with one embodiment of the present invention.

[0088] FIGURE 56 depicts an exemplary set of workgroup keys in accordance with one embodiment of the present invention.

[0089] FIGURE 57 depicts the use of workgroup keys in an example application of military use in accordance with one embodiment of the present invention.

[0090] FIGURE 58 depicts the use of workgroup keys in a multi-level security (MLS) solution in accordance with one embodiment of the present invention.

[0091] FIGURE 59 depicts a backup application in accordance with one embodiment of the present invention.

[0092] FIGURE 60 depicts another backup application in accordance with one embodiment of the present invention.

Detailed Description of the Invention

[0093] One aspect of the present invention is to provide a cryptographic system where one or more secure servers, or a trust engine, stores cryptographic keys and user authentication data. Users access the functionality of conventional cryptographic systems through network access to the trust engine, however, the trust engine does not release actual keys and other authentication data and therefore, the keys and data remain secure. This server-centric storage of keys and authentication data provides for user-independent security, portability, availability, and straightforwardness.

[0094] Because users can be confident in, or trust, the cryptographic system to perform user and document authentication and other cryptographic functions, a wide variety of functionality may be incorporated into the system. For example, the trust engine provider can ensure against agreement repudiation by, for example, authenticating the agreement participants, digitally signing the agreement on behalf of or for the participants, and storing a record of the agreement digitally signed by each participant. In addition, the cryptographic system may monitor agreements and determine to apply varying degrees of authentication, based on, for example, price, user, vendor, geographic location, place of use, or the like.

[0095] To facilitate a complete understanding of the invention, the remainder of the detailed description describes the invention with reference to the figures, wherein like elements are referenced with like numerals throughout.

[0096] FIGURE 1 illustrates a block diagram of a cryptographic system 100, according to aspects of an embodiment of the invention. As shown in FIGURE 1, the cryptographic system 100 includes a user system 105, a trust engine 110, a certificate authority 115, and a vendor system 120, communicating through a communication link 125.

[0097] According to one embodiment of the invention, the user system 105 comprises a conventional general-purpose computer having one or more microprocessors, such as, for example, an Intel-based processor. Moreover, the user system 105 includes an appropriate operating system, such as, for example, an operating system capable of including graphics or windows, such as Windows, Unix, Linux, or the like. As shown in FIGURE 1, the user system 105 may include a biometric device 107. The biometric device 107 may advantageously capture a user's biometric and transfer the captured biometric to the trust engine 110. According to one embodiment of the invention, the biometric device may advantageously comprise a device having attributes and features similar to those disclosed in U.S. Patent Application No. 08/926,277, filed on September 5, 1997, entitled *"RELIEF OBJECT IMAGE GENERATOR,"* U.S. Patent Application No. 09/558,634, filed on April 26, 2000, entitled *"IMAGING DEVICE FOR A RELIEF OBJECT AND SYSTEM AND METHOD OF USING THE IMAGE DEVICE,"* U.S. Patent Application No. 09/435,011, filed on November 5, 1999,

entitled *"RELIEF OBJECT SENSOR ADAPTOR,"* and U.S. Patent Application No. 09/477,943, filed on January 5, 2000, entitled *"PLANAR OPTICAL IMAGE SENSOR AND SYSTEM FOR GENERATING AN ELECTRONIC IMAGE OF A RELIEF OBJECT FOR FINGERPRINT READING,"* all of which are owned by the instant assignee, and all of which are hereby incorporated by reference herein.

[0098] In addition, the user system 105 may connect to the communication link 125 through a conventional service provider, such as, for example, a dial up, digital subscriber line (DSL), cable modem, fiber connection, or the like. According to another embodiment, the user system 105 connects the communication link 125 through network connectivity such as, for example, a local or wide area network. According to one embodiment, the operating system includes a TCP/IP stack that handles all incoming and outgoing message traffic passed over the communication link 125.

[0099] Although the user system 105 is disclosed with reference to the foregoing embodiments, the invention is not intended to be limited thereby. Rather, a skilled artisan will recognize from the disclosure herein, a wide number of alternatives embodiments of the user system 105, including almost any computing device capable of sending or receiving information from another computer system. For example, the user system 105 may include, but is not limited to, a computer workstation, an interactive television, an interactive kiosk, a personal mobile computing device, such as a digital assistant, mobile phone, laptop, or the like, a wireless communications device, a smartcard, an embedded computing device, or the like, which can interact with the communication link 125. In such alternative systems, the operating systems will likely differ and be adapted for the particular device. However, according to one embodiment, the operating systems advantageously continue to provide the appropriate communications protocols needed to establish communication with the communication link 125.

[0100] FIGURE 1 illustrates the trust engine 110. According to one embodiment, the trust engine 110 comprises one or more secure servers for accessing and storing sensitive information, which may be any type or form of data, such as, but not limited to text, audio, video, user authentication data and public and private cryptographic keys. According to one embodiment, the

authentication data includes data designed to uniquely identify a user of the cryptographic system 100. For example, the authentication data may include a user identification number, one or more biometrics, and a series of questions and answers generated by the trust engine 110 or the user, but answered initially by the user at enrollment. The foregoing questions may include demographic data, such as place of birth, address, anniversary, or the like, personal data, such as mother's maiden name, favorite ice cream, or the like, or other data designed to uniquely identify the user. The trust engine 110 compares a user's authentication data associated with a current transaction, to the authentication data provided at an earlier time, such as, for example, during enrollment. The trust engine 110 may advantageously require the user to produce the authentication data at the time of each transaction, or, the trust engine 110 may advantageously allow the user to periodically produce authentication data, such as at the beginning of a string of transactions or the logging onto a particular vendor website.

[0101] According to the embodiment where the user produces biometric data, the user provides a physical characteristic, such as, but not limited to, facial scan, hand scan, ear scan, iris scan, retinal scan, vascular pattern, DNA, a fingerprint, writing or speech, to the biometric device 107. The biometric device advantageously produces an electronic pattern, or biometric, of the physical characteristic. The electronic pattern is transferred through the user system 105 to the trust engine 110 for either enrollment or authentication purposes.

[0102] Once the user produces the appropriate authentication data and the trust engine 110 determines a positive match between that authentication data (current authentication data) and the authentication data provided at the time of enrollment (enrollment authentication data), the trust engine 110 provides the user with complete cryptographic functionality. For example, the properly authenticated user may advantageously employ the trust engine 110 to perform hashing, digitally signing, encrypting and decrypting (often together referred to only as encrypting), creating or distributing digital certificates, and the like. However, the private cryptographic keys used in the cryptographic functions will not be available outside the trust engine 110, thereby ensuring the integrity of the cryptographic keys.

[0103] According to one embodiment, the trust engine 110 generates and stores cryptographic keys. According to another embodiment, at least one cryptographic key is associated with each user. Moreover, when the cryptographic keys include public-key technology, each private key associated with a user is generated within, and not released from, the trust engine 110. Thus, so long as the user has access to the trust engine 110, the user may perform cryptographic functions using his or her private or public key. Such remote access advantageously allows users to remain completely mobile and access cryptographic functionality through practically any Internet connection, such as cellular and satellite phones, kiosks, laptops, hotel rooms and the like.

[0104] According to another embodiment, the trust engine 110 performs the cryptographic functionality using a key pair generated for the trust engine 110. According to this embodiment, the trust engine 110 first authenticates the user, and after the user has properly produced authentication data matching the enrollment authentication data, the trust engine 110 uses its own cryptographic key pair to perform cryptographic functions on behalf of the authenticated user.

[0105] A skilled artisan will recognize from the disclosure herein that the cryptographic keys may advantageously include some or all of symmetric keys, public keys, and private keys. In addition, a skilled artisan will recognize from the disclosure herein that the foregoing keys may be implemented with a wide number of algorithms available from commercial technologies, such as, for example, RSA, ELGAMAL, or the like.

[0106] FIGURE 1 also illustrates the certificate authority 115. According to one embodiment, the certificate authority 115 may advantageously comprise a trusted third-party organization or company that issues digital certificates, such as, for example, VeriSign, Baltimore, Entrust, or the like. The trust engine 110 may advantageously transmit requests for digital certificates, through one or more conventional digital certificate protocols, such as, for example, PKCS10, to the certificate authority 115. In response, the certificate authority 115 will issue a digital certificate in one or more of a number of differing protocols, such as, for example, PKCS7. According to one embodiment of the invention, the trust engine 110 requests digital certificates from several or all of the prominent certificate

authorities 115 such that the trust engine 110 has access to a digital certificate corresponding to the certificate standard of any requesting party.

[0107] According to another embodiment, the trust engine 110 internally performs certificate issuances. In this embodiment, the trust engine 110 may access a certificate system for generating certificates and/or may internally generate certificates when they are requested, such as, for example, at the time of key generation or in the certificate standard requested at the time of the request. The trust engine 110 will be disclosed in greater detail below.

[0108] FIGURE 1 also illustrates the vendor system 120. According to one embodiment, the vendor system 120 advantageously comprises a Web server. Typical Web servers generally serve content over the Internet using one of several internet markup languages or document format standards, such as the Hyper-Text Markup Language (HTML) or the Extensible Markup Language (XML). The Web server accepts requests from browsers like Netscape and Internet Explorer and then returns the appropriate electronic documents. A number of server or client-side technologies can be used to increase the power of the Web server beyond its ability to deliver standard electronic documents. For example, these technologies include Common Gateway Interface (CGI) scripts, Secure Sockets Layer (SSL) security, and Active Server Pages (ASPs). The vendor system 120 may advantageously provide electronic content relating to commercial, personal, educational, or other transactions.

[0109] Although the vendor system 120 is disclosed with reference to the foregoing embodiments, the invention is not intended to be limited thereby. Rather, a skilled artisan will recognize from the disclosure herein that the vendor system 120 may advantageously comprise any of the devices described with reference to the user system 105 or combination thereof.

[0110] FIGURE 1 also illustrates the communication link 125 connecting the user system 105, the trust engine 110, the certificate authority 115, and the vendor system 120. According to one embodiment, the communication link 125 preferably comprises the Internet. The Internet, as used throughout this disclosure is a global network of computers. The structure of the Internet, which is well known to those of ordinary skill in the art, includes a network backbone with

networks branching from the backbone. These branches, in turn, have networks branching from them, and so on. Routers move information packets between network levels, and then from network to network, until the packet reaches the neighborhood of its destination. From the destination, the destination network's host directs the information packet to the appropriate terminal, or node. In one advantageous embodiment, the Internet routing hubs comprise domain name system (DNS) servers using Transmission Control Protocol/Internet Protocol (TCP/IP) as is well known in the art. The routing hubs connect to one or more other routing hubs via high-speed communication links.

[0111] One popular part of the Internet is the World Wide Web. The World Wide Web contains different computers, which store documents capable of displaying graphical and textual information. The computers that provide information on the World Wide Web are typically called "websites." A website is defined by an Internet address that has an associated electronic page. The electronic page can be identified by a Uniform Resource Locator (URL). Generally, an electronic page is a document that organizes the presentation of text, graphical images, audio, video, and so forth.

[0112] Although the communication link 125 is disclosed in terms of its preferred embodiment, one of ordinary skill in the art will recognize from the disclosure herein that the communication link 125 may include a wide range of interactive communications links. For example, the communication link 125 may include interactive television networks, telephone networks, wireless data transmission systems, two-way cable systems, customized private or public computer networks, interactive kiosk networks, automatic teller machine networks, direct links, satellite or cellular networks, and the like.

[0113] FIGURE 2 illustrates a block diagram of the trust engine 110 of FIGURE 1 according to aspects of an embodiment of the invention. As shown in FIGURE 2, the trust engine 110 includes a transaction engine 205, a depository 210, an authentication engine 215, and a cryptographic engine 220. According to one embodiment of the invention, the trust engine 110 also includes mass storage 225. As further shown in FIGURE 2, the transaction engine 205 communicates with the depository 210, the authentication engine 215, and the cryptographic engine 220,

along with the mass storage 225. In addition, the depository 210 communicates with the authentication engine 215, the cryptographic engine 220, and the mass storage 225. Moreover, the authentication engine 215 communicates with the cryptographic engine 220. According to one embodiment of the invention, some or all of the foregoing communications may advantageously comprise the transmission of XML documents to IP addresses that correspond to the receiving device. As mentioned in the foregoing, XML documents advantageously allow designers to create their own customized document tags, enabling the definition, transmission, validation, and interpretation of data between applications and between organizations. Moreover, some or all of the foregoing communications may include conventional SSL technologies.

[0114] According to one embodiment, the transaction engine 205 comprises a data routing device, such as a conventional Web server available from Netscape, Microsoft, Apache, or the like. For example, the Web server may advantageously receive incoming data from the communication link 125. According to one embodiment of the invention, the incoming data is addressed to a front-end security system for the trust engine 110. For example, the front-end security system may advantageously include a firewall, an intrusion detection system searching for known attack profiles, and/or a virus scanner. After clearing the front-end security system, the data is received by the transaction engine 205 and routed to one of the depository 210, the authentication engine 215, the cryptographic engine 220, and the mass storage 225. In addition, the transaction engine 205 monitors incoming data from the authentication engine 215 and cryptographic engine 220, and routes the data to particular systems through the communication link 125. For example, the transaction engine 205 may advantageously route data to the user system 105, the certificate authority 115, or the vendor system 120.

[0115] According to one embodiment, the data is routed using conventional HTTP routing techniques, such as, for example, employing URLs or Uniform Resource Indicators (URIs). URIs are similar to URLs, however, URIs typically indicate the source of files or actions, such as, for example, executables, scripts, and the like. Therefore, according to the one embodiment, the user system 105, the

certificate authority 115, the vendor system 120, and the components of the trust engine 210, advantageously include sufficient data within communication URLs or URIs for the transaction engine 205 to properly route data throughout the cryptographic system.

[0116] Although the data routing is disclosed with reference to its preferred embodiment, a skilled artisan will recognize a wide number of possible data routing solutions or strategies. For example, XML or other data packets may advantageously be unpacked and recognized by their format, content, or the like, such that the transaction engine 205 may properly route data throughout the trust engine 110. Moreover, a skilled artisan will recognize that the data routing may advantageously be adapted to the data transfer protocols conforming to particular network systems, such as, for example, when the communication link 125 comprises a local network.

[0117] According to yet another embodiment of the invention, the transaction engine 205 includes conventional SSL encryption technologies, such that the foregoing systems may authenticate themselves, and vise-versa, with transaction engine 205, during particular communications. As will be used throughout this disclosure, the term "½ SSL" refers to communications where a server but not necessarily the client, is SSL authenticated, and the term "FULL SSL" refers to communications where the client and the server are SSL authenticated. When the instant disclosure uses the term "SSL", the communication may comprise ½ or FULL SSL.

[0118] As the transaction engine 205 routes data to the various components of the cryptographic system 100, the transaction engine 205 may advantageously create an audit trail. According to one embodiment, the audit trail includes a record of at least the type and format of data routed by the transaction engine 205 throughout the cryptographic system 100. Such audit data may advantageously be stored in the mass storage 225.

[0119] FIGURE 2 also illustrates the depository 210. According to one embodiment, the depository 210 comprises one or more data storage facilities, such as, for example, a directory server, a database server, or the like. As shown in FIGURE 2, the depository 210 stores cryptographic keys and enrollment

authentication data. The cryptographic keys may advantageously correspond to the trust engine 110 or to users of the cryptographic system 100, such as the user or vendor. The enrollment authentication data may advantageously include data designed to uniquely identify a user, such as, user ID, passwords, answers to questions, biometric data, or the like. This enrollment authentication data may advantageously be acquired at enrollment of a user or another alternative later time. For example, the trust engine 110 may include periodic or other renewal or reissue of enrollment authentication data.

[0120] According to one embodiment, the communication from the transaction engine 205 to and from the authentication engine 215 and the cryptographic engine 220 comprises secure communication, such as, for example conventional SSL technology. In addition, as mentioned in the foregoing, the data of the communications to and from the depository 210 may be transferred using URLs, URIs, HTTP or XML documents, with any of the foregoing advantageously having data requests and formats embedded therein.

[0121] As mentioned above, the depository 210 may advantageously comprises a plurality of secure data storage facilities. In such an embodiment, the secure data storage facilities may be configured such that a compromise of the security in one individual data storage facility will not compromise the cryptographic keys or the authentication data stored therein. For example, according to this embodiment, the cryptographic keys and the authentication data are mathematically operated on so as to statistically and substantially randomize the data stored in each data storage facility. According to one embodiment, the randomization of the data of an individual data storage facility renders that data undecipherable. Thus, compromise of an individual data storage facility produces only a randomized undecipherable number and does not compromise the security of any cryptographic keys or the authentication data as a whole.

[0122] FIGURE 2 also illustrates the trust engine 110 including the authentication engine 215. According to one embodiment, the authentication engine 215 comprises a data comparator configured to compare data from the transaction engine 205 with data from the depository 210. For example, during authentication, a user supplies current authentication data to the trust engine 110

such that the transaction engine 205 receives the current authentication data. As mentioned in the foregoing, the transaction engine 205 recognizes the data requests, preferably in the URL or URI, and routes the authentication data to the authentication engine 215. Moreover, upon request, the depository 210 forwards enrollment authentication data corresponding to the user to the authentication engine 215. Thus, the authentication engine 215 has both the current authentication data and the enrollment authentication data for comparison.

[0123] According to one embodiment, the communications to the authentication engine comprise secure communications, such as, for example, SSL technology. Additionally, security can be provided within the trust engine 110 components, such as, for example, super-encryption using public key technologies. For example, according to one embodiment, the user encrypts the current authentication data with the public key of the authentication engine 215. In addition, the depository 210 also encrypts the enrollment authentication data with the public key of the authentication engine 215. In this way, only the authentication engine's private key can be used to decrypt the transmissions.

[0124] As shown in FIGURE 2, the trust engine 110 also includes the cryptographic engine 220. According to one embodiment, the cryptographic engine comprises a cryptographic handling module, configured to advantageously provide conventional cryptographic functions, such as, for example, public-key infrastructure (PKI) functionality. For example, the cryptographic engine 220 may advantageously issue public and private keys for users of the cryptographic system 100. In this manner, the cryptographic keys are generated at the cryptographic engine 220 and forwarded to the depository 210 such that at least the private cryptographic keys are not available outside of the trust engine 110. According to another embodiment, the cryptographic engine 220 randomizes and splits at least the private cryptographic key data, thereby storing only the randomized split data. Similar to the splitting of the enrollment authentication data, the splitting process ensures the stored keys are not available outside the cryptographic engine 220. According to another embodiment, the functions of the cryptographic engine can be combined with and performed by the authentication engine 215.

[0125] According to one embodiment, communications to and from the cryptographic engine include secure communications, such as SSL technology. In addition, XML documents may advantageously be employed to transfer data and/or make cryptographic function requests.

[0126] FIGURE 2 also illustrates the trust engine 110 having the mass storage 225. As mentioned in the foregoing, the transaction engine 205 keeps data corresponding to an audit trail and stores such data in the mass storage 225. Similarly, according to one embodiment of the invention, the depository 210 keeps data corresponding to an audit trail and stores such data in the mass storage device 225. The depository audit trail data is similar to that of the transaction engine 205 in that the audit trail data comprises a record of the requests received by the depository 210 and the response thereof. In addition, the mass storage 225 may be used to store digital certificates having the public key of a user contained therein.

[0127] Although the trust engine 110 is disclosed with reference to its preferred and alternative embodiments, the invention is not intended to be limited thereby. Rather, a skilled artisan will recognize in the disclosure herein, a wide number of alternatives for the trust engine 110. For example, the trust engine 110, may advantageously perform only authentication, or alternatively, only some or all of the cryptographic functions, such as data encryption and decryption. According to such embodiments, one of the authentication engine 215 and the cryptographic engine 220 may advantageously be removed, thereby creating a more straightforward design for the trust engine 110. In addition, the cryptographic engine 220 may also communicate with a certificate authority such that the certificate authority is embodied within the trust engine 110. According to yet another embodiment, the trust engine 110 may advantageously perform authentication and one or more cryptographic functions, such as, for example, digital signing.

[0128] FIGURE 3 illustrates a block diagram of the transaction engine 205 of FIGURE 2, according to aspects of an embodiment of the invention. According to this embodiment, the transaction engine 205 comprises an operating system 305 having a handling thread and a listening thread. The operating system 305 may advantageously be similar to those found in conventional high volume servers,

such as, for example, Web servers available from Apache. The listening thread monitors the incoming communication from one of the communication link 125, the authentication engine 215, and the cryptographic engine 220 for incoming data flow. The handling thread recognizes particular data structures of the incoming data flow, such as, for example, the foregoing data structures, thereby routing the incoming data to one of the communication link 125, the depository 210, the authentication engine 215, the cryptographic engine 220, or the mass storage 225. As shown in FIGURE 3, the incoming and outgoing data may advantageously be secured through, for example, SSL technology.

[0129] FIGURE 4 illustrates a block diagram of the depository 210 of FIGURE 2 according to aspects of an embodiment of the invention. According to this embodiment, the depository 210 comprises one or more lightweight directory access protocol (LDAP) servers. LDAP directory servers are available from a wide variety of manufacturers such as Netscape, ISO, and others. FIGURE 4 also shows that the directory server preferably stores data 405 corresponding to the cryptographic keys and data 410 corresponding to the enrollment authentication data. According to one embodiment, the depository 210 comprises a single logical memory structure indexing authentication data and cryptographic key data to a unique user ID. The single logical memory structure preferably includes mechanisms to ensure a high degree of trust, or security, in the data stored therein. For example, the physical location of the depository 210 may advantageously include a wide number of conventional security measures, such as limited employee access, modern surveillance systems, and the like. In addition to, or in lieu of, the physical securities, the computer system or server may advantageously include software solutions to protect the stored data. For example, the depository 210 may advantageously create and store data 415 corresponding to an audit trail of actions taken. In addition, the incoming and outgoing communications may advantageously be encrypted with public key encryption coupled with conventional SSL technologies.

[0130] According to another embodiment, the depository 210 may comprise distinct and physically separated data storage facilities, as disclosed further with reference to FIGURE 7.

[0131] FIGURE 5 illustrates a block diagram of the authentication engine 215 of FIGURE 2 according to aspects of an embodiment of the invention. Similar to the transaction engine 205 of FIGURE 3, the authentication engine 215 comprises an operating system 505 having at least a listening and a handling thread of a modified version of a conventional Web server, such as, for example, Web servers available from Apache. As shown in FIGURE 5, the authentication engine 215 includes access to at least one private key 510. The private key 510 may advantageously be used for example, to decrypt data from the transaction engine 205 or the depository 210, which was encrypted with a corresponding public key of the authentication engine 215.

[0132] FIGURE 5 also illustrates the authentication engine 215 comprising a comparator 515, a data splitting module 520, and a data assembling module 525. According to the preferred embodiment of the invention, the comparator 515 includes technology capable of comparing potentially complex patterns related to the foregoing biometric authentication data. The technology may include hardware, software, or combined solutions for pattern comparisons, such as, for example, those representing finger print patterns or voice patterns. In addition, according to one embodiment, the comparator 515 of the authentication engine 215 may advantageously compare conventional hashes of documents in order to render a comparison result. According to one embodiment of the invention, the comparator 515 includes the application of heuristics 530 to the comparison. The heuristics 530 may advantageously address circumstances surrounding an authentication attempt, such as, for example, the time of day, IP address or subnet mask, purchasing profile, email address, processor serial number or ID, or the like.

[0133] Moreover, the nature of biometric data comparisons may result in varying degrees of confidence being produced from the matching of current biometric authentication data to enrollment data. For example, unlike a traditional password which may only return a positive or negative match, a fingerprint may be determined to be a partial match, e.g. a 90% match, a 75% match, or a 10% match, rather than simply being correct or incorrect. Other biometric identifiers such as voice print analysis or face recognition may share this property of probabilistic authentication, rather than absolute authentication.

[0134] When working with such probabilistic authentication or in other cases where an authentication is considered less than absolutely reliable, it is desirable to apply the heuristics 530 to determine whether the level of confidence in the authentication provided is sufficiently high to authenticate the transaction which is being made.

[0135] It will sometimes be the case that the transaction at issue is a relatively low value transaction where it is acceptable to be authenticated to a lower level of confidence. This could include a transaction which has a low dollar value associated with it (e.g., a $10 purchase) or a transaction with low risk (e.g., admission to a members-only web site).

[0136] Conversely, for authenticating other transactions, it may be desirable to require a high degree of confidence in the authentication before allowing the transaction to proceed. Such transactions may include transactions of large dollar value (e.g., signing a multi-million dollar supply contract) or transaction with a high risk if an improper authentication occurs (e.g., remotely logging onto a government computer).

[0137] The use of the heuristics 530 in combination with confidence levels and transactions values may be used as will be described below to allow the comparator to provide a dynamic context-sensitive authentication system.

[0138] According to another embodiment of the invention, the comparator 515 may advantageously track authentication attempts for a particular transaction. For example, when a transaction fails, the trust engine 110 may request the user to re-enter his or her current authentication data. The comparator 515 of the authentication engine 215 may advantageously employ an attempt limiter 535 to limit the number of authentication attempts, thereby prohibiting brute-force attempts to impersonate a user's authentication data. According to one embodiment, the attempt limiter 535 comprises a software module monitoring transactions for repeating authentication attempts and, for example, limiting the authentication attempts for a given transaction to three. Thus, the attempt limiter 535 will limit an automated attempt to impersonate an individual's authentication data to, for example, simply three "guesses." Upon three failures, the attempt limiter 535 may advantageously deny additional authentication attempts. Such

denial may advantageously be implemented through, for example, the comparator 515 returning a negative result regardless of the current authentication data being transmitted. On the other hand, the transaction engine 205 may advantageously block any additional authentication attempts pertaining to a transaction in which three attempts have previously failed.

[0139] The authentication engine 215 also includes the data splitting module 520 and the data assembling module 525. The data splitting module 520 advantageously comprises a software, hardware, or combination module having the ability to mathematically operate on various data so as to substantially randomize and split the data into portions. According to one embodiment, original data is not recreatable from an individual portion. The data assembling module 525 advantageously comprises a software, hardware, or combination module configured to mathematically operate on the foregoing substantially randomized portions, such that the combination thereof provides the original deciphered data. According to one embodiment, the authentication engine 215 employs the data splitting module 520 to randomize and split enrollment authentication data into portions, and employs the data assembling module 525 to reassemble the portions into usable enrollment authentication data.

[0140] FIGURE 6 illustrates a block diagram of the cryptographic engine 220 of the trust engine 200 of FIGURE 2 according to aspects of one embodiment of the invention. Similar to the transaction engine 205 of FIGURE 3, the cryptographic engine 220 comprises an operating system 605 having at least a listening and a handling thread of a modified version of a conventional Web server, such as, for example, Web servers available from Apache. As shown in FIGURE 6, the cryptographic engine 220 comprises a data splitting module 610 and a data assembling module 620 that function similar to those of FIGURE 5. However, according to one embodiment, the data splitting module 610 and the data assembling module 620 process cryptographic key data, as opposed to the foregoing enrollment authentication data. Although, a skilled artisan will recognize from the disclosure herein that the data splitting module 910 and the data splitting module 620 may be combined with those of the authentication engine 215.

[0141] The cryptographic engine 220 also comprises a cryptographic handling module 625 configured to perform one, some or all of a wide number of cryptographic functions. According to one embodiment, the cryptographic handling module 625 may comprise software modules or programs, hardware, or both. According to another embodiment, the cryptographic handling module 625 may perform data comparisons, data parsing, data splitting, data separating, data hashing, data encryption or decryption, digital signature verification or creation, digital certificate generation, storage, or requests, cryptographic key generation, or the like. Moreover, a skilled artisan will recognize from the disclosure herein that the cryptographic handling module 825 may advantageously comprises a public-key infrastructure, such as Pretty Good Privacy (PGP), an RSA-based public-key system, or a wide number of alternative key management systems. In addition, the cryptographic handling module 625 may perform public-key encryption, symmetric-key encryption, or both. In addition to the foregoing, the cryptographic handling module 625 may include one or more computer programs or modules, hardware, or both, for implementing seamless, transparent, interoperability functions.

[0142] A skilled artisan will also recognize from the disclosure herein that the cryptographic functionality may include a wide number or variety of functions generally relating to cryptographic key management systems.

[0143] FIGURE 7 illustrates a simplified block diagram of a depository system 700 according to aspects of an embodiment of the invention. As shown in FIGURE 7, the depository system 700 advantageously comprises multiple data storage facilities, for example, data storage facilities D1, D2, D3, and D4. However, it is readily understood by those of ordinary skill in the art that the depository system may have only one data storage facility. According to one embodiment of the invention, each of the data storage facilities D1 through D4 may advantageously comprise some or all of the elements disclosed with reference to the depository 210 of FIGURE 4. Similar to the depository 210, the data storage facilities D1 through D4 communicate with the transaction engine 205, the authentication engine 215, and the cryptographic engine 220, preferably through conventional SSL. Communication links transferring, for example, XML

documents. Communications from the transaction engine 205 may advantageously include requests for data, wherein the request is advantageously broadcast to the IP address of each data storage facility D1 through D4. On the other hand, the transaction engine 205 may broadcast requests to particular data storage facilities based on a wide number of criteria, such as, for example, response time, server loads, maintenance schedules, or the like.

[0144] In response to requests for data from the transaction engine 205, the depository system 700 advantageously forwards stored data to the authentication engine 215 and the cryptographic engine 220. The respective data assembling modules receive the forwarded data and assemble the data into useable formats. On the other hand, communications from the authentication engine 215 and the cryptographic engine 220 to the data storage facilities D1 through D4 may include the transmission of sensitive data to be stored. For example, according to one embodiment, the authentication engine 215 and the cryptographic engine 220 may advantageously employ their respective data splitting modules to divide sensitive data into undecipherable portions, and then transmit one or more undecipherable portions of the sensitive data to a particular data storage facility.

[0145] According to one embodiment, each data storage facility, D1 through D4, comprises a separate and independent storage system, such as, for example, a directory server. According to another embodiment of the invention, the depository system 700 comprises multiple geographically separated independent data storage systems. By distributing the sensitive data into distinct and independent storage facilities D1 through D4, some or all of which may be advantageously geographically separated, the depository system 700 provides redundancy along with additional security measures. For example, according to one embodiment, only data from two of the multiple data storage facilities, D1 through D4, are needed to decipher and reassemble the sensitive data. Thus, as many as two of the four data storage facilities D1 through D4 may be inoperative due to maintenance, system failure, power failure, or the like, without affecting the functionality of the trust engine 110. In addition, because, according to one embodiment, the data stored in each data storage facility is randomized and undecipherable, compromise of any individual data storage facility does not

necessarily compromise the sensitive data. Moreover, in the embodiment having geographical separation of the data storage facilities, a compromise of multiple geographically remote facilities becomes increasingly difficult. In fact, even a rogue employee will be greatly challenged to subvert the needed multiple independent geographically remote data storage facilities.

[0146] Although the depository system 700 is disclosed with reference to its preferred and alternative embodiments, the invention is not intended to be limited thereby. Rather, a skilled artisan will recognize from the disclosure herein, a wide number of alternatives for the depository system 700. For example, the depository system 700 may comprise one, two or more data storage facilities. In addition, sensitive data may be mathematically operated such that portions from two or more data storage facilities are needed to reassemble and decipher the sensitive data.

[0147] As mentioned in the foregoing, the authentication engine 215 and the cryptographic engine 220 each include a data splitting module 520 and 610, respectively, for splitting any type or form of sensitive data, such as, for example, text, audio, video, the authentication data and the cryptographic key data. FIGURE 8 illustrates a flowchart of a data splitting process 800 performed by the data splitting module according to aspects of an embodiment of the invention. As shown in FIGURE 8, the data splitting process 800 begins at step 805 when sensitive data "S" is received by the data splitting module of the authentication engine 215 or the cryptographic engine 220. Preferably, in step 810, the data splitting module then generates a substantially random number, value, or string or set of bits, "A." For example, the random number A may be generated in a wide number of varying conventional techniques available to one of ordinary skill in the art, for producing high quality random numbers suitable for use in cryptographic applications. In addition, according to one embodiment, the random number A comprises a bit length which may be any suitable length, such as shorter, longer or equal to the bit length of the sensitive data, S.

[0148] In addition, in step 820 the data splitting process 800 generates another statistically random number "C." According to the preferred embodiment, the generation of the statistically random numbers A and C may advantageously be done in parallel. The data splitting module then combines the numbers A and C

with the sensitive data S such that new numbers "B" and "D" are generated. For example, number B may comprise the binary combination of A XOR S and number D may comprise the binary combination of C XOR S. The XOR function, or the "exclusive-or" function, is well known to those of ordinary skill in the art. The foregoing combinations preferably occur in steps 825 and 830, respectively, and, according to one embodiment, the foregoing combinations also occur in parallel. The data splitting process 800 then proceeds to step 835 where the random numbers A and C and the numbers B and D are paired such that none of the pairings contain sufficient data, by themselves, to reorganize and decipher the original sensitive data S. For example, the numbers may be paired as follows: AC, AD, BC, and BD. According to one embodiment, each of the foregoing pairings is distributed to one of the depositories D1 through D4 of FIGURE 7. According to another embodiment, each of the foregoing pairings is randomly distributed to one of the depositories D1 through D4. For example, during a first data splitting process 800, the pairing AC may be sent to depository D2, through, for example, a random selection of D2's IP address. Then, during a second data splitting process 800, the pairing AC may be sent to depository D4, through, for example, a random selection of D4's IP address. In addition, the pairings may all be stored on one depository, and may be stored in separate locations on said depository.

[0149] Based on the foregoing, the data splitting process 800 advantageously places portions of the sensitive data in each of the four data storage facilities D1 through D4, such that no single data storage facility D1 through D4 includes sufficient encrypted data to recreate the original sensitive data S. As mentioned in the foregoing, such randomization of the data into individually unusable encrypted portions increases security and provides for maintained trust in the data even if one of the data storage facilities, D1 through D4, is compromised.

[0150] Although the data splitting process 800 is disclosed with reference to its preferred embodiment, the invention is not intended to be limited thereby. Rather a skilled artisan will recognize from the disclosure herein, a wide number of alternatives for the data splitting process 800. For example, the data splitting process may advantageously split the data into two numbers, for example, random number A and number B and, randomly distribute A and B through two data

storage facilities. Moreover, the data splitting process 800 may advantageously split the data among a wide number of data storage facilities through generation of additional random numbers. The data may be split into any desired, selected, predetermined, or randomly assigned size unit, including but not limited to, a bit, bits, bytes, kilobytes, megabytes or larger, or any combination or sequence of sizes. In addition, varying the sizes of the data units resulting from the splitting process may render the data more difficult to restore to a useable form, thereby increasing security of sensitive data. It is readily apparent to those of ordinary skill in the art that the split data unit sizes may be a wide variety of data unit sizes or patterns of sizes or combinations of sizes. For example, the data unit sizes may be selected or predetermined to be all of the same size, a fixed set of different sizes, a combination of sizes, or randomly generates sizes. Similarly, the data units may be distributed into one or more shares according to a fixed or predetermined data unit size, a pattern or combination of data unit sizes, or a randomly generated data unit size or sizes per share.

[0151] As mentioned in the foregoing, in order to recreate the sensitive data S, the data portions need to be derandomized and reorganized. This process may advantageously occur in the data assembling modules, 525 and 620, of the authentication engine 215 and the cryptographic engine 220, respectively. The data assembling module, for example, data assembly module 525, receives data portions from the data storage facilities D1 through D4, and reassembles the data into useable form. For example, according to one embodiment where the data splitting module 520 employed the data splitting process 800 of FIGURE 8, the data assembling module 525 uses data portions from at least two of the data storage facilities D1 through D4 to recreate the sensitive data S. For example, the pairings of AC, AD, BC, and BD, were distributed such that any two provide one of A and B, or, C and D. Noting that S = A XOR B or S = C XOR D indicates that when the data assembling module receives one of A and B, or, C and D, the data assembling module 525 can advantageously reassemble the sensitive data S. Thus, the data assembling module 525 may assemble the sensitive data S, when, for example, it receives data portions from at least the first two of the data storage facilities D1 through D4 to respond to an assemble request by the trust engine 110.

[0152] Based on the above data splitting and assembling processes, the sensitive data S exists in usable format only in a limited area of the trust engine 110. For example, when the sensitive data S includes enrollment authentication data, usable, nonrandomized enrollment authentication data is available only in the authentication engine 215. Likewise, when the sensitive data S includes private cryptographic key data, usable, nonrandomized private cryptographic key data is available only in the cryptographic engine 220.

[0153] Although the data splitting and assembling processes are disclosed with reference to their preferred embodiments, the invention is not intended to be limited thereby. Rather, a skilled artisan will recognize from the disclosure herein, a wide number of alternatives for splitting and reassembling the sensitive data S. For example, public-key encryption may be used to further secure the data at the data storage facilities D1 through D4. In addition, it is readily apparent to those of ordinary skill in the art that the data splitting module described herein is also a separate and distinct embodiment of the present invention that may be incorporated into, combined with or otherwise made part of any pre-existing computer systems, software suites, database, or combinations thereof, or other embodiments of the present invention, such as the trust engine, authentication engine, and transaction engine disclosed and described herein.

[0154] FIGURE 9A illustrates a data flow of an enrollment process 900 according to aspects of an embodiment of the invention. As shown in FIGURE 9A, the enrollment process 900 begins at step 905 when a user desires to enroll with the trust engine 110 of the cryptographic system 100. According to this embodiment, the user system 105 advantageously includes a client-side applet, such as a Java-based, that queries the user to enter enrollment data, such as demographic data and enrollment authentication data. According to one embodiment, the enrollment authentication data includes user ID, password(s), biometric(s), or the like. According to one embodiment, during the querying process, the client-side applet preferably communicates with the trust engine 110 to ensure that a chosen user ID is unique. When the user ID is nonunique, the trust engine 110 may advantageously suggest a unique user ID. The client-side applet gathers the enrollment data and transmits the enrollment data, for example, through

and XML document, to the trust engine 110, and in particular, to the transaction engine 205. According to one embodiment, the transmission is encoded with the public key of the authentication engine 215.

[0155] According to one embodiment, the user performs a single enrollment during step 905 of the enrollment process 900. For example, the user enrolls himself or herself as a particular person, such as Joe User. When Joe User desires to enroll as Joe User, CEO of Mega Corp., then according to this embodiment, Joe User enrolls a second time, receives a second unique user ID and the trust engine 110 does not associate the two identities. According to another embodiment of the invention, the enrollment process 900 provides for multiple user identities for a single user ID. Thus, in the above example, the trust engine 110 will advantageously associate the two identities of Joe User. As will be understood by a skilled artisan from the disclosure herein, a user may have many identities, for example, Joe User the head of household, Joe User the member of the Charitable Foundations, and the like. Even though the user may have multiple identities, according to this embodiment, the trust engine 110 preferably stores only one set of enrollment data. Moreover, users may advantageously add, edit/update, or delete identities as they are needed.

[0156] Although the enrollment process 900 is disclosed with reference to its preferred embodiment, the invention is not intended to be limited thereby. Rather, a skilled artisan will recognize from the disclosure herein, a wide number of alternatives for gathering of enrollment data, and in particular, enrollment authentication data. For example, the applet may be common object model (COM) based applet or the like.

[0157] On the other hand, the enrollment process may include graded enrollment. For example, at a lowest level of enrollment, the user may enroll over the communication link 125 without producing documentation as to his or her identity. According to an increased level of enrollment, the user enrolls using a trusted third party, such as a digital notary. For example, and the user may appear in person to the trusted third party, produce credentials such as a birth certificate, driver's license, military ID, or the like, and the trusted third party may advantageously include, for example, their digital signature in enrollment submission. The trusted

third party may include an actual notary, a government agency, such as the Post Office or Department of Motor Vehicles, a human resources person in a large company enrolling an employee, or the like. A skilled artisan will understand from the disclosure herein that a wide number of varying levels of enrollment may occur during the enrollment process 900.

[0158] After receiving the enrollment authentication data, at step 915, the transaction engine 205, using conventional FULL SSL technology forwards the enrollment authentication data to the authentication engine 215. In step 920, the authentication engine 215 decrypts the enrollment authentication data using the private key of the authentication engine 215. In addition, the authentication engine 215 employs the data splitting module to mathematically operate on the enrollment authentication data so as to split the data into at least two independently undecipherable, randomized, numbers. As mentioned in the foregoing, at least two numbers may comprise a statistically random number and a binary X0Red number. In step 925, the authentication engine 215 forwards each portion of the randomized numbers to one of the data storage facilities D1 through D4. As mentioned in the foregoing, the authentication engine 215 may also advantageously randomize which portions are transferred to which depositories.

[0159] Often during the enrollment process 900, the user will also desire to have a digital certificate issued such that he or she may receive encrypted documents from others outside the cryptographic system 100. As mentioned in the foregoing, the certificate authority 115 generally issues digital certificates according to one or more of several conventional standards. Generally, the digital certificate includes a public key of the user or system, which is known to everyone.

[0160] Whether the user requests a digital certificate at enrollment, or at another time, the request is transferred through the trust engine 110 to the authentication engine 215. According to one embodiment, the request includes an XML document having, for example, the proper name of the user. According to step 935, the authentication engine 215 transfers the request to the cryptographic engine 220 instructing the cryptographic engine 220 to generate a cryptographic key or key pair.

[0161] Upon request, at step 935, the cryptographic engine 220 generates at least one cryptographic key. According to one embodiment, the cryptographic handling module 625 generates a key pair, where one key is used as a private key, and one is used as a public key. The cryptographic engine 220 stores the private key and, according to one embodiment, a copy of the public key. In step 945, the cryptographic engine 220 transmits a request for a digital certificate to the transaction engine 205. According to one embodiment, the request advantageously includes a standardized request, such as PKCS10, embedded in, for example, an XML document. The request for a digital certificate may advantageously correspond to one or more certificate authorities and the one or more standard formats the certificate authorities require.

[0162] In step 950 the transaction engine 205 forwards this request to the certificate authority 115, who, in step 955, returns a digital certificate. The return digital certificate may advantageously be in a standardized format, such as PKCS7, or in a proprietary format of one or more of the certificate authorities 115. In step 960, the digital certificate is received by the transaction engine 205, and a copy is forwarded to the user and a copy is stored with the trust engine 110. The trust engine 110 stores a copy of the certificate such that the trust engine 110 will not need to rely on the availability of the certificate authority 115. For example, when the user desires to send a digital certificate, or a third party requests the user's digital certificate, the request for the digital certificate is typically sent to the certificate authority 115. However, if the certificate authority 115 is conducting maintenance or has been victim of a failure or security compromise, the digital certificate may not be available.

[0163] At any time after issuing the cryptographic keys, the cryptographic engine 220 may advantageously employ the data splitting process 800 described above such that the cryptographic keys are split into independently undecipherable randomized numbers. Similar to the authentication data, at step 965 the cryptographic engine 220 transfers the randomized numbers to the data storage facilities D1 through D4.

[0164] A skilled artisan will recognize from the disclosure herein that the user may request a digital certificate anytime after enrollment. Moreover, the

communications between systems may advantageously include FULL SSL or public-key encryption technologies. Moreover, the enrollment process may issue multiple digital certificates from multiple certificate authorities, including one or more proprietary certificate authorities internal or external to the trust engine 110.

[0165] As disclosed in steps 935 through 960, one embodiment of the invention includes the request for a certificate that is eventually stored on the trust engine 110. Because, according to one embodiment, the cryptographic handling module 625 issues the keys used by the trust engine 110, each certificate corresponds to a private key. Therefore, the trust engine 110 may advantageously provide for interoperability through monitoring the certificates owned by, or associated with, a user. For example, when the cryptographic engine 220 receives a request for a cryptographic function, the cryptographic handling module 625 may investigate the certificates owned by the requesting user to determine whether the user owns a private key matching the attributes of the request. When such a certificate exists, the cryptographic handling module 625 may use the certificate or the public or private keys associated therewith, to perform the requested function. When such a certificate does not exist, the cryptographic handling module 625 may advantageously and transparently perform a number of actions to attempt to remedy the lack of an appropriate key. For example, FIGURE 9B illustrates a flowchart of an interoperability process 970, which according to aspects of an embodiment of the invention, discloses the foregoing steps to ensure the cryptographic handling module 625 performs cryptographic functions using appropriate keys.

[0166] As shown in FIGURE 9B, the interoperability process 970 begins with step 972 where the cryptographic handling module 925 determines the type of certificate desired. According to one embodiment of the invention, the type of certificate may advantageously be specified in the request for cryptographic functions, or other data provided by the requestor. According to another embodiment, the certificate type may be ascertained by the data format of the request. For example, the cryptographic handling module 925 may advantageously recognize the request corresponds to a particular type.

[0167] According to one embodiment, the certificate type may include one or more algorithm standards, for example, RSA, ELGAMAL, or the like. In addition, the certificate type may include one or more key types, such as symmetric keys, public keys, strong encryption keys such as 256 bit keys, less secure keys, or the like. Moreover, the certificate type may include upgrades or replacements of one or more of the foregoing algorithm standards or keys, one or more message or data formats, one or more data encapsulation or encoding schemes, such as Base 32 or Base 64. The certificate type may also include compatibility with one or more third-party cryptographic applications or interfaces, one or more communication protocols, or one or more certificate standards or protocols. A skilled artisan will recognize from the disclosure herein that other differences may exist in certificate types, and translations to and from those differences may be implemented as disclosed herein.

[0168] Once the cryptographic handling module 625 determines the certificate type, the interoperability process 970 proceeds to step 974, and determines whether the user owns a certificate matching the type determined in step 974. When the user owns a matching certificate, for example, the trust engine 110 has access to the matching certificate through, for example, prior storage thereof, the cryptographic handling module 825 knows that a matching private key is also stored within the trust engine 110. For example, the matching private key may be stored within the depository 210 or depository system 700. The cryptographic handling module 625 may advantageously request the matching private key be assembled from, for example, the depository 210, and then in step 976, use the matching private key to perform cryptographic actions or functions. For example, as mentioned in the foregoing, the cryptographic handling module 625 may advantageously perform hashing, hash comparisons, data encryption or decryption, digital signature verification or creation, or the like.

[0169] When the user does not own a matching certificate, the interoperability process 970 proceeds to step 978 where the cryptographic handling module 625 determines whether the users owns a cross-certified certificate. According to one embodiment, cross-certification between certificate authorities occurs when a first certificate authority determines to trust certificates from a second certificate

authority. In other words, the first certificate authority determines that certificates from the second certificate authority meets certain quality standards, and therefore, may be "certified" as equivalent to the first certificate authority's own certificates. Cross-certification becomes more complex when the certificate authorities issue, for example, certificates having levels of trust. For example, the first certificate authority may provide three levels of trust for a particular certificate, usually based on the degree of reliability in the enrollment process, while the second certificate authority may provide seven levels of trust. Cross-certification may advantageously track which levels and which certificates from the second certificate authority may be substituted for which levels and which certificates from the first. When the foregoing cross-certification is done officially and publicly between two certification authorities, the mapping of certificates and levels to one another is often called "chaining."

[0170] According to another embodiment of the invention, the cryptographic handling module 625 may advantageously develop cross-certifications outside those agreed upon by the certificate authorities. For example, the cryptographic handling module 625 may access a first certificate authority's certificate practice statement (CPS), or other published policy statement, and using, for example, the authentication tokens required by particular trust levels, match the first certificate authority's certificates to those of another certificate authority.

[0171] When, in step 978, the cryptographic handling module 625 determines that the users owns a cross-certified certificate, the interoperability process 970 proceeds to step 976, and performs the cryptographic action or function using the cross-certified public key, private key, or both. Alternatively, when the cryptographic handling module 625 determines that the users does not own a cross-certified certificate, the interoperability process 970 proceeds to step 980, where the cryptographic handling module 625 selects a certificate authority that issues the requested certificate type, or a certificate cross-certified thereto. In step 982, the cryptographic handling module 625 determines whether the user enrollment authentication data, discussed in the foregoing, meets the authentication requirements of the chosen certificate authority. For example, if the user enrolled over a network by, for example, answering demographic and other questions, the

authentication data provided may establish a lower level of trust than a user providing biometric data and appearing before a third-party, such as, for example, a notary. According to one embodiment, the foregoing authentication requirements may advantageously be provided in the chosen authentication authority's CPS.

[0172] When the user has provided the trust engine 110 with enrollment authentication data meeting the requirements of chosen certificate authority, the interoperability process 970 proceeds to step 984, where the cryptographic handling module 825 acquires the certificate from the chosen certificate authority. According to one embodiment, the cryptographic handling module 625 acquires the certificate by following steps 945 through 960 of the enrollment process 900. For example, the cryptographic handling module 625 may advantageously employ one or more public keys from one or more of the key pairs already available to the cryptographic engine 220, to request the certificate from the certificate authority. According to another embodiment, the cryptographic handling module 625 may advantageously generate one or more new key pairs, and use the public keys corresponding thereto, to request the certificate from the certificate authority.

[0173] According to another embodiment, the trust engine 110 may advantageously include one or more certificate issuing modules capable of issuing one or more certificate types. According to this embodiment, the certificate issuing module may provide the foregoing certificate. When the cryptographic handling module 625 acquires the certificate, the interoperability process 970 proceeds to step 976, and performs the cryptographic action or function using the public key, private key, or both corresponding to the acquired certificate.

[0174] When the user, in step 982, has not provided the trust engine 110 with enrollment authentication data meeting the requirements of chosen certificate authority, the cryptographic handling module 625 determines, in step 986 whether there are other certificate authorities that have different authentication requirements. For example, the cryptographic handling module 625 may look for certificate authorities having lower authentication requirements, but still issue the chosen certificates, or cross-certifications thereof.

[0175] When the foregoing certificate authority having lower requirements exists, the interoperability process 970 proceeds to step 980 and chooses that certificate authority. Alternatively, when no such certificate authority exists, in step 988, the trust engine 110 may request additional authentication tokens from the user. For example, the trust engine 110 may request new enrollment authentication data comprising, for example, biometric data. Also, the trust engine 110 may request the user appear before a trusted third party and provide appropriate authenticating credentials, such as, for example, appearing before a notary with a drivers license, social security card, bank card, birth certificate, military ID, or the like. When the trust engine 110 receives updated authentication data, the interoperability process 970 proceeds to step 984 and acquires the foregoing chosen certificate.

[0176] Through the foregoing interoperability process 970, the cryptographic handling module 625 advantageously provides seamless, transparent, translations and conversions between differing cryptographic systems. A skilled artisan will recognize from the disclosure herein, a wide number of advantages and implementations of the foregoing interoperable system. For example, the foregoing step 986 of the interoperability process 970 may advantageously include aspects of trust arbitrage, discussed in further detail below, where the certificate authority may under special circumstances accept lower levels of cross-certification. In addition, the interoperability process 970 may include ensuring interoperability between and employment of standard certificate revocations, such as employing certificate revocation lists (CRL), online certificate status protocols (OCSP), or the like.

[0177] FIGURE 10 illustrates a data flow of an authentication process 1000 according to aspects of an embodiment of the invention. According to one embodiment, the authentication process 1000 includes gathering current authentication data from a user and comparing that to the enrollment authentication data of the user. For example, the authentication process 1000 begins at step 1005 where a user desires to perform a transaction with, for example, a vendor. Such transactions may include, for example, selecting a purchase option, requesting access to a restricted area or device of the vendor system 120, or the like. At step

1010, a vendor provides the user with a transaction ID and an authentication request. The transaction ID may advantageously include a 192 bit quantity having a 32 bit timestamp concatenated with a 128 bit random quantity, or a "nonce," concatenated with a 32 bit vendor specific constant. Such a transaction ID uniquely identifies the transaction such that copycat transactions can be refused by the trust engine 110.

[0178] The authentication request may advantageously include what level of authentication is needed for a particular transaction. For example, the vendor may specify a particular level of confidence that is required for the transaction at issue. If authentication cannot be made to this level of confidence, as will be discussed below, the transaction will not occur without either further authentication by the user to raise the level of confidence, or a change in the terms of the authentication between the vendor and the server. These issues are discussed more completely below.

[0179] According to one embodiment, the transaction ID and the authentication request may be advantageously generated by a vendor-side applet or other software program. In addition, the transmission of the transaction ID and authentication data may include one or more XML documents encrypted using conventional SSL technology, such as, for example, ½ SSL, or, in other words vendor-side authenticated SSL.

[0180] After the user system 105 receives the transaction ID and authentication request, the user system 105 gathers the current authentication data, potentially including current biometric information, from the user. The user system 105, at step 1015, encrypts at least the current authentication data "B" and the transaction ID, with the public key of the authentication engine 215, and transfers that data to the trust engine 110. The transmission preferably comprises XML documents encrypted with at least conventional ½ SSL technology. In step 1020, the transaction engine 205 receives the transmission, preferably recognizes the data format or request in the URL or URI, and forwards the transmission to the authentication engine 215.

[0181] During steps 1015 and 1020, the vendor system 120, at step 1025, forwards the transaction ID and the authentication request to the trust engine 110,

using the preferred FULL SSL technology. This communication may also include a vendor ID, although vendor identification may also be communicated through a non-random portion of the transaction ID. At steps 1030 and 1035, the transaction engine 205 receives the communication, creates a record in the audit trail, and generates a request for the user's enrollment authentication data to be assembled from the data storage facilities D1 through D4. At step 1040, the depository system 700 transfers the portions of the enrollment authentication data corresponding to the user to the authentication engine 215. At step 1045, the authentication engine 215 decrypts the transmission using its private key and compares the enrollment authentication data to the current authentication data provided by the user.

[0182] The comparison of step 1045 may advantageously apply heuristical context sensitive authentication, as referred to in the forgoing, and discussed in further detail below. For example, if the biometric information received does not match perfectly, a lower confidence match results. In particular embodiments, the level of confidence of the authentication is balanced against the nature of the transaction and the desires of both the user and the vendor. Again, this is discussed in greater detail below.

[0183] At step 1050, the authentication engine 215 fills in the authentication request with the result of the comparison of step 1045. According to one embodiment of the invention, the authentication request is filled with a YES/NO or TRUE/FALSE result of the authentication process 1000. In step 1055 the filled-in authentication request is returned to the vendor for the vendor to act upon, for example, allowing the user to complete the transaction that initiated the authentication request. According to one embodiment, a confirmation message is passed to the user.

[0184] Based on the foregoing, the authentication process 1000 advantageously keeps sensitive data secure and produces results configured to maintain the integrity of the sensitive data. For example, the sensitive data is assembled only inside the authentication engine 215. For example, the enrollment authentication data is undecipherable until it is assembled in the authentication engine 215 by the data assembling module, and the current authentication data is undecipherable until

it is unwrapped by the conventional SSL technology and the private key of the authentication engine 215. Moreover, the authentication result transmitted to the vendor does not include the sensitive data, and the user may not even know whether he or she produced valid authentication data.

[0185] Although the authentication process 1000 is disclosed with reference to its preferred and alternative embodiments, the invention is not intended to be limited thereby. Rather, a skilled artisan will recognize from the disclosure herein, a wide number of alternatives for the authentication process 1000. For example, the vendor may advantageously be replaced by almost any requesting application, even those residing with the user system 105. For example, a client application, such as Microsoft Word, may use an application program interface (API) or a cryptographic API (CAPI) to request authentication before unlocking a document. Alternatively, a mail server, a network, a cellular phone, a personal or mobile computing device, a workstation, or the like, may all make authentication requests that can be filled by the authentication process 1000. In fact, after providing the foregoing trusted authentication process 1000, the requesting application or device may provide access to or use of a wide number of electronic or computer devices or systems.

[0186] Moreover, the authentication process 1000 may employ a wide number of alternative procedures in the event of authentication failure. For example, authentication failure may maintain the same transaction ID and request that the user reenter his or her current authentication data. As mentioned in the foregoing, use of the same transaction ID allows the comparator of the authentication engine 215 to monitor and limit the number of authentication attempts for a particular transaction, thereby creating a more secure cryptographic system 100.

[0187] In addition, the authentication process 1000 may be advantageously be employed to develop elegant single sign-on solutions, such as, unlocking a sensitive data vault. For example, successful or positive authentication may provide the authenticated user the ability to automatically access any number of passwords for an almost limitless number of systems and applications. For example, authentication of a user may provide the user access to password, login, financial credentials, or the like, associated with multiple online vendors, a local

area network, various personal computing devices, Internet service providers, auction providers, investment brokerages, or the like. By employing a sensitive data vault, users may choose truly large and random passwords because they no longer need to remember them through association. Rather, the authentication process 1000 provides access thereto. For example, a user may choose a random alphanumeric string that is twenty plus digits in length rather than something associated with a memorable data, name, etc.

[0188] According to one embodiment, a sensitive data vault associated with a given user may advantageously be stored in the data storage facilities of the depository 210, or split and stored in the depository system 700. According to this embodiment, after positive user authentication, the trust engine 110 serves the requested sensitive data, such as, for example, to the appropriate password to the requesting application. According to another embodiment, the trust engine 110 may include a separate system for storing the sensitive data vault. For example, the trust engine 110 may include a stand-alone software engine implementing the data vault functionality and figuratively residing "behind" the foregoing front-end security system of the trust engine 110. According to this embodiment, the software engine serves the requested sensitive data after the software engine receives a signal indicating positive user authentication from the trust engine 110.

[0189] In yet another embodiment, the data vault may be implemented by a third-party system. Similar to the software engine embodiment, the third-party system may advantageously serve the requested sensitive data after the third-party system receives a signal indicating positive user authentication from the trust engine 110. According to yet another embodiment, the data vault may be implemented on the user system 105. A user-side software engine may advantageously serve the foregoing data after receiving a signal indicating positive user authentication from the trust engine 110.

[0190] Although the foregoing data vaults are disclosed with reference to alternative embodiments, a skilled artisan will recognize from the disclosure herein, a wide number of additional implementations thereof. For example, a particular data vault may include aspects from some or all of the foregoing embodiments. In addition, any of the foregoing data vaults may employ one or

more authentication requests at varying times. For example, any of the data vaults may require authentication every one or more transactions, periodically, every one or more sessions, every access to one or more Webpages or Websites, at one or more other specified intervals, or the like.

[0191] FIGURE 11 illustrates a data flow of a signing process 1100 according to aspects of an embodiment of the invention. As shown in FIGURE 11, the signing process 1100 includes steps similar to those of the authentication process 1000 described in the foregoing with reference to FIGURE 10. According to one embodiment of the invention, the signing process 1100 first authenticates the user and then performs one or more of several digital signing functions as will be discussed in further detail below. According to another embodiment, the signing process 1100 may advantageously store data related thereto, such as hashes of messages or documents, or the like. This data may advantageously be used in an audit or any other event, such as for example, when a participating party attempts to repudiate a transaction.

[0192] As shown in FIGURE 11, during the authentication steps, the user and vendor may advantageously agree on a message, such as, for example, a contract. During signing, the signing process 1100 advantageously ensures that the contract signed by the user is identical to the contract supplied by the vendor. Therefore, according to one embodiment, during authentication, the vendor and the user include a hash of their respective copies of the message or contract, in the data transmitted to the authentication engine 215. By employing only a hash of a message or contract, the trust engine 110 may advantageously store a significantly reduced amount of data, providing for a more efficient and cost effective cryptographic system. In addition, the stored hash may be advantageously compared to a hash of a document in question to determine whether the document in question matches one signed by any of the parties. The ability to determine whether the document is identical to one relating to a transaction provides for additional evidence that can be used against a claim for repudiation by a party to a transaction.

[0193] In step 1103, the authentication engine 215 assembles the enrollment authentication data and compares it to the current authentication data provided by

the user. When the comparator of the authentication engine 215 indicates that the enrollment authentication data matches the current authentication data, the comparator of the authentication engine 215 also compares the hash of the message supplied by the vendor to the hash of the message supplied by the user. Thus, the authentication engine 215 advantageously ensures that the message agreed to by the user is identical to that agreed to by the vendor.

[0194] In step 1105, the authentication engine 215 transmits a digital signature request to the cryptographic engine 220. According to one embodiment of the invention, the request includes a hash of the message or contract. However, a skilled artisan will recognize from the disclosure herein that the cryptographic engine 220 may encrypt virtually any type of data, including, but not limited to, video, audio, biometrics, images or text to form the desired digital signature. Returning to step 1105, the digital signature request preferably comprises an XML document communicated through conventional SSL technologies.

[0195] In step 1110, the authentication engine 215 transmits a request to each of the data storage facilities D1 through D4, such that each of the data storage facilities D1 through D4 transmit their respective portion of the cryptographic key or keys corresponding to a signing party. According to another embodiment, the cryptographic engine 220 employs some or all of the steps of the interoperability process 970 discussed in the foregoing, such that the cryptographic engine 220 first determines the appropriate key or keys to request from the depository 210 or the depository system 700 for the signing party, and takes actions to provide appropriate matching keys. According to still another embodiment, the authentication engine 215 or the cryptographic engine 220 may advantageously request one or more of the keys associated with the signing party and stored in the depository 210 or depository system 700.

[0196] According to one embodiment, the signing party includes one or both the user and the vendor. In such case, the authentication engine 215 advantageously requests the cryptographic keys corresponding to the user and/or the vendor. According to another embodiment, the signing party includes the trust engine 110. In this embodiment, the trust engine 110 is certifying that the authentication process 1000 properly authenticated the user, vendor, or both. Therefore, the

authentication engine 215 requests the cryptographic key of the trust engine 110, such as, for example, the key belonging to the cryptographic engine 220, to perform the digital signature. According to another embodiment, the trust engine 110 performs a digital notary-like function. In this embodiment, the signing party includes the user, vendor, or both, along with the trust engine 110. Thus, the trust engine 110 provides the digital signature of the user and/or vendor, and then indicates with its own digital signature that the user and/or vendor were properly authenticated. In this embodiment, the authentication engine 215 may advantageously request assembly of the cryptographic keys corresponding to the user, the vendor, or both. According to another embodiment, the authentication engine 215 may advantageously request assembly of the cryptographic keys corresponding to the trust engine 110.

[0197] According to another embodiment, the trust engine 110 performs power of attorney-like functions. For example, the trust engine 110 may digitally sign the message on behalf of a third party. In such case, the authentication engine 215 requests the cryptographic keys associated with the third party. According to this embodiment, the signing process 1100 may advantageously include authentication of the third party, before allowing power of attorney-like functions. In addition, the authentication process 1000 may include a check for third party constraints, such as, for example, business logic or the like dictating when and in what circumstances a particular third-party's signature may be used.

[0198] Based on the foregoing, in step 1110, the authentication engine requested the cryptographic keys from the data storage facilities D1 through D4 corresponding to the signing party. In step 1115, the data storage facilities D1 through D4 transmit their respective portions of the cryptographic key corresponding to the signing party to the cryptographic engine 220. According to one embodiment, the foregoing transmissions include SSL technologies. According to another embodiment, the foregoing transmissions may advantageously be super-encrypted with the public key of the cryptographic engine 220.

[0199] In step 1120, the cryptographic engine 220 assembles the foregoing cryptographic keys of the signing party and encrypts the message therewith,

thereby forming the digital signature(s). In step 1125 of the signing process 1100, the cryptographic engine 220 transmits the digital signature(s) to the authentication engine 215. In step 1130, the authentication engine 215 transmits the filled-in authentication request along with a copy of the hashed message and the digital signature(s) to the transaction engine 205. In step 1135, the transaction engine 205 transmits a receipt comprising the transaction ID, an indication of whether the authentication was successful, and the digital signature(s), to the vendor. According to one embodiment, the foregoing transmission may advantageously include the digital signature of the trust engine 110. For example, the trust engine 110 may encrypt the hash of the receipt with its private key, thereby forming a digital signature to be attached to the transmission to the vendor.

[0200] According to one embodiment, the transaction engine 205 also transmits a confirmation message to the user. Although the signing process 1100 is disclosed with reference to its preferred and alternative embodiments, the invention is not intended to be limited thereby. Rather, a skilled artisan will recognize from the disclosure herein, a wide number of alternatives for the signing process 1100. For example, the vendor may be replaced with a user application, such as an email application. For example, the user may wish to digitally sign a particular email with his or her digital signature. In such an embodiment, the transmission throughout the signing process 1100 may advantageously include only one copy of a hash of the message. Moreover, a skilled artisan will recognize from the disclosure herein that a wide number of client applications may request digital signatures. For example, the client applications may comprise word processors, spreadsheets, emails, voicemail, access to restricted system areas, or the like.

[0201] In addition, a skilled artisan will recognize from the disclosure herein that steps 1105 through 1120 of the signing process 1100 may advantageously employ some or all of the steps of the interoperability process 970 of FIGURE 9B, thereby providing interoperability between differing cryptographic systems that may, for example, need to process the digital signature under differing signature types.

[0202] FIGURE 12 illustrates a data flow of an encryption/decryption process 1200 according to aspects of an embodiment of the invention. As shown in FIGURE 12, the decryption process 1200 begins by authenticating the user using

the authentication process 1000. According to one embodiment, the authentication process 1000 includes in the authentication request, a synchronous session key. For example, in conventional PKI technologies, it is understood by skilled artisans that encrypting or decrypting data using public and private keys is mathematically intensive and may require significant system resources. However, in symmetric key cryptographic systems, or systems where the sender and receiver of a message share a single common key that is used to encrypt and decrypt a message, the mathematical operations are significantly simpler and faster. Thus, in the conventional PKI technologies, the sender of a message will generate synchronous session key, and encrypt the message using the simpler, faster symmetric key system. Then, the sender will encrypt the session key with the public key of the receiver. The encrypted session key will be attached to the synchronously encrypted message and both data are sent to the receiver. The receiver uses his or her private key to decrypt the session key, and then uses the session key to decrypt the message. Based on the foregoing, the simpler and faster symmetric key system is used for the majority of the encryption/decryption processing. Thus, in the decryption process 1200, the decryption advantageously assumes that a synchronous key has been encrypted with the public key of the user. Thus, as mentioned in the foregoing, the encrypted session key is included in the authentication request.

[0203] Returning to the decryption process 1200, after the user has been authenticated in step 1205, the authentication engine 215 forwards the encrypted session key to the cryptographic engine 220. In step 1210, the authentication engine 215 forwards a request to each of the data storage facilities, D1 through D4, requesting the cryptographic key data of the user. In step 1215, each data storage facility, D1 through D4, transmits their respective portion of the cryptographic key to the cryptographic engine 220. According to one embodiment, the foregoing transmission is encrypted with the public key of the cryptographic engine 220.

[0204] In step 1220 of the decryption process 1200, the cryptographic engine 220 assembles the cryptographic key and decrypts the session key therewith. In step 1225, the cryptographic engine forwards the session key to the authentication engine 215. In step 1227, the authentication engine 215 fills in the authentication

request including the decrypted session key, and transmits the filled-in authentication request to the transaction engine 205. In step 1230, the transaction engine 205 forwards the authentication request along with the session key to the requesting application or vendor. Then, according to one embodiment, the requesting application or vendor uses the session key to decrypt the encrypted message.

[0205] Although the decryption process 1200 is disclosed with reference to its preferred and alternative embodiments, a skilled artisan will recognize from the disclosure herein, a wide number of alternatives for the decryption process 1200. For example, the decryption process 1200 may forego synchronous key encryption and rely on full public-key technology. In such an embodiment, the requesting application may transmit the entire message to the cryptographic engine 220, or, may employ some type of compression or reversible hash in order to transmit the message to the cryptographic engine 220. A skilled artisan will also recognize from the disclosure herein that the foregoing communications may advantageously include XML documents wrapped in SSL technology.

[0206] The encryption/decryption process 1200 also provides for encryption of documents or other data. Thus, in step 1235, a requesting application or vendor may advantageously transmit to the transaction engine 205 of the trust engine 110, a request for the public key of the user. The requesting application or vendor makes this request because the requesting application or vendor uses the public key of the user, for example, to encrypt the session key that will be used to encrypt the document or message. As mentioned in the enrollment process 900, the transaction engine 205 stores a copy of the digital certificate of the user, for example, in the mass storage 225. Thus, in step 1240 of the encryption process 1200, the transaction engine 205 requests the digital certificate of the user from the mass storage 225. In step 1245, the mass storage 225 transmits the digital certificate corresponding to the user, to the transaction engine 205. In step 1250, the transaction engine 205 transmits the digital certificate to the requesting application or vendor. According to one embodiment, the encryption portion of the encryption process 1200 does not include the authentication of a user. This is

because the requesting vendor needs only the public key of the user, and is not requesting any sensitive data.

[0207] A skilled artisan will recognize from the disclosure herein that if a particular user does not have a digital certificate, the trust engine 110 may employ some or all of the enrollment process 900 in order to generate a digital certificate for that particular user. Then, the trust engine 110 may initiate the encryption/decryption process 1200 and thereby provide the appropriate digital certificate. In addition, a skilled artisan will recognize from the disclosure herein that steps 1220 and 1235 through 1250 of the encryption/decryption process 1200 may advantageously employ some or all of the steps of the interoperability process of FIGURE 9B, thereby providing interoperability between differing cryptographic systems that may, for example, need to process the encryption.

[0208] FIGURE 13 illustrates a simplified block diagram of a trust engine system 1300 according to aspects of yet another embodiment of the invention. As shown in FIGURE 13, the trust engine system 1300 comprises a plurality of distinct trust engines 1305, 1310, 1315, and 1320, respectively. To facilitate a more complete understanding of the invention, FIGURE 13 illustrates each trust engine, 1305, 1310, 1315, and 1320 as having a transaction engine, a depository, and an authentication engine. However, a skilled artisan will recognize that each transaction engine may advantageously comprise some, a combination, or all of the elements and communication channels disclosed with reference to FIGURES 1-8. For example, one embodiment may advantageously include trust engines having one or more transaction engines, depositories, and cryptographic servers or any combinations thereof.

[0209] According to one embodiment of the invention, each of the trust engines 1305, 1310, 1315 and 1320 are geographically separated, such that, for example, the trust engine 1305 may reside in a first location, the trust engine 1310 may reside in a second location, the trust engine 1315 may reside in a third location, and the trust engine 1320 may reside in a fourth location. The foregoing geographic separation advantageously decreases system response time while increasing the security of the overall trust engine system 1300.

[0210] For example, when a user logs onto the cryptographic system 100, the user may be nearest the first location and may desire to be authenticated. As described with reference to FIGURE 10, to be authenticated, the user provides current authentication data, such as a biometric or the like, and the current authentication data is compared to that user's enrollment authentication data. Therefore, according to one example, the user advantageously provides current authentication data to the geographically nearest trust engine 1305. The transaction engine 1321 of the trust engine 1305 then forwards the current authentication data to the authentication engine 1322 also residing at the first location. According to another embodiment, the transaction engine 1321 forwards the current authentication data to one or more of the authentication engines of the trust engines 1310, 1315, or 1320.

[0211] The transaction engine 1321 also requests the assembly of the enrollment authentication data from the depositories of, for example, each of the trust engines, 1305 through 1320. According to this embodiment, each depository provides its portion of the enrollment authentication data to the authentication engine 1322 of the trust engine 1305. The authentication engine 1322 then employs the encrypted data portions from, for example, the first two depositories to respond, and assembles the enrollment authentication data into deciphered form. The authentication engine 1322 compares the enrollment authentication data with the current authentication data and returns an authentication result to the transaction engine 1321 of the trust engine 1305.

[0212] Based on the above, the trust engine system 1300 employs the nearest one of a plurality of geographically separated trust engines, 1305 through 1320, to perform the authentication process. According to one embodiment of the invention, the routing of information to the nearest transaction engine may advantageously be performed at client-side applets executing on one or more of the user system 105, vendor system 120, or certificate authority 115. According to an alternative embodiment, a more sophisticated decision process may be employed to select from the trust engines 1305 through 1320. For example, the decision may be based on the availability, operability, speed of connections, load, performance, geographic proximity, or a combination thereof, of a given trust engine.

[0213] In this way, the trust engine system 1300 lowers its response time while maintaining the security advantages associated with geographically remote data storage facilities, such as those discussed with reference to FIGURE 7 where each data storage facility stores randomized portions of sensitive data. For example, a security compromise at, for example, the depository 1325 of the trust engine 1315 does not necessarily compromise the sensitive data of the trust engine system 1300. This is because the depository 1325 contains only non-decipherable randomized data that, without more, is entirely useless.

[0214] According to another embodiment, the trust engine system 1300 may advantageously include multiple cryptographic engines arranged similar to the authentication engines. The cryptographic engines may advantageously perform cryptographic functions such as those disclosed with reference to FIGURES 1-8. According to yet another embodiment, the trust engine system 1300 may advantageously replace the multiple authentication engines with multiple cryptographic engines, thereby performing cryptographic functions such as those disclosed with reference to FIGURES 1-8. According to yet another embodiment of the invention, the trust engine system 1300 may replace each multiple authentication engine with an engine having some or all of the functionality of the authentication engines, cryptographic engines, or both, as disclosed in the foregoing,

[0215] Although the trust engine system 1300 is disclosed with reference to its preferred and alternative embodiments, a skilled artisan will recognize that the trust engine system 1300 may comprise portions of trust engines 1305 through 1320. For example, the trust engine system 1300 may include one or more transaction engines, one or more depositories, one or more authentication engines, or one or more cryptographic engines or combinations thereof.

[0216] FIGURE 14 illustrates a simplified block diagram of a trust engine System 1400 according to aspects of yet another embodiment of the invention. As shown in FIGURE 14, the trust engine system 1400 includes multiple trust engines 1405, 1410, 1415 and 1420. According to one embodiment, each of the trust engines 1405, 1410, 1415 and 1420, comprise some or all of the elements of trust engine 110 disclosed with reference to FIGURES 1-8. According to this

embodiment, when the client side applets of the user system 105, the vendor system 120, or the certificate authority 115, communicate with the trust engine system 1400, those communications are sent to the IP address of each of the trust engines 1405 through 1420. Further, each transaction engine of each of the trust engines, 1405, 1410, 1415, and 1420, behaves similar to the transaction engine 1321 of the trust engine 1305 disclosed with reference to FIGURE 13. For example, during an authentication process, each transaction engine of each of the trust engines 1405, 1410, 1415, and 1420 transmits the current authentication data to their respective authentication engines and transmits a request to assemble the randomized data stored in each of the depositories of each of the trust engines 1405 through 1420. FIGURE 14 does not illustrate all of these communications; as such illustration would become overly complex. Continuing with the authentication process, each of the depositories then communicates its portion of the randomized data to each of the authentication engines of the each of the trust engines 1405 through 1420. Each of the authentication engines of the each of the trust engines employs its comparator to determine whether the current authentication data matches the enrollment authentication data provided by the depositories of each of the trust engines 1405 through 1420. According to this embodiment, the result of the comparison by each of the authentication engines is then transmitted to a redundancy module of the other three trust engines. For example, the result of the authentication engine from the trust engine 1405 is transmitted to the redundancy modules of the trust engines 1410, 1415, and 1420. Thus, the redundancy module of the trust engine 1405 likewise receives the result of the authentication engines from the trust engines 1410, 1415, and 1420.

[0217] FIGURE 15 illustrates a block diagram of the redundancy module of FIGURE 14. The redundancy module comprises a comparator configured to receive the authentication result from three authentication engines and transmit that result to the transaction engine of the fourth trust engine. The comparator compares the authentication result form the three authentication engines, and if two of the results agree, the comparator concludes that the authentication result should match that of the two agreeing authentication engines. This result is then

transmitted back to the transaction engine corresponding to the trust engine not associated with the three authentication engines.

[0218] Based on the foregoing, the redundancy module determines an authentication result from data received from authentication engines that are preferably geographically remote from the trust engine of that the redundancy module. By providing such redundancy functionality, the trust engine system 1400 ensures that a compromise of the authentication engine of one of the trust engines 1405 through 1420, is insufficient to compromise the authentication result of the redundancy module of that particular trust engine. A skilled artisan will recognize that redundancy module functionality of the trust engine system 1400 may also be applied to the cryptographic engine of each of the trust engines 1405 through 1420. However, such cryptographic engine communication was not shown in FIGURE 14 to avoid complexity. Moreover, a skilled artisan will recognize a wide number of alternative authentication result conflict resolution algorithms for the comparator of FIGURE 15 are suitable for use in the present invention.

[0219] According to yet another embodiment of the invention, the trust engine system 1400 may advantageously employ the redundancy module during cryptographic comparison steps. For example, some or all of the foregoing redundancy module disclosure with reference to FIGURES 14 and 15 may advantageously be implemented during a hash comparison of documents provided by one or more parties during a particular transaction.

[0220] Although the foregoing invention has been described in terms of certain preferred and alternative embodiments, other embodiments will be apparent to those of ordinary skill in the art from the disclosure herein. For example, the trust engine 110 may issue short-term certificates, where the private cryptographic key is released to the user for a predetermined period of time. For example, current certificate standards include a validity field that can be set to expire after a predetermined amount of time. Thus, the trust engine 110 may release a private key to a user where the private key would be valid for, for example, 24 hours. According to such an embodiment, the trust engine 110 may advantageously issue a new cryptographic key pair to be associated with a particular user and then release the private key of the new cryptographic key pair. Then, once the private

cryptographic key is released, the trust engine 110 immediately expires any internal valid use of such private key, as it is no longer securable by the trust engine 110.

[0221] In addition, a skilled artisan will recognize that the cryptographic system 100 or the trust engine 110 may include the ability to recognize any type of devices, such as, but not limited to, a laptop, a cell phone, a network, a biometric device or the like. According to one embodiment, such recognition may come from data supplied in the request for a particular service, such as, a request for authentication leading to access or use, a request for cryptographic functionality, or the like. According to one embodiment, the foregoing request may include a unique device identifier, such as, for example, a processor ID. Alternatively, the request may include data in a particular recognizable data format. For example, mobile and satellite phones often do not include the processing power for full X509.v3 heavy encryption certificates, and therefore do not request them. According to this embodiment, the trust engine 110 may recognize the type of data format presented, and respond only in kind.

[0222] In an additional aspect of the system described above, context sensitive authentication can be provided using various techniques as will be described below. Context sensitive authentication, for example as shown in FIGURE 16, provides the possibility of evaluating not only the actual data which is sent by the user when attempting to authenticate himself, but also the circumstances surrounding the generation and delivery of that data. Such techniques may also support transaction specific trust arbitrage between the user and trust engine 110 or between the vendor and trust engine 110, as will be described below.

[0223] As discussed above, authentication is the process of proving that a user is who he says he is. Generally, authentication requires demonstrating some fact to an authentication authority. The trust engine 110 of the present invention represents the authority to which a user must authenticate himself. The user must demonstrate to the trust engine 110 that he is who he says he is by either: knowing something that only the user should know (knowledge-based authentication), having something that only the user should have (token-based authentication), or by being something that only the user should be (biometric-based authentication).

[0224] Examples of knowledge-based authentication include without limitation a password, PIN number, or lock combination. Examples of token-based authentication include without limitation a house key, a physical credit card, a driver's license, or a particular phone number. Examples of biometric-based authentication include without limitation a fingerprint, handwriting analysis, facial scan, hand scan, ear scan, iris scan, vascular pattern, DNA, a voice analysis, or a retinal scan.

[0225] Each type of authentication has particular advantages and disadvantages, and each provides a different level of security. For example, it is generally harder to create a false fingerprint that matches someone else's than it is to overhear someone's password and repeat it. Each type of authentication also requires a different type of data to be known to the authenticating authority in order to verify someone using that form of authentication.

[0226] As used herein, "authentication" will refer broadly to the overall process of verifying someone's identity to be who he says he is. An "authentication technique" will refer to a particular type of authentication based upon a particular piece of knowledge, physical token, or biometric reading. "Authentication data" refers to information which is sent to or otherwise demonstrated to an authentication authority in order to establish identity. "Enrollment data" will refer to the data which is initially submitted to an authentication authority in order to establish a baseline for comparison with authentication data. An "authentication instance" will refer to the data associated with an attempt to authenticate by an authentication technique.

[0227] The internal protocols and communications involved in the process of authenticating a user is described with reference to FIGURE 10 above. The part of this process within which the context sensitive authentication takes place occurs within the comparison step shown as step 1045 of FIGURE 10. This step takes place within the authentication engine 215 and involves assembling the enrollment data 410 retrieved from the depository 210 and comparing the authentication data provided by the user to it. One particular embodiment of this process is shown in FIGURE 16 and described below.

[0228] The current authentication data provided by the user and the enrollment data retrieved from the depository 210 are received by the authentication engine 215 in step 1600 of FIGURE 16. Both of these sets of data may contain data which is related to separate techniques of authentication. The authentication engine 215 separates the authentication data associated with each individual authentication instance in step 1605. This is necessary so that the authentication data is compared with the appropriate subset of the enrollment data for the user (e.g. fingerprint authentication data should be compared with fingerprint enrollment data, rather than password enrollment data).

[0229] Generally, authenticating a user involves one or more individual authentication instances, depending on which authentication techniques are available to the user. These methods are limited by the enrollment data which were provided by the user during his enrollment process (if the user did not provide a retinal scan when enrolling, he will not be able to authenticate himself using a retinal scan), as well as the means which may be currently available to the user (e.g. if the user does not have a fingerprint reader at his current location, fingerprint authentication will not be practical). In some cases, a single authentication instance may be sufficient to authenticate a user; however, in certain circumstances a combination of multiple authentication instances may be used in order to more confidently authenticate a user for a particular transaction.

[0230] Each authentication instance consists of data related to a particular authentication technique (e.g. fingerprint, password, smart card, etc.) and the circumstances which surround the capture and delivery of the data for that particular technique. For example, a particular instance of attempting to authenticate via password will generate not only the data related to the password itself, but also circumstantial data, known as "metadata", related to that password attempt. This circumstantial data includes information such as: the time at which the particular authentication instance took place, the network address from which the authentication information was delivered, as well as any other information as is known to those of skill in the art which may be determined about the origin of the authentication data (the type of connection, the processor serial number, etc.).

[0231] In many cases, only a small amount of circumstantial metadata will be available. For example, if the user is located on a network which uses proxies or network address translation or another technique which masks the address of the originating computer, only the address of the proxy or router may be determined. Similarly, in many cases information such as the processor serial number will not be available because of either limitations of the hardware or operating system being used, disabling of such features by the operator of the system, or other limitations of the connection between the user's system and the trust engine 110.

[0232] As shown in FIGURE 16, once the individual authentication instances represented within the authentication data are extracted and separated in step 1605, the authentication engine 215 evaluates each instance for its reliability in indicating that the user is who he claims to be. The reliability for a single authentication instance will generally be determined based on several factors. These may be grouped as factors relating to the reliability associated with the authentication technique, which are evaluated in step 1610, and factors relating to the reliability of the particular authentication data provided, which are evaluated in step 1815. The first group includes without limitation the inherent reliability of the authentication technique being used, and the reliability of the enrollment data being used with that method. The second group includes without limitation the degree of match between the enrollment data and the data provided with the authentication instance, and the metadata associated with that authentication instance. Each of these factors may vary independently of the others.

[0233] The inherent reliability of an authentication technique is based on how hard it is for an imposter to provide someone else's correct data, as well as the overall error rates for the authentication technique. For passwords and knowledge based authentication methods, this reliability is often fairly low because there is nothing that prevents someone from revealing their password to another person and for that second person to use that password. Even a more complex knowledge based system may have only moderate reliability since knowledge may be transferred from person to person fairly easily. Token based authentication, such as having a proper smart card or using a particular terminal to perform the

authentication, is similarly of low reliability used by itself, since there is no guarantee that the right person is in possession of the proper token.

[0234] However, biometric techniques are more inherently reliable because it is generally difficult to provide someone else with the ability to use your fingerprints in a convenient manner, even intentionally. Because subverting biometric authentication techniques is more difficult, the inherent reliability of biometric methods is generally higher than that of purely knowledge or token based authentication techniques. However, even biometric techniques may have some occasions in which a false acceptance or false rejection is generated. These occurrences may be reflected by differing reliabilities for different implementations of the same biometric technique. For example, a fingerprint matching system provided by one company may provide a higher reliability than one provided by a different company because one uses higher quality optics or a better scanning resolution or some other improvement which reduces the occurrence of false acceptances or false rejections.

[0235] Note that this reliability may be expressed in different manners. The reliability is desirably expressed in some metric which can be used by the heuristics 530 and algorithms of the authentication engine 215 to calculate the confidence level of each authentication. One preferred mode of expressing these reliabilities is as a percentage or fraction. For instance, fingerprints might be assigned an inherent reliability of 97%, while passwords might only be assigned an inherent reliability of 50%. Those of skill in the art will recognize that these particular values are merely exemplary and may vary between specific implementations.

[0236] The second factor for which reliability must be assessed is the reliability of the enrollment. This is part of the "graded enrollment" process referred to above. This reliability factor reflects the reliability of the identification provided during the initial enrollment process. For instance, if the individual initially enrolls in a manner where they physically produce evidence of their identity to a notary or other public official, and enrollment data is recorded at that time and notarized, the data will be more reliable than data which is provided over a network during

enrollment and only vouched for by a digital signature or other information which is not truly tied to the individual.

[0237] Other enrollment techniques with varying levels of reliability include without limitation: enrollment at a physical office of the trust engine 110 operator; enrollment at a user's place of employment; enrollment at a post office or passport office; enrollment through an affiliated or trusted party to the trust engine 110 operator; anonymous or pseudonymous enrollment in which the enrolled identity is not yet identified with a particular real individual, as well as such other means as are known in the art.

[0238] These factors reflect the trust between the trust engine 110 and the source of identification provided during the enrollment process. For instance, if enrollment is performed in association with an employer during the initial process of providing evidence of identity, this information may be considered extremely reliable for purposes within the company, but may be trusted to a lesser degree by a government agency, or by a competitor. Therefore, trust engines operated by each of these other organizations may assign different levels of reliability to this enrollment.

[0239] Similarly, additional data which is submitted across a network, but which is authenticated by other trusted data provided during a previous enrollment with the same trust engine 110 may be considered as reliable as the original enrollment data was, even though the latter data were submitted across an open network. In such circumstances, a subsequent notarization will effectively increase the level of reliability associated with the original enrollment data. In this way for example, an anonymous or pseudonymous enrollment may then be raised to a full enrollment by demonstrating to some enrollment official the identity of the individual matching the enrolled data.

[0240] The reliability factors discussed above are generally values which may be determined in advance of any particular authentication instance. This is because they are based upon the enrollment and the technique, rather than the actual authentication. In one embodiment, the step of generating reliability based upon these factors involves looking up previously determined values for this particular authentication technique and the enrollment data of the user. In a further aspect of

an advantageous embodiment of the present invention, such reliabilities may be included with the enrollment data itself. In this way, these factors are automatically delivered to the authentication engine 215 along with the enrollment data sent from the depository 210.

[0241] While these factors may generally be determined in advance of any individual authentication instance, they still have an effect on each authentication instance which uses that particular technique of authentication for that user. Furthermore, although the values may change over time (e.g. if the user re-enrolls in a more reliable fashion), they are not dependent on the authentication data itself. By contrast, the reliability factors associated with a single specific instance's data may vary on each occasion. These factors, as discussed below, must be evaluated for each new authentication in order to generate reliability scores in step 1815.

[0242] The reliability of the authentication data reflects the match between the data provided by the user in a particular authentication instance and the data provided during the authentication enrollment. This is the fundamental question of whether the authentication data matches the enrollment data for the individual the user is claiming to be. Normally, when the data do not match, the user is considered to not be successfully authenticated, and the authentication fails. The manner in which this is evaluated may change depending on the authentication technique used. The comparison of such data is performed by the comparator 515 function of the authentication engine 215 as shown in FIGURE 5.

[0243] For instance, matches of passwords are generally evaluated in a binary fashion. In other words, a password is either a perfect match, or a failed match. It is usually not desirable to accept as even a partial match a password which is close to the correct password if it is not exactly correct. Therefore, when evaluating a password authentication, the reliability of the authentication returned by the comparator 515 is typically either 100% (correct) or 0% (wrong), with no possibility of intermediate values.

[0244] Similar rules to those for passwords are generally applied to token based authentication methods, such as smart cards. This is because having a smart card which has a similar identifier or which is similar to the correct one, is still just as

wrong as having any other incorrect token. Therefore tokens tend also to be binary authenticators: a user either has the right token, or he doesn't.

[0245] However, certain types of authentication data, such as questionnaires and biometrics, are generally not binary authenticators. For example, a fingerprint may match a reference fingerprint to varying degrees. To some extent, this may be due to variations in the quality of the data captured either during the initial enrollment or in subsequent authentications. (A fingerprint may be smudged or a person may have a still healing scar or burn on a particular finger.) In other instances the data may match less than perfectly because the information itself is somewhat variable and based upon pattern matching. (A voice analysis may seem close but not quite right because of background noise, or the acoustics of the environment in which the voice is recorded, or because the person has a cold.) Finally, in situations where large amounts of data are being compared, it may simply be the case that much of the data matches well, but some doesn't. (A ten-question questionnaire may have resulted in eight correct answers to personal questions, but two incorrect answers.) For any of these reasons, the match between the enrollment data and the data for a particular authentication instance may be desirably assigned a partial match value by the comparator 515. In this way, the fingerprint might be said to be a 85% match, the voice print a 65% match, and the questionnaire an 80% match, for example.

[0246] This measure (degree of match) produced by the comparator 515 is the factor representing the basic issue of whether an authentication is correct or not. However, as discussed above, this is only one of the factors which may be used in determining the reliability of a given authentication instance. Note also that even though a match to some partial degree may be determined, that ultimately, it may be desirable to provide a binary result based upon a partial match. In an alternate mode of operation, it is also possible to treat partial matches as binary, i.e. either perfect (100%) or failed (0%) matches, based upon whether or not the degree of match passes a particular threshold level of match. Such a process may be used to provide a simple pass/fail level of matching for systems which would otherwise produce partial matches.

[0247] Another factor to be considered in evaluating the reliability of a given authentication instance concerns the circumstances under which the authentication data for this particular instance are provided. As discussed above, the circumstances refer to the metadata associated with a particular authentication instance. This may include without limitation such information as: the network address of the authenticator, to the extent that it can be determined; the time of the authentication; the mode of transmission of the authentication data (phone line, cellular, network, etc.); and the serial number of the system of the authenticator.

[0248] These factors can be used to produce a profile of the type of authentication that is normally requested by the user. Then, this information can be used to assess reliability in at least two manners. One manner is to consider whether the user is requesting authentication in a manner which is consistent with the normal profile of authentication by this user. If the user normally makes authentication requests from one network address during business days (when she is at work) and from a different network address during evenings or weekends (when she is at home), an authentication which occurs from the home address during the business day is less reliable because it is outside the normal authentication profile. Similarly, if the user normally authenticates using a fingerprint biometric and in the evenings, an authentication which originates during the day using only a password is less reliable.

[0249] An additional way in which the circumstantial metadata can be used to evaluate the reliability of an instance of authentication is to determine how much corroboration the circumstance provides that the authenticator is the individual he claims to be. For instance, if the authentication comes from a system with a serial number known to be associated with the user, this is a good circumstantial indicator that the user is who they claim to be. Conversely, if the authentication is coming from a network address which is known to be in Los Angeles when the user is known to reside in London, this is an indication that this authentication is less reliable based on its circumstances.

[0250] It is also possible that a cookie or other electronic data may be placed upon the system being used by a user when they interact with a vendor system or with the trust engine 110. This data is written to the storage of the system of the

user and may contain an identification which may be read by a Web browser or other software on the user system. If this data is allowed to reside on the user system between sessions (a "persistent cookie"), it may be sent with the authentication data as further evidence of the past use of this system during authentication of a particular user. In effect, the metadata of a given instance, particularly a persistent cookie, may form a sort of token based authenticator itself.

[0251] Once the appropriate reliability factors based on the technique and data of the authentication instance are generated as described above in steps 1610 and 1615 respectively, they are used to produce an overall reliability for the authentication instance provided in step 1620. One means of doing this is simply to express each reliability as a percentage and then to multiply them together.

[0252] For example, suppose the authentication data is being sent in from a network address known to be the user's home computer completely in accordance with the user's past authentication profile (100%), and the technique being used is fingerprint identification (97%), and the initial finger print data was roistered through the user's employer with the trust engine 110 (90%), and the match between the authentication data and the original fingerprint template in the enrollment data is very good (99%). The overall reliability of this authentication instance could then be calculated as the product of these reliabilities: 100% * 97% * 90% * 99% - 86.4% reliability.

[0253] This calculated reliability represents the reliability of one single instance of authentication. The overall reliability of a single authentication instance may also be calculated using techniques which treat the different reliability factors differently, for example by using formulas where different weights are assigned to each reliability factor. Furthermore, those of skill in the art will recognize that the actual values used may represent values other than percentages and may use non-arithmetic systems. One embodiment may include a module used by an authentication requestor to set the weights for each factor and the algorithms used in establishing the overall reliability of the authentication instance.

[0254] The authentication engine 215 may use the above techniques and variations thereof to determine the reliability of a single authentication instance, indicated as step 1620. However, it may be useful in many authentication

situations for multiple authentication instances to be provided at the same time. For example, while attempting to authenticate himself using the system of the present invention, a user may provide a user identification, fingerprint authentication data, a smart card, and a password. In such a case, three independent authentication instances are being provided to the trust engine 110 for evaluation. Proceeding to step 1625, if the authentication engine 215 determines that the data provided by the user includes more than one authentication instance, then each instance in turn will be selected as shown in step 1630 and evaluated as described above in steps 1610, 1615 and 1620.

[0255] Note that many of the reliability factors discussed may vary from one of these instances to another. For instance, the inherent reliability of these techniques is likely to be different, as well as the degree of match provided between the authentication data and the enrollment data. Furthermore, the user may have provided enrollment data at different times and under different circumstances for each of these techniques, providing different enrollment reliabilities for each of these instances as well. Finally, even though the circumstances under which the data for each of these instances is being submitted is the same, the use of such techniques may each fit the profile of the user differently, and so may be assigned different circumstantial reliabilities. (For example, the user may normally use their password and fingerprint, but not their smart card.)

[0256] As a result, the final reliability for each of these authentication instances may be different from One another. However, by using multiple instances together, the overall confidence level for the authentication will tend to increase.

[0257] Once the authentication engine has performed steps 1610 through 1620 for all of the authentication instances provided in the authentication data, the reliability of each instance is used in step 1635 to evaluate the overall authentication confidence level. This process of combining the individual authentication instance reliabilities into the authentication confidence level may be modeled by various methods relating the individual reliabilities produced, and may also address the particular interaction between some of these authentication techniques. (For example, multiple knowledge-based systems such as passwords

may produce less confidence than a single password and even a fairly weak biometric, such as a basic voice analysis.)

[0258] One means in which the authentication engine 215 may combine the reliabilities of multiple concurrent authentication instances to generate a final confidence level is to multiply the unreliability of each instance to arrive at a total unreliability. The unreliability is generally the complementary percentage of the reliability. For example, a technique which is 84% reliable is 16% unreliable. The three authentication instances described above (fingerprint, smart card, password)which produce reliabilities of 86%, 75%, and 72% would have corresponding unreliabilities of (100- 86)%, (100- 75)% and (100- 72)%, or 14%, 25%, and 28%, respectively. By multiplying these unreliabilities, we get a cumulative unreliability of 14% * 25% * 28% - .98% unreliability, which corresponds to a reliability of 99.02%.

[0259] In an additional mode of operation, additional factors and heuristics 530 may be applied within the authentication engine 215 to account for the interdependence of various authentication techniques. For example, if someone has unauthorized access to a particular home computer, they probably have access to the phone line at that address as well. Therefore, authenticating based on an originating phone number as well as upon the serial number of the authenticating system does not add much to the overall confidence in the authentication. However, knowledge based authentication is largely independent of token based authentication (i.e. if someone steals your cellular phone or keys, they are no more likely to know your PIN or password than if they hadn't).

[0260] Furthermore, different vendors or other authentication requestors may wish to weigh different aspects of the authentication differently. This may include the use of separate weighing factors or algorithms used in calculating the reliability of individual instances as well as the use of different means to evaluate authentication events with multiple instances.

[0261] For instance, vendors for certain types of transactions, for instance corporate email systems, may desire to authenticate primarily based upon heuristics and other circumstantial data by default. Therefore, they may apply high weights to factors related to the metadata and other profile related information

associated with the circumstances surrounding authentication events. This arrangement could be used to ease the burden on users during normal operating hours, by not requiring more from the user than that he be logged on to the correct machine during business hours. However, another vendor may weigh authentications coming from a particular technique most heavily, for instance fingerprint matching, because of a policy decision that such a technique is most suited to authentication for the particular vendor's purposes.

[0262] Such varying weights may be defined by the authentication requestor in generating the authentication request and sent to the trust engine 110 with the authentication request in one mode of operation. Such options could also be set as preferences during an initial enrollment process for the authentication requestor and stored within the authentication engine in another mode of operation.

[0263] Once the authentication engine 215 produces an authentication confidence level for the authentication data provided, this confidence level is used to complete the authentication request in step 1640, and this information is forwarded from the authentication engine 215 to the transaction engine 205 for inclusion in a message to the authentication requestor.

[0264] The process described above is merely exemplary, and those of skill in the art will recognize that the steps need not be performed in the order shown or that only certain of the steps are desired to be performed, or that a variety of combinations of steps may be desired. Furthermore, certain steps, such as the evaluation of the reliability of each authentication instance provided, may be carried out in parallel with one another if circumstances permit.

[0265] In a further aspect of this invention, a method is provided to accommodate conditions when the authentication confidence level produced by the process described above fails to meet the required trust level of the vendor or other party requiring the authentication. In circumstances such as these where a gap exists between the level of confidence provided and the level of trust desired, the operator of the trust engine 110 is in a position to provide opportunities for one or both parties to provide alternate data or requirements in order to close this trust gap. This process will be referred to as "trust arbitrage" herein.

[0266] Trust arbitrage may take place within a framework of cryptographic authentication as described above with reference to FIGURES 10 and 11. As shown therein, a vendor or other party will request authentication of a particular user in association with a particular transaction. In one circumstance, the vendor simply requests an authentication, either positive or negative, and after receiving appropriate data from the user, the trust engine 110 will provide such a binary authentication. In circumstances such as these, the degree of confidence required in order to secure a positive authentication is determined based upon preferences set within the trust engine 110.

[0267] However, it is also possible that the vendor may request a particular level of trust in order to complete a particular transaction. This required level may be included with the authentication request (e.g. authenticate this user to 98% confidence) or may be determined by the trust engine 110 based on other factors associated with the transaction (i.e. authenticate this user as appropriate for this transaction). One such factor might be the economic value of the transaction. For transactions which have greater economic value, a higher degree of trust may be required. Similarly, for transactions with high degrees of risk a high degree of trust may be required. Conversely, for transactions which are either of low risk or of low value, lower trust levels may be required by the vendor or other authentication requestor.

[0268] The process of trust arbitrage occurs between the steps of the trust engine 110 receiving the authentication data in step 1050 of FIGURE 10 and the return of an authentication result to the vendor in step 1055 of FIGURE 10. Between these steps, the process which leads to the evaluation of trust levels and the potential trust arbitrage occurs as shown in FIGURE 17. In circumstances where simple binary authentication is performed, the process shown in FIGURE 17 reduces to having the transaction engine 205 directly compare the authentication data provided with the enrollment data for the identified user as discussed above with reference to FIGURE 10, flagging any difference as a negative authentication.

[0269] As shown in FIGURE 17, the first step after receiving the data in step 1050 is for the transaction engine 205 to determine the trust level which is required for a positive authentication for this particular transaction in step 1710. This step

may be performed by one of several different methods. The required trust level may be specified to the trust engine 110 by the authentication requestor at the time when the authentication request is made. The authentication requestor may also set a preference in advance which is stored within the depository 210 or other storage which is accessible by the transaction engine 205. This preference may then be read and used each time an authentication request is made by this authentication requestor. The preference may also be associated with a particular user as a security measure such that a particular level of trust is always required in order to authenticate that user, the user preference being stored in the depository 210 or other storage media accessible by the transaction engine 205. The required level may also be derived by the transaction engine 205 or authentication engine 215 based upon information provided in the authentication request, such as the value and risk level of the transaction to be authenticated.

[0270] In one mode of operation, a policy management module or other software which is used when generating the authentication request is used to specify the required degree of trust for the authentication of the transaction. This may be used to provide a series of rules to follow when assigning the required level of trust based upon the policies which are specified within the policy management module. One advantageous mode of operation is for such a module to be incorporated with the web server of a vendor in order to appropriately determine required level of trust for transactions initiated with the vendor's web server. In this way, transaction requests from users may be assigned a required trust level in accordance with the policies of the vendor and such information may be forwarded to the trust engine 110 along with the authentication request.

[0271] This required trust level correlates with the degree of certainty that the vendor wants to have that the individual authenticating is in fact who he identifies himself as. For example, if the transaction is one where the vendor wants a fair degree of certainty because goods are changing hands, the vendor may require a trust level of 85%. For situation where the vendor is merely authenticating the user to allow him to view members only content or exercise privileges on a chat room, the downside risk may be small enough that the vendor requires only a 60% trust

level. However, to enter into a production contract with a value of tens of thousands of dollars, the vendor may require a trust level of 99% or more.

[0272] This required trust level represents a metric to which the user must authenticate himself in order to complete the transaction. If the required trust level is 85% for example, the user must provide authentication to the trust engine 110 sufficient for the trust engine 110 to say with 85% confidence that the user is who they say they are. It is the balance between this required trust level and the authentication confidence level which produces either a positive authentication (to the satisfaction of the vendor) or a possibility of trust arbitrage.

[0273] As shown in FIGURE 17, after the transaction engine 205 receives the required trust level, it compares in step 1720 the required trust level to the authentication confidence level which the authentication engine 215 calculated for the current authentication (as discussed with reference to FIGURE 16). If the authentication confidence level is higher than the required trust level for the transaction in step 1730, then the process moves to step 1740 where a positive authentication for this transaction is produced by the transaction engine 205. A message to this effect will then be inserted into the authentication results and returned to the vendor by the transaction engine 205 as shown in step 1055 (see FIGURE 10).

[0274] However, if the authentication confidence level does not fulfill the required trust level in step 1730, then a confidence gap exists for the current authentication, and trust arbitrage is conducted in step 1750. Trust arbitrage is described more completely with reference to FIGURE 18 below. This process as described below takes place within the transaction engine 205 of the trust engine 110. Because no authentication or other cryptographic operations are needed to execute trust arbitrage (other than those required for the SSL communication between the transaction engine 205 and other components), the process may be performed outside the authentication engine 215. However, as will be discussed below, any reevaluation of authentication data or other cryptographic or authentication events will require the transaction engine 205 to resubmit the appropriate data to the authentication engine 215. Those of skill in the art will

recognize that the trust arbitrage process could alternately be structured to take place partially or entirely within the authentication engine 215 itself.

[0275] As mentioned above, trust arbitrage is a process where the trust engine 110 mediates a negotiation between the vendor and user in an attempt to secure a positive authentication where appropriate. As shown in step 1805, the transaction engine 205 first determines whether or not the current situation is appropriate for trust arbitrage. This may be determined based upon the circumstances of the authentication, e.g. whether this authentication has already been through multiple cycles of arbitrage, as well as upon the preferences of either the vendor or user, as will be discussed further below.

[0276] In such circumstances where arbitrage is not possible, the process proceeds to step 1810 where the transaction engine 205 generates a negative authentication and then inserts it into the authentication results which are sent to the vendor in step 1055 (see FIGURE 10). One limit which may be advantageously used to prevent authentications from pending indefinitely is to set a time-out period from the initial authentication request. In this way, any transaction which is not positively authenticated within the time limit is denied further arbitrage and negatively authenticated. Those of skill in the art will recognize that such a time limit may vary depending upon the circumstances of the transaction and the desires of the user and vendor. Limitations may also be placed upon the number of attempts that may be made at providing a successful authentication. Such limitations may be handled by an attempt limiter 535 as shown in FIGURE 5.

[0277] If arbitrage is not prohibited in step 1805, the transaction engine 205 will then engage in negotiation with one or both of the transacting parties. The transaction engine 205 may send a message to the user requesting some form of additional authentication in order to boost the authentication confidence level produced as shown in step 1820. In the simplest form, this may simply indicates that authentication was insufficient. A request to produce one or more additional authentication instances to improve the overall confidence level of the authentication may also be sent.

[0278] If the user provides some additional authentication instances in step 1825, then the transaction engine 205 adds these authentication instances to the

authentication data for the transaction and forwards it to the authentication engine 215 as shown in step 1015 (see FIGURE 10), and the authentication is reevaluated based upon both the pre-existing authentication instances for this transaction and the newly provided authentication instances.

[0279] An additional type of authentication may be a request from the trust engine 110 to make some form of person-to-person contact between the trust engine 110 operator (or a trusted associate) and the user, for example, by phone call. This phone call or other non-computer authentication can be used to provide personal contact with the individual and also to conduct some form of questionnaire based authentication. This also may give the opportunity to verify an originating telephone number and potentially a voice analysis of the user when he calls in. Even if no additional authentication data can be provided, the additional context associated with the user's phone number may improve the reliability of the authentication context. Any revised data or circumstances based upon this phone call are fed into the trust engine 110 for use in consideration of the authentication request.

[0280] Additionally, in step 1820 the trust engine 110 may provide an opportunity for the user to purchase insurance, effectively buying a more confident authentication. The operator of the trust engine 110 may, at times, only want to make such an option available if the confidence level of the authentication is above a certain threshold to begin with. In effect, this user side insurance is a way for the trust engine 110 to vouch for the user when the authentication meets the normal required trust level of the trust engine 110 for authentication, but does not meet the required trust level of the vendor for this transaction. In this way, the user may still successfully authenticate to a very high level as may be required by the vendor, even though he only has authentication instances which produce confidence sufficient for the trust engine 110.

[0281] This function of the trust engine 110 allows the trust engine 110 to vouch for someone who is authenticated to the satisfaction of the trust engine 110, but not of the vendor. This is analogous to the function performed by a notary in adding his signature to a document in order to indicate to someone reading the document at a later time that the person whose signature appears on the document is in fact

the person who signed it. The signature of the notary testifies to the act of signing by the user. In the same way, the trust engine is providing an indication that the person transacting is who they say they are.

[0282] However, because the trust engine 110 is artificially boosting the level of confidence provided by the user, there is a greater risk to the trust engine 110 operator, since the user is not actually meeting the required trust level of the vendor. The cost of the insurance is designed to offset the risk of a false positive authentication to the trust engine 110 (who may be effectively notarizing the authentications of the user). The user pays the trust engine 110 operator to take the risk of authenticating to a higher level of confidence than has actually been provided.

[0283] Because such an insurance system allows someone to effectively buy a higher confidence rating from the trust engine 110, both vendors and users may wish to prevent the use of user side insurance in certain transactions. Vendors may wish to limit positive authentications to circumstances where they know that actual authentication data supports the degree of confidence which they require and so may indicate to the trust engine 110 that user side insurance is not to be allowed. Similarly, to protect his online identity, a user may wish to prevent the use of user side insurance on his account, or may wish to limit its use to situations where the authentication confidence level without the insurance is higher than a certain limit. This may be used as a security measure to prevent someone from overhearing a password or stealing a smart card and using them to falsely authenticate to a low level of confidence, and then purchasing insurance to produce a very high level of (false) confidence. These factors may be evaluated in determining whether user side insurance is allowed.

[0284] If user purchases insurance in step 1840, then the authentication confidence level is adjusted based upon the insurance purchased in step 1845, and the authentication confidence level and required trust level are again compared in step 1730 (see FIGURE 17). The process continues from there, and may lead to either a positive authentication in step 1740 (see FIGURE 17), or back into the trust arbitrage process in step 1750 for either further arbitrage (if allowed) or a negative authentication in step 1810 if further arbitrage is prohibited.

[0285] In addition to sending a message to the user in step 1820, the transaction engine 205 may also send a message to the vendor in step 1830 which indicates that a pending authentication is currently below the required trust level. The message may also offer various options on how to proceed to the vendor. One of these Options is to simply inform the vendor of what the current authentication confidence level is and ask if the vendor wishes to maintain their current unfulfilled required trust level. This may be beneficial because in some cases, the vendor may have independent means for authenticating the transaction or may have been using a default set of requirements which generally result in a higher required level being initially specified than is actually needed for the particular transaction at hand.

[0286] For instance, it may be standard practice that all incoming purchase order transactions with the vendor are expected to meet a 98% trust level. However, if an order was recently discussed by phone between the vendor and a long-standing customer, and immediately thereafter the transaction is authenticated, but only to a 93% confidence level, the vendor may wish to simply lower the acceptance threshold for this transaction, because the phone call effectively provides additional authentication to the vendor. In certain circumstances, the vendor may be willing to lower their required trust level, but not all the way to the level of the current authentication confidence. For instance, the vendor in the above example might consider that the phone call prior to the order might merit a 4% reduction in the degree of trust needed; however, this is still greater than the 93% confidence produced by the user.

[0287] If the vendor does adjust their required trust level in step 1835, then the authentication confidence level produced by the authentication and the required trust level are compared in step 1730 (see FIGURE 17). If the confidence level now exceeds the required trust level, a positive authentication may be generated in the transaction engine 205 in step 1740 (see FIGURE 17). If not, further arbitrage may be attempted as discussed above if it is permitted.

[0288] In addition to requesting an adjustment to the required trust level, the transaction engine 205 may also offer vendor side insurance to the vendor requesting the authentication. This insurance serves a similar purpose to that

described above for the user side insurance. Here, however, rather than the cost corresponding to the risk being taken by the trust engine 110 in authenticating above the actual authentication confidence level produced, the cost of the insurance corresponds to the risk being taken by the vendor in accepting a lower trust level in the authentication.

[0289] Instead of just lowering their actual required trust level, the vendor has the option of purchasing insurance to protect itself from the additional risk associated with a lower level of trust in the authentication of the user. As described above, it may be advantageous for the vendor to only consider purchasing such insurance to cover the trust gap in conditions where the existing authentication is already above a certain threshold.

[0290] The availability of such vendor side insurance allows the vendor the option to either: lower his trust requirement directly at no additional cost to himself, bearing the risk of a false authentication himself (based on the lower trust level required); or, buying insurance for the trust gap between the authentication confidence level and his requirement, with the trust engine 110 operator bearing the risk of the lower confidence level which has been provided. By purchasing the insurance, the vendor effectively keeps his high trust level requirement; because the risk of a false authentication is shifted to the trust engine 110 operator.

[0291] If the vendor purchases insurance in step 1840, the authentication confidence level and required trust levels are compared in step 1730 (see FIGURE 17), and the process continues as described above.

[0292] Note that it is also possible that both the user and the vendor respond to messages from the trust engine 110. Those of skill in the art will recognize that there are multiple ways in which such situations can be handled. One advantageous mode of handling the possibility of multiple responses is simply to treat the responses in a first-come, first-served manner. For example, if the vendor responds with a lowered required trust level and immediately thereafter the user also purchases insurance to raise his authentication level, the authentication is first reevaluated based upon the lowered trust requirement from the vendor. If the authentication is now positive, the user's insurance purchase is ignored. In another advantageous mode of operation, the user might only be charged for the level of

insurance required to meet the new, lowered trust requirement of the vendor (if a trust gap remained even with the lowered vendor trust requirement).

[0293] If no response from either party is received during the trust arbitrage process at step 1850 within the time limit set for the authentication, the arbitrage is reevaluated in step 1805. This effectively begins the arbitrage process again. If the time limit was final or other circumstances prevent further arbitrage in step 1805, a negative authentication is generated by the transaction engine 205 in step 1810 and returned to the vendor in step 1055 (see FIGURE 10). If not, new messages may be sent to the user and vendor, and the process may be repeated as desired.

[0294] Note that for certain types of transactions, for instance, digitally signing documents which are not part of a transaction, there may not necessarily be a vendor or other third party; therefore the transaction is primarily between the user and the trust engine 110. In circumstances such as these, the trust engine 110 will have its own required trust level which must be satisfied in order to generate a positive authentication. However, in such circumstances, it will often not be desirable for the trust engine 110 to offer insurance to the user in order for him to raise the confidence of his own signature.

[0295] The process described above and shown in FIGURES 16-18 may be carried out using various communications modes as described above with reference to the trust engine 110. For instance, the messages may be web-based and sent using SSL connections between the trust engine 110 and applets downloaded in real time to browsers running on the user or vendor systems. In an alternate mode of operation, certain dedicated applications may be in use by the user and vendor which facilitate such arbitrage and insurance transactions. In another alternate mode of operation, secure email operations may be used to mediate the arbitrage described above, thereby allowing deferred evaluations and batch processing of authentications. Those of skill in the art will recognize that different communications modes may be used as are appropriate for the circumstances and authentication requirements of the vendor.

[0296] The following description with reference to FIGURE 19 describes a sample transaction which integrates the various aspects of the present invention as

described above. This example illustrates the overall process between a user and a vendor as mediates by the trust engine 110. Although the various steps and components as described in detail above may be used to carry out the following transaction, the process illustrated focuses on the interaction between the trust engine 110, user and vendor.

[0297] The transaction begins when the user, while viewing web pages online, fills out an order form on the web site of the vendor in step 1900. The user wishes to submit this order form to the vendor, signed with his digital signature. In order to do this, the user submits the order form with his request for a signature to the trust engine 110 in step 1905. The user will also provide authentication data which will be used as described above to authenticate his identity.

[0298] In step 1910 the authentication data is compared to the enrollment data by the trust engine 110 as discussed above, and if a positive authentication is produced, the hash of the order form, signed with the private key of the user, is forwarded to the vendor along with the order form itself.

[0299] The vendor receives the signed form in step 1915, and then the vendor will generate an invoice or other contract related to the purchase to be made in step 1920. This contract is sent back to the user with a request for a signature in step 1925. The vendor also sends an authentication request for this contract transaction to the trust engine 110 in step 1930 including a hash of the contract which will be signed by both parties. To allow the contract to be digitally signed by both parties, the vendor also includes authentication data for itself so that the vendor's signature upon the contract can later be verified if necessary.

[0300] As discussed above, the trust engine 110 then verifies the authentication data provided by the vendor to confirm the vendor's identity, and if the data produces a positive authentication in step 1935, continues with step 1955 when the data is received from the user. If the vendor's authentication data does not match the enrollment data of the vendor to the desired degree, a message is returned to the vendor requesting further authentication. Trust arbitrage may be performed here if necessary, as described above, in order for the vendor to successfully authenticate itself to the trust engine 110.

[0301] When the user receives the contract in step 1940, he reviews it, generates authentication data to sign it if it is acceptable in step 1945, and then sends a hash of the contract and his authentication data to the trust engine 110 in step 1950. The trust engine 110 verifies the authentication data in step 1955 and if the authentication is good, proceeds to process the contract as described below. As discussed above with reference to FIGURES 17 and 18, trust arbitrage may be performed as appropriate to close any trust gap which exists between the authentication confidence level and the required authentication level for the transaction.

[0302] The trust engine 110 signs the hash of the contract with the user's private key, and sends this signed hash to the vendor in step 1960, signing the complete message on its own behalf, i.e., including a hash of the complete message (including the user's signature) encrypted with the private key 510 of the trust engine 110. This message is received by the vendor in step 1965. The message represents a signed contract (hash of contract encrypted using user's private key) and a receipt from the trust engine 110 (the hash of the message including the signed contract, encrypted using the trust engine 110's private key).

[0303] The trust engine 110 similarly prepares a hash of the contract with the vendor's private key in step 1970, and forwards this to the user, signed by the trust engine 110. In this way, the user also receives a copy of the contract, signed by the vendor, as well as a receipt, signed by the trust engine 110, for delivery of the signed contract in step 1975.

[0304] In addition to the foregoing, an additional aspect of the invention provides a cryptographic Service Provider Module (SPM) which may be available to a client side application as a means to access functions provided by the trust engine 110 described above. One advantageous way to provide such a service is for the cryptographic SPM is to mediate communications between a third party Application Programming Interface (API) and a trust engine 110 which is accessible via a network or other remote connection. A sample cryptographic SPM is described below with reference to FIGURE 20.

[0305] For example, on a typical system, a number of API's are available to programmers. Each API provides a set of function calls which may be made by an

application 2000 running upon the system. Examples of API's which provide programming interfaces suitable for cryptographic functions, authentication functions, and other security function include the Cryptographic API (CAPI) 2010 provided by Microsoft with its Windows operating systems, and the Common Data Security Architecture (CDSA), sponsored by IBM, Intel and other members of the Open Group. CAPI will be used as an exemplary security API in the discussion that follows. However, the cryptographic SPM described could be used with CDSA or other security API's as are known in the art.

[0306] This API is used by a user system 105 or vendor system 120 when a call is made for a cryptographic function. Included among these functions may be requests associated with performing various cryptographic operations, such as encrypting a document with a particular key, signing a document, requesting a digital certificate, verifying a signature upon a signed document, and such other cryptographic functions as are described herein or known to those of skill in the art.

[0307] Such cryptographic functions are normally performed locally to the system upon which CAPI 2010 is located. This is because generally the functions called require the use of either resources of the local user system 105, such as a fingerprint reader, or software functions which are programmed using libraries which are executed on the local machine. Access to these local resources is normally provided by one or more Service Provider Modules (SPM's) 2015, 2020 as referred to above which provide resources with which the cryptographic functions are carried out. Such SPM's may include software libraries 2015 to perform encrypting or decrypting operations, or drivers and applications 2020 which are capable of accessing specialized hardware 2025, such as biometric scanning devices. In much the way that CAPI 2010 provides functions which may be used by an application 2000 of the system 105, the SPM's 2015, 2020 provide CAPI with access to the lower level functions and resources associated with the available services upon the system.

[0308] In accordance with the invention, it is possible to provide a cryptographic SPM 2030 which is capable of accessing the cryptographic functions provided by the trust engine 110 and making these functions available to an application 2000

through CAPI 2010. Unlike embodiments where CAPI 2010 is only able to access resources which are locally available through SPM's 2015, 2020, a cryptographic SPM 2030 as described herein would be able to submit requests for cryptographic operations to a remotely-located, network-accessible trust engine 110 in order to perform the operations desired.

[0309] For instance, if an application 2000 has a need for a cryptographic operation, such as signing a document, the application 2000 makes a function call to the appropriate CAPI 2010 function. CAPI 2010 in turn will execute this function, making use of the resources which are made available to it by the SPM's 2015, 2020 and the cryptographic SPM 2030. In the case of a digital signature function, the cryptographic SPM 2030 will generate an appropriate request which will be sent to the trust engine 110 across the communication link 125.

[0310] The operations which occur between the cryptographic SPM 2030 and the trust engine 110 are the same operations that would be possible between any other system and the trust engine 110. However, these functions are effectively made available to a user system 105 through CAPI 2010 such that they appear to be locally available upon the user system 105 itself. However, unlike ordinary SPM's 2015, 2020, the functions are being carried out on the remote trust engine 110 and the results relayed to the cryptographic SPM 2030 in response to appropriate requests across the communication link 125.

[0311] This cryptographic SPM 2030 makes a number of operations available to the user system 105 or a vendor system 120 which might not otherwise be available. These functions include without limitation: encryption and decryption of documents; issuance of digital certificates; digital signing of documents; verification of digital signatures; and such other operations as will be apparent to those of skill in the art.

[0312] In a separate embodiment, the present invention comprises a complete system for performing the data securing methods of the present invention on any data set. The computer system of this embodiment comprises a data splitting module that comprises the functionality shown in FIGURE 8 and described herein. In one embodiment of the present invention, the data splitting module, sometimes referred to herein as a secure data parser, comprises a parser program or software

suite which comprises data splitting, encryption and decryption, reconstitution or reassembly functionality. This embodiment may further comprise a data storage facility or multiple data storage facilities, as well. The data splitting module, or secure data parser, comprises a cross-platform software module suite which integrates within an electronic infrastructure, or as an add-on to any application which requires the ultimate security of its data elements. This parsing process operates on any type of data set, and on any and all file types, or in a database on any row, column or cell of data in that database.

[0313] The parsing process of the present invention may, in one embodiment, be designed in a modular tiered fashion, and any encryption process is suitable for use in the process of the present invention. The modular tiers of the parsing and splitting process of the present invention may include, but are not limited to, 1) cryptographic split, dispersed and securely stored in multiple locations; 2) encrypt, cryptographically split, dispersed and securely stored in multiple locations; 3) encrypt, cryptographically split, encrypt each share, then dispersed and securely stored in multiple locations; and 4) encrypt, cryptographically split, encrypt each share with a different type of encryption than was used in the first step, then dispersed and securely stored in multiple locations.

[0314] The process comprises, in one embodiment, splitting of the data according to the contents of a generated random number, or key and performing the same cryptographic splitting of the key used in the encryption of splitting of the data to be secured into two or more portions, or shares, of parsed and split data, and in one embodiment, preferably into four or more portions of parsed and split data, encrypting all of the portions, then scattering and storing these portions back into the database, or relocating them to any named device, fixed or removable, depending on the requestor's need for privacy and security. Alternatively, in another embodiment, encryption may occur prior to the splitting of the data set by the splitting module or secure data parser. The original data processed as described in this embodiment is encrypted and obfuscated and is secured. The dispersion of the encrypted elements, if desired, can be virtually anywhere, including, but not limited to, a single server or data storage device, or among separate data storage facilities or devices. Encryption key management in one

embodiment may be included within the software suite, or in another embodiment may be integrated into an existing infrastructure or any other desired location.

[0315] A cryptographic split (cryptosplit) partitions the data into N number of shares. The partitioning can be on any size unit of data, including an individual bit, bits, bytes, kilobytes, megabytes, or larger units, as well as any pattern or combination of data unit sizes whether predetermined or randomly generated. The units can also be of different sized, based on either a random or predetermined set of values. This means the data can be viewed as a sequence of these units. In this manner the size of the data units themselves may render the data more secure, for example by using one or more predetermined or randomly generated pattern, sequence or combination of data unit sizes. The units are then distributed (either randomly or by a predetermined set of values) into the N shares. This distribution could also involve a shuffling of the order of the units in the shares. It is readily apparent to those of ordinary skill in the art that the distribution of the data units into the shares may be performed according to a wide variety of possible selections, including but not limited to size-fixed, predetermined sizes, or one or more combination, pattern or sequence of data unit sizes that are predetermined or randomly generated.

[0316] One example of this cryptographic split process, or cryptosplit, would be to consider the data to be 23 bytes in size, with the data unit size chosen to be one byte, and with the number of shares selected to be 4. Each byte would be distributed into one of the 4 shares. Assuming a random distribution, a key would be obtained to create a sequence of 23 random numbers (r1, r2, r3 through r23), each with a value between 1 and 4 corresponding to the four shares. Each of the units of data (in this example 23 individual bytes of data) is associated with one of the 23 random numbers corresponding to one of the four shares. The distribution of the bytes of data into the four shares would occur by placing the first byte of the data into share number r1, byte two into share r2, byte three into share r3, through the 23rd byte of data into share r23. It is readily apparent to those of ordinary skill in the art that a wide variety of other possible steps or combination or sequence of steps, including the size of the data units, may be used in the cryptosplit process of the present invention, and the above example is a non-limiting description of one

process for cryptosplitting data. To recreate the original data, the reverse operation would be performed.

[0317] In another embodiment of the cryptosplit process of the present invention, an option for the cryptosplitting process is to provide sufficient redundancy in the shares such that only a subset of the shares are needed to reassemble or restore the data to its original or useable form. As a non-limiting example, the cryptosplit may be done as a "3 of 4" cryptosplit such that only three of the four shares are necessary to reassemble or restore the data to its original or useable form. This is also referred to as a "M of N cryptosplit" wherein N is the total number of shares, and M is at least one less than N. It is readily apparent to those of ordinary skill in the art that there are many possibilities for creating this redundancy in the cryptosplitting process of the present invention.

[0318] In one embodiment of the cryptosplitting process of the present invention, each unit of data is stored in two shares, the primary share and the backup share. Using the "3 of 4" cryptosplitting process described above, any one share can be missing, and this is sufficient to reassemble or restore the original data with no missing data units since only three of the total four shares are required. As described herein, a random number is generated that corresponds to one of the shares. The random number is associated with a data unit, and stored in the corresponding share, based on a key. One key is used, in this embodiment, to generate the primary and backup share random number. As described herein for the cryptosplitting process of the present invention, a set of random numbers (also referred to as primary share numbers) from 0 to 3 are generated equal to the number of data units. Then another set of random numbers is generated (also referred to as backup share numbers) from 1 to 3 equal to the number of data units. Each unit of data is then associated with a primary share number and a backup share number. Alternatively, a set of random numbers may be generated that is fewer than the number of data units, and repeating the random number set, but this may reduce the security of the sensitive data. The primary share number is used to determine into which share the data unit is stored. The backup share number is combined with the primary share number to create a third share number between 0

and 3, and this number is used to determine into which share the data unit is stored. In this example, the equation to determine the third share number is:
(primary share number + backup share number) MOD 4 = third share number.

[0319] In the embodiment described above where the primary share number is between 0 and 3, and the backup share number is between 1 and 3 ensures that the third share number is different from the primary share number. This results in the data unit being stored in two different shares. It is readily apparent to those of ordinary skill in the art that there are many ways of performing redundant cryptosplitting and non-redundant cryptosplitting in addition to the embodiments disclosed herein. For example, the data units in each share could be shuffled utilizing a different algorithm. This data unit shuffling may be performed as the original data is split into the data units, or after the data units are placed into the shares, or after the share is full, for example.

[0320] The various cryptosplitting processes and data shuffling processes described herein, and all other embodiments of the cryptosplitting and data shuffling methods of the present invention may be performed on data units of any size, including but not limited to, as small as an individual bit, bits, bytes, kilobytes, megabytes or larger.

[0321] An example of one embodiment of source code that would perform the cryptosplitting process described herein is:

```
DATA [1:24] – array of bytes with the data to be split
SHARES[0:3; 1:24] – 2-dimensionalarray with each row representing one of the shares
RANDOM[1:24] – array random numbers in the range of 0..3
S1 = 1;
S2 = 1;
S3 = 1;
S4 = 1;

For J = 1 to 24 do
        Begin
        IF RANDOM[J[ ==0 then
```

```
        Begin
        SHARES[1,S1] = DATA [J];
        S1 = S1 + 1;
        End
    ELSE IF RANDOM[J[ ==1 then
        Begin
        SHARES[2,S2] = DATA [J];
        S2 = S2 + 1;
        END
    ELSE IF RANDOM[J[ ==2 then
        Begin
        Shares[3,S3] = data [J];
        S3 = S3 + 1;
        End
    Else   begin
        Shares[4,S4] = data [J];
        S4 = S4 + 1;
        End;
    END;
```

[0322] An example of one embodiment of source code that would perform the cryptosplitting RAID process described herein is:

[0323] Generate two sets of numbers, PrimaryShare is 0 to 3, BackupShare is 1 to 3. Then put each data unit into share[primaryshare[1]] and share[(primaryshare[1]+backupshare[1]) mod 4, with the same process as in cryptosplitting described above. This method will be scalable to any size N, where only N-1 shares are necessary to restore the data.

[0324] The retrieval, recombining, reassembly or reconstituting of the encrypted data elements may utilize any number of authentication techniques, including, but not limited to, biometrics, such as fingerprint recognition, facial scan, hand scan, iris scan, retinal scan, ear scan, vascular pattern recognition or DNA analysis. The data splitting and/or parser modules of the present invention may be integrated into a wide variety of infrastructure products or applications as desired.

[0325] Traditional encryption technologies known in the art rely on one or more key used to encrypt the data and render it unusable without the key. The data, however, remains whole and intact and subject to attack. The secure data parser of the present invention, in one embodiment, addresses this problem by performing a cryptographic parsing and splitting of the encrypted file into two or more portions or shares, and in another embodiment, preferably four or more shares, adding another layer of encryption to each share of the data, then storing the shares in different physical and/or logical locations. When one or more data shares are physically removed from the system, either by using a removable device, such as a data storage device, or by placing the share under another party's control, any possibility of compromise of secured data is effectively removed.

[0326] An example of one embodiment of the secure data parser of the present invention and an example of how it may be utilized is shown in FIGURE 21 and described below. However, it is readily apparent to those of ordinary skill in the art that the secure data parser of the present invention may be utilized in a wide variety of ways in addition to the non-limiting example below. As a deployment option, and in one embodiment, the secure data parser may be implemented with external session key management or secure internal storage of session keys. Upon implementation, a Parser Master Key will be generated which will be used for securing the application and for encryption purposes. It should be also noted that the incorporation of the Parser Master key in the resulting secured data allows for a flexibility of sharing of secured data by individuals within a workgroup, enterprise or extended audience.

[0327] As shown in Figure 21, this embodiment of the present invention shows the steps of the process performed by the secure data parser on data to store the session master key with the parsed data:

[0328] 1. Generating a session master key and encrypt the data using RS1 stream cipher.

[0329] 2. Separating the resulting encrypted data into four shares or portions of parsed data according to the pattern of the session master key.

[0330] 3. In this embodiment of the method, the session master key will be stored along with the secured data shares in a data depository. Separating the session

master key according to the pattern of the Parser Master Key and append the key data to the encrypted parsed data.

[0331] 4. The resulting four shares of data will contain encrypted portions of the original data and portions of the session master key. Generate a stream cipher key for each of the four data shares.

[0332] 5. Encrypting each share, then store the encryption keys in different locations from the encrypted data portions or shares: Share 1 gets Key 4, Share 2 gets Key 1, Share 3 gets Key 2, Share 4 gets Key 3.

[0333] To restore the original data format, the steps are reversed.

[0334] It is readily apparent to those of ordinary skill in the art that certain steps of the methods described herein may be performed in different order, or repeated multiple times, as desired. It is also readily apparent to those skilled in the art that the portions of the data may be handled differently from one another. For example, multiple parsing steps may be performed on only one portion of the parsed data. Each portion of parsed data may be uniquely secured in any desirable way provided only that the data may be reassembled, reconstituted, reformed, decrypted or restored to its original or other usable form.

[0335] As shown in FIGURE 22 and described herein, another embodiment of the present invention comprises the steps of the process performed by the secure data parser on data to store the session master key data in one or more separate key management table:

[0336] 1. Generating a session master key and encrypt the data using RS1 stream cipher.

[0337] 2. Separating the resulting encrypted data into four shares or portions of parsed data according to the pattern of the session master key.

[0338] 3. In this embodiment of the method of the present invention, the session master key will be stored in a separate key management table in a data depository. Generating a unique transaction ID for this transaction. Storing the transaction ID and session master key in a separate key management table. Separating the transaction ID according to the pattern of the Parser Master Key and append the data to the encrypted parsed or separated data.

[0339] 4. The resulting four shares of data will contain encrypted portions of the original data and portions of the transaction ID.

[0340] 5. Generating a stream cipher key for each of the four data shares.

[0341] 6. Encrypting each share, then store the encryption keys in different locations from the encrypted data portions or shares: Share 1 gets Key 4, Share 2 gets Key 1, Share 3 gets Key 2, Share 4 gets Key 3.

[0342] To restore the original data format, the steps are reversed.

[0343] It is readily apparent to those of ordinary skill in the art that certain steps of the method described herein may be performed in different order, or repeated multiple times, as desired. It is also readily apparent to those skilled in the art that the portions of the data may be handled differently from one another. For example, multiple separating or parsing steps may be performed on only one portion of the parsed data. Each portion of parsed data may be uniquely secured in any desirable way provided only that the data may be reassembled, reconstituted, reformed, decrypted or restored to its original or other usable form.

[0344] As shown in Figure 23, this embodiment of the present invention shows the steps of the process performed by the secure data parser on data to store the session master key with the parsed data:

[0345] 1. Accessing the parser master key associated with the authenticated user

[0346] 2. Generating a unique Session Master key

[0347] 3. Derive an Intermediary Key from an exclusive OR function of the Parser Master Key and Session Master key

[0348] 4. Optional encryption of the data using an existing or new encryption algorithm keyed with the Intermediary Key.

[0349] 5. Separating the resulting optionally encrypted data into four shares or portions of parsed data according to the pattern of the Intermediary key.

[0350] 6. In this embodiment of the method, the session master key will be stored along with the secured data shares in a data depository. Separating the session master key according to the pattern of the Parser Master Key and append the key data to the optionally encrypted parsed data shares.

[0351] 7. The resulting multiple shares of data will contain optionally encrypted portions of the original data and portions of the session master key.

[0352] 8. Optionally generate an encryption key for each of the four data shares.

[0353] 9. Optionally encrypting each share with an existing or new encryption algorithm, then store the encryption keys in different locations from the encrypted data portions or shares: for example, Share 1 gets Key 4, Share 2 gets Key 1, Share 3 gets Key 2, Share 4 gets Key 3.

[0354] To restore the original data format, the steps are reversed.

[0355] It is readily apparent to those of ordinary skill in the art that certain steps of the methods described herein may be performed in different order, or repeated multiple times, as desired. It is also readily apparent to those skilled in the art that the portions of the data may be handled differently from one another. For example, multiple parsing steps may be performed on only one portion of the parsed data. Each portion of parsed data may be uniquely secured in any desirable way provided only that the data may be reassembled, reconstituted, reformed, decrypted or restored to its original or other usable form.

[0356] As shown in FIGURE 24 and described herein, another embodiment of the present invention comprises the steps of the process performed by the secure data parser on data to store the session master key data in one or more separate key management table:

[0357] 1. Accessing the Parser Master Key associated with the authenticated user

[0358] 2. Generating a unique Session Master Key

[0359] 3. Derive an Intermediary Key from an exclusive OR function of the Parser Master Key and Session Master key

[0360] 4. Optionally encrypt the data using an existing or new encryption algorithm keyed with the Intermediary Key.

[0361] 5. Separating the resulting optionally encrypted data into four shares or portions of parsed data according to the pattern of the Intermediary Key.

[0362] 6. In this embodiment of the method of the present invention, the session master key will be stored in a separate key management table in a data

depository. Generating a unique transaction ID for this transaction. Storing the transaction ID and session master key in a separate key management table or passing the Session Master Key and transaction ID back to the calling program for external management. Separating the transaction ID according to the pattern of the Parser Master Key and append the data to the optionally encrypted parsed or separated data.

[0363] 7. The resulting four shares of data will contain optionally encrypted portions of the original data and portions of the transaction ID.

[0364] 8. Optionally generate an encryption key for each of the four data shares.

[0365] 9. Optionally encrypting each share, then store the encryption keys in different locations from the encrypted data portions or shares. For example: Share 1 gets Key 4, Share 2 gets Key 1, Share 3 gets Key 2, Share 4 gets Key 3.

[0366] To restore the original data format, the steps are reversed.

[0367] It is readily apparent to those of ordinary skill in the art that certain steps of the method described herein may be performed in different order, or repeated multiple times, as desired. It is also readily apparent to those skilled in the art that the portions of the data may be handled differently from one another. For example, multiple separating or parsing steps may be performed on only one portion of the parsed data. Each portion of parsed data may be uniquely secured in any desirable way provided only that the data may be reassembled, reconstituted, reformed, decrypted or restored to its original or other usable form.

[0368] A wide variety of encryption methodologies are suitable for use in the methods of the present invention, as is readily apparent to those skilled in the art. The One Time Pad algorithm, is often considered one of the most secure encryption methods, and is suitable for use in the method of the present invention. Using the One Time Pad algorithm requires that a key be generated which is as long as the data to be secured. The use of this method may be less desirable in certain circumstances such as those resulting in the generation and management of very long keys because of the size of the data set to be secured. In the One-Time Pad (OTP) algorithm, the simple exclusive-or function, XOR, is used. For two

binary streams x and y of the same length, x XOR y means the bitwise exclusive-or of x and y.

[0369] At the bit level is generated:

0 XOR 0 = 0

0 XOR 1 = 1

1 XOR 0 = 1

1 XOR 1 = 0

[0370] An example of this process is described herein for an n-byte secret, s, (or data set) to be split. The process will generate an n-byte random value, a, and then set:

b = a XOR s.

[0371] Note that one can derive "s" via the equation:

s = a XOR b.

[0372] The values a and b are referred to as shares or portions and are placed in separate depositories. Once the secret s is split into two or more shares, it is discarded in a secure manner.

[0373] The secure data parser of the present invention may utilize this function, performing multiple XOR functions incorporating multiple distinct secret key values: K1, K2, K3, Kn, K5. At the beginning of the operation, the data to be secured is passed through the first encryption operation, secure data = data XOR secret key 5:

S = D XOR K5

[0374] In order to securely store the resulting encrypted data in, for example, four shares, S1, S2, S3, Sn, the data is parsed and split into "n" segments, or shares, according to the value of K5. This operation results in "n" pseudorandom shares of the original encrypted data. Subsequent XOR functions may then be performed on each share with the remaining secret key values, for example: Secure data segment 1 = encrypted data share 1 XOR secret key 1:

SD1 = S1 XOR K1

SD2 = S2 XOR K2

SD3 = S3 XOR K3

SDn = Sn XOR Kn.

[0375] In one embodiment, it may not be desired to have any one depository contain enough information to decrypt the information held there, so the key required to decrypt the share is stored in a different data depository:

Depository 1: SD1, Kn

Depository 2: SD2, K1

Depository 3: SD3, K2

Depository n: SDn, K3.

[0376] Additionally, appended to each share may be the information required to retrieve the original session encryption key, K5. Therefore, in the key management example described herein, the original session master key is referenced by a transaction ID split into "n" shares according to the contents of the installation dependant Parser Master Key (TID1, TID2, TID3, TIDn):

Depository 1: SD1, Kn, TID1

Depository 2: SD2, K1, TID2

Depository 3: SD3, K2, TID3

Depository n: SDn, K3, TIDn.

[0377] In the incorporated session key example described herein, the session master key is split into "n" shares according to the contents of the installation dependant Parser Master Key (SK1, SK2, SK3, SKn):

Depository 1: SD1, Kn, SK1

Depository 2: SD2, K1, SK2

Depository 3: SD3, K2, SK3

Depository n: SDn, K3, SKn.

[0378] Unless all four shares are retrieved, the data cannot be reassembled according to this example. Even if all four shares are captured, there is no possibility of reassembling or restoring the original information without access to the session master key and the Parser Master Key.

[0379] This example has described an embodiment of the method of the present invention, and also describes, in another embodiment, the algorithm used to place shares into depositories so that shares from all depositories can be combined to form the secret authentication material. The computations needed are very simple and fast. However, with the One Time Pad (OTP) algorithm there may be circumstances that cause it to be less desirable, such as a large data set to be secured, because the key size is the same size as the data to be stored. Therefore, there would be a need to store and transmit about twice the amount of the original data which may be less desirable under certain circumstances.

Stream Cipher RS1

[0380] The stream cipher RS1 splitting technique is very similar to the OTP splitting technique described herein. Instead of an n-byte random value, an n' = min(n, 16)-byte random value is generated and used to key the RS1 Stream Cipher algorithm. The advantage of the RS1 Stream Cipher algorithm is that a pseudorandom key is generated from a much smaller seed number. The speed of execution of the RS1 Stream Cipher encryption is also rated at approximately 10 times the speed of the well known in the art Triple DES encryption without compromising security. The RS1 Stream Cipher algorithm is well known in the art, and may be used to generate the keys used in the XOR function. The RS1 Stream Cipher algorithm is interoperable with other commercially available stream cipher algorithms, such as the RC4™ stream cipher algorithm of RSA Security, Inc and is suitable for use in the methods of the present invention.

[0381] Using the key notation above, K1 thru K5 are now an n' byte random values and we set:

SD1 = S1 XOR E(K1)

SD2 = S2 XOR E(K2)

SD3 = S3 XOR E(K3)

SDn = Sn XOR E(Kn)

where E(K1) thru E(Kn) are the first n' bytes of output from the RS1 Stream Cipher algorithm keyed by K1 thru Kn. The shares are now placed into data depositories as described herein.

[0382] In this stream cipher RS1 algorithm, the required computations needed are nearly as simple and fast as the OTP algorithm. The benefit in this example using the RS1 Stream Cipher is that the system needs to store and transmit on average only about 16 bytes more than the size of the original data to be secured per share. When the size of the original data is more than 16 bytes, this RS1 algorithm is more efficient than the OTP algorithm because it is simply shorter. It is readily apparent to those of ordinary skill in the art that a wide variety of encryption methods or algorithms are suitable for use in the present invention, including, but not limited to RS1, OTP, RC4™, Triple DES and AES.

[0383] There are major advantages provided by the data security methods and computer systems of the present invention over traditional encryption methods. One advantage is the security gained from moving shares of the data to different locations on one or more data depositories or storage devices, that may be in different logical, physical or geographical locations. When the shares of data are split physically and under the control of different personnel, for example, the possibility of compromising the data is greatly reduced.

[0384] Another advantage provided by the methods and system of the present invention is the combination of the steps of the method of the present invention for securing data to provide a comprehensive process of maintaining security of sensitive data. The data is encrypted with a secure key and split into one or more shares, and in one embodiment, four shares, according to the secure key. The secure key is stored safely with a reference pointer which is secured into four shares according to a secure key. The data shares are then encrypted individually and the keys are stored safely with different encrypted shares. When combined, the entire process for securing data according to the methods disclosed herein becomes a comprehensive package for data security.

[0385] The data secured according to the methods of the present invention is readily retrievable and restored, reconstituted, reassembled, decrypted, or otherwise returned into its original or other suitable form for use. In order to restore the original data, the following items may be utilized:

[0386] 1. All shares or portions of the data set.

[0387] 2. Knowledge of and ability to reproduce the process flow of the method used to secure the data.

[0388] 3. Access to the session master key.

[0389] 4. Access to the Parser Master Key.

[0390] Therefore, it may be desirable to plan a secure installation wherein at least one of the above elements may be physically separated from the remaining components of the system (under the control of a different system administrator for example).

[0391] Protection against a rogue application invoking the data securing methods application may be enforced by use of the Parser Master Key. A mutual authentication handshake between the secure data parser and the application may be required in this embodiment of the present invention prior to any action taken.

[0392] The security of the system dictates that there be no "backdoor" method for recreation of the original data. For installations where data recovery issues may arise, the secure data parser can be enhanced to provide a mirror of the four shares and session master key depository. Hardware options such as RAID (redundant array of inexpensive disks, used to spread information over several disks) and software options such as replication can assist as well in the data recovery planning.

Key Management

[0393] In one embodiment of the present invention, the data securing method uses three sets of keys for an encryption operation. Each set of keys may have individual key storage, retrieval, security and recovery options, based on the installation. The keys that may be used, include, but are not limited to:

The Parser Master Key

[0394] This key is an individual key associated with the installation of the secure data parser. It is installed on the server on which the secure data parser has been deployed. There are a variety of options suitable for securing this key including, but not limited to, a smart card, separate hardware key store, standard key stores, custom key stores or within a secured database table, for example.

The Session Master Key

[0395] A Session Master Key may be generated each time data is secured. The Session Master Key is used to encrypt the data prior to the parsing and splitting operations. It may also be incorporated (if the Session Master Key is not integrated into the parsed data) as a means of parsing the encrypted data. The Session Master Key may be secured in a variety of manners, including, but not limited to, a standard key store, custom key store, separate database table, or secured within the encrypted shares, for example.

The Share Encryption Keys

[0396] For each share or portions of a data set that is created, an individual Share Encryption Key may be generated to further encrypt the shares. The Share Encryption Keys may be stored in different shares than the share that was encrypted.

[0397] It is readily apparent to those of ordinary skill in the art that the data securing methods and computer system of the present invention are widely applicable to any type of data in any setting or environment. In addition to commercial applications conducted over the Internet or between customers and vendors, the data securing methods and computer systems of the present invention are highly applicable to non-commercial or private settings or environments. Any data set that is desired to be kept secure from any unauthorized user may be secured using the methods and systems described herein. For example, access to a particular database within a company or organization may be advantageously restricted to only selected users by employing the methods and systems of the present invention for securing data. Another example is the generation, modification or access to documents wherein it is desired to restrict access or prevent unauthorized or accidental access or disclosure outside a group of selected individuals, computers or workstations. These and other examples of the ways in which the methods and systems of data securing of the present invention are applicable to any non-commercial or commercial environment or setting for any setting, including, but not limited to any organization, government agency or corporation.

[0398] In another embodiment of the present invention, the data securing method uses three sets of keys for an encryption operation. Each set of keys may have

individual key storage, retrieval, security and recovery options, based on the installation. The keys that may be used, include, but are not limited to:

1. The Parser Master Key

[0399] This key is an individual key associated with the installation of the secure data parser. It is installed on the server on which the secure data parser has been deployed. There are a variety of options suitable for securing this key including, but not limited to, a smart card, separate hardware key store, standard key stores, custom key stores or within a secured database table, for example.

2. The Session Master Key

[0400] A Session Master Key may be generated each time data is secured. The Session Master Key is used in conjunction with the Parser Master key to derive the Intermediary Key. The Session Master Key may be secured in a variety of manners, including, but not limited to, a standard key store, custom key store, separate database table, or secured within the encrypted shares, for example.

3. The Intermediary Key

[0401] An Intermediary Key may be generated each time data is secured. The Intermediary Key is used to encrypt the data prior to the parsing and splitting operation. It may also be incorporated as a means of parsing the encrypted data.

4. The Share Encryption Keys

[0402] For each share or portions of a data set that is created, an individual Share Encryption Key may be generated to further encrypt the shares. The Share Encryption Keys may be stored in different shares than the share that was encrypted.

[0403] It is readily apparent to those of ordinary skill in the art that the data securing methods and computer system of the present invention are widely applicable to any type of data in any setting or environment. In addition to commercial applications conducted over the Internet or between customers and vendors, the data securing methods and computer systems of the present invention are highly applicable to non-commercial or private settings or environments. Any data set that is desired to be kept secure from any unauthorized user may be secured using the methods and systems described herein. For example, access to a particular database within a company or organization may be advantageously

restricted to only selected users by employing the methods and systems of the present invention for securing data. Another example is the generation, modification or access to documents wherein it is desired to restrict access or prevent unauthorized or accidental access or disclosure outside a group of selected individuals, computers or workstations. These and other examples of the ways in which the methods and systems of data securing of the present invention are applicable to any non-commercial or commercial environment or setting for any setting, including, but not limited to any organization, government agency or corporation.

Workgroup, Project, Individual PC/Laptop or Cross Platform Data Security

[0404] The data securing methods and computer systems of the present invention are also useful in securing data by workgroup, project, individual PC/Laptop and any other platform that is in use in, for example, businesses, offices, government agencies, or any setting in which sensitive data is created, handled or stored. The present invention provides methods and computer systems to secure data that is known to be sought after by organizations, such as the U.S. Government, for implementation across the entire government organization or between governments at a state or federal level.

[0405] The data securing methods and computer systems of the present invention provide the ability to not only parse and split flat files but also data fields, sets and or table of any type. Additionally, all forms of data are capable of being secured under this process, including, but not limited to, text, video, images, biometrics and voice data. Scalability, speed and data throughput of the methods of securing data of the present invention are only limited to the hardware the user has at their disposal.

[0406] In one embodiment of the present invention, the data securing methods are utilized as described below in a workgroup environment. In one embodiment, as shown in FIGURE 23 and described below, the Workgroup Scale data securing method of the present invention uses the private key management functionality of the TrustEngine to store the user/group relationships and the associated private keys (Parser Group Master Keys) necessary for a group of users to share secure data. The method of the present invention has the capability to secure data for an

enterprise, workgroup, or individual user, depending on how the Parser Master Key was deployed.

[0407] In one embodiment, additional key management and user/group management programs may be provided, enabling wide scale workgroup implementation with a single point of administration and key management. Key generation, management and revocation are handled by the single maintenance program, which all become especially important as the number of users increase. In another embodiment, key management may also be set up across one or several different system administrators, which may not allow any one person or group to control data as needed. This allows for the management of secured data to be obtained by roles, responsibilities, membership, rights, etc., as defined by an organization, and the access to secured data can be limited to just those who are permitted or required to have access only to the portion they are working on, while others, such as managers or executives, may have access to all of the secured data. This embodiment allows for the sharing of secured data among different groups within a company or organization while at the same time only allowing certain selected individuals, such as those with the authorized and predetermined roles and responsibilities, to observe the data as a whole. In addition, this embodiment of the methods and systems of the present invention also allows for the sharing of data among, for example, separate companies, or separate departments or divisions of companies, or any separate organization departments, groups, agencies, or offices, or the like, of any government or organization or any kind, where some sharing is required, but not any one party may be permitted to have access to all the data. Particularly apparent examples of the need and utility for such a method and system of the present invention are to allow sharing, but maintain security, in between government areas, agencies and offices, and between different divisions, departments or offices of a large company, or any other organization, for example.

[0408] An example of the applicability of the methods of the present invention on a smaller scale is as follows. A Parser Master key is used as a serialization or branding of the secure data parser to an organization. As the scale of use of the Parser Master key is reduced from the whole enterprise to a smaller workgroup, the

data securing methods described herein are used to share files within groups of users.

[0409] In the example shown in FIGURE 25 and described below, there are six users defined along with their title or role within the organization. The side bar represents five possible groups that the users can belong to according to their role. The arrow represents membership by the user in one or more of the groups.

[0410] When configuring the secure data parser for use in this example, the system administrator accesses the user and group information from the operating system by a maintenance program. This maintenance program generates and assigns Parser Group Master Keys to users based on their membership in groups.

[0411] In this example, there are three members in the Senior Staff group. For this group, the actions would be:

[0412] 1. Access Parser Group Master Key for the Senior Staff group (generate a key if not available);

[0413] 2. Generate a digital certificate associating CEO with the Senior Staff group;

[0414] 3. Generate a digital certificate associating CFO with the Senior Staff group;

[0415] 4. Generate a digital certificate associating Vice President, Marketing with the Senior Staff group.

[0416] The same set of actions would be done for each group, and each member within each group. When the maintenance program is complete, the Parser Group Master Key becomes a shared credential for each member of the group. Revocation of the assigned digital certificate may be done automatically when a user is removed from a group through the maintenance program without affecting the remaining members of the group.

[0417] Once the shared credentials have been defined, the parsing and splitting process remains the same. When a file, document or data element is to be secured, the user is prompted for the target group to be used when securing the data. The resulting secured data is only accessible by other members of the target group. This functionality of the methods and systems of the present invention may be used

with any other computer system or software platform, any may be, for example, integrated into existing application programs or used standalone for file security.

[0418] It is readily apparent to those of ordinary skill in the art that any one or combination of encryption algorithms are suitable for use in the methods and systems of the present invention. For example, the encryption steps may, in one embodiment, be repeated to produce a multi-layered encryption scheme. In addition, a different encryption algorithm, or combination of encryption algorithms, may be used in repeat encryption steps such that different encryption algorithms are applied to the different layers of the multi-layered encryption scheme. As such, the encryption scheme itself may become a component of the methods of the present invention for securing sensitive data from unauthorized use or access.

[0419] The secure data parser may include as an internal component, as an external component, or as both an error-checking component. For example, in one suitable approach, as portions of data are created using the secure data parser in accordance with the present invention, to assure the integrity of the data within a portion, a hash value is taken at preset intervals within the portion and is appended to the end of the interval. The hash value is a predictable and reproducible numeric representation of the data. If any bit within the data changes, the hash value would be different. A scanning module (either as a stand-alone component external to the secure data parser or as an internal component) may then scan the portions of data generated by the secure data parser. Each portion of data (or alternatively, less than all portions of data according to some interval or by a random or pseudo-random sampling) is compared to the appended hash value or values and an action may be taken. This action may include a report of values that match and do not match, an alert for values that do not match, or invoking of some external or internal program to trigger a recovery of the data. For example, recovery of the data could be performed by invoking a recovery module based on the concept that fewer than all portions may be needed to generate original data in accordance with the present invention.

[0420] Any other suitable integrity checking may be implemented using any suitable integrity information appended anywhere in all or a subset of data

portions. Integrity information may include any suitable information that can be used to determine the integrity of data portions. Examples of integrity information may include hash values computed based on any suitable parameter (e.g., based on respective data portions), digital signature information, message authentication code (MAC) information, any other suitable information, or any combination thereof.

[0421] The secure data parser of the present invention may be used in any suitable application. Namely, the secure data parser described herein has a variety of applications in different areas of computing and technology. Several such areas are discussed below. It will be understood that these are merely illustrative in nature and that any other suitable applications may make use of the secure data parser. It will further be understood that the examples described are merely illustrative embodiments that may be modified in any suitable way in order to satisfy any suitable desires. For example, parsing and splitting may be based on any suitable units, such as by bits, by bytes, by kilobytes, by megabytes, by any combination thereof, or by any other suitable unit.

[0422] The secure data parser of the present invention may be used to implement secure physical tokens, whereby data stored in a physical token may be required in order to access additional data stored in another storage area. In one suitable approach, a physical token, such as a compact USB flash drive, a floppy disk, an optical disk, a smart card, or any other suitable physical token, may be used to store one of at least two portions of parsed data in accordance with the present invention. In order to access the original data, the USB flash drive would need to be accessed. Thus, a personal computer holding one portion of parsed data would need to have the USB flash drive, having the other portion of parsed data, attached before the original data can be accessed. FIGURE 26 illustrates this application. Storage area 2500 includes a portion of parsed data 2502. Physical token 2504, having a portion of parsed data 2506 would need to be coupled to storage area 2500 using any suitable communications interface 2508 (e.g., USB, serial, parallel, Bluetooth, IR, IEEE 1394, ethernet, or any other suitable communications interface) in order to access the original data. This is useful in a situation where, for example, sensitive data on a computer is left alone and subject to unauthorized

access attempts. By removing the physical token (e.g., the USB flash drive), the sensitive data is inaccessible. It will be understood that any other suitable approach for using physical tokens may be used.

[0423] The secure data parser of the present invention may be used to implement a secure authentication system whereby user enrollment data (e.g., passwords, private encryption keys, fingerprint templates, biometric data or any other suitable user enrollment data) is parsed and split using the secure data parser. The user enrollment data may be parsed and split whereby one or more portions are stored on a smart card, a government Common Access Card, any suitable physical storage device (e.g., magnetic or optical disk, USB key drive, etc.), or any other suitable device. One or more other portions of the parsed user enrollment data may be stored in the system performing the authentication. This provides an added level of security to the authentication process (e.g., in addition to the biometric authentication information obtained from the biometric source, the user enrollment data must also be obtained via the appropriate parsed and split data portion).

[0424] The secure data parser of the present invention may be integrated into any suitable existing system in order to provide the use of its functionality in each system's respective environment. FIGURE 27 shows a block diagram of an illustrative system 2600, which may include software, hardware, or both for implementing any suitable application. System 2600 may be an existing system in which secure data parser 2602 may be retrofitted as an integrated component. Alternatively, secure data parser 2602 may be integrated into any suitable system 2600 from, for example, its earliest design stage. Secure data parser 2600 may be integrated at any suitable level of system 2600. For example, secure data parser 2602 may be integrated into system 2600 at a sufficiently back-end level such that the presence of secure data parser 2602 may be substantially transparent to an end user of system 2600. Secure data parser 2602 may be used for parsing and splitting data among one or more storage devices 2604 in accordance with the present invention. Some illustrative examples of systems having the secure data parser integrated therein are discussed below.

[0425] The secure data parser of the present invention may be integrated into an operating system kernel (e.g., Linux, Unix, or any other suitable commercial or

proprietary operating system). This integration may be used to protect data at the device level whereby, for example, data that would ordinarily be stored in one or more devices is separated into a certain number of portions by the secure data parser integrated into the operating system and stored among the one or more devices. When original data is attempted to be accessed, the appropriate software, also integrated into the operating system, may recombine the parsed data portions into the original data in a way that may be transparent to the end user.

[0426] The secure data parser of the present invention may be integrated into a volume manager or any other suitable component of a storage system to protect local and networked data storage across any or all supported platforms. For example, with the secure data parser integrated, a storage system may make use of the redundancy offered by the secure data parser (i.e., which is used to implement the feature of needing fewer than all separated portions of data in order to reconstruct the original data) to protect against data loss. The secure data parser also allows all data written to storage devices, whether using redundancy or not, to be in the form of multiple portions that are generated according to the parsing of the present invention. When original data is attempted to be accessed, the appropriate software, also integrated into the volume manager or other suitable component of the storage system, may recombine the parsed data portions into the original data in a way that may be transparent to the end user.

[0427] In one suitable approach, the secure data parser of the present invention may be integrated into a RAID controller (as either hardware or software). This allows for the secure storage of data to multiple drives while maintaining fault tolerance in case of drive failure.

[0428] The secure data parser of the present invention may be integrated into a database in order to, for example, protect sensitive table information. For example, in one suitable approach, data associated with particular cells of a database table (e.g., individual cells, one or more particular columns, one or more particular rows, any combination thereof, or an entire database table) may be parsed and separated according to the present invention (e.g., where the different portions are stored on one or more storage devices at one or more locations or on a single storage device).

Access to recombine the portions in order to view the original data may be granted by traditional authentication methods (e.g., username and password query).

[0429] The secure parser of the present invention may be integrated in any suitable system that involves data in motion (i.e., transfer of data from one location to another). Such systems include, for example, email, streaming data broadcasts, and wireless (e.g., WiFi) communications. With respect to email, in one suitable approach, the secure parser may be used to parse outgoing messages (i.e., containing text, binary data, or both (e.g., files attached to an email message)) and sending the different portions of the parsed data along different paths thus creating multiple streams of data. If any one of these streams of data is compromised, the original message remains secure because the system may require that more than one of the portions be combined, in accordance with the present invention, in order to generate the original data. In another suitable approach, the different portions of data may be communicated along one path sequentially so that if one portion is obtained, it may not be sufficient to generate the original data. The different portions arrive at the intended recipient's location and may be combined to generate the original data in accordance with the present invention.

[0430] FIGURES 27 and 28 are illustrative block diagrams of such email systems. FIGURE 28 shows a sender system 2700, which may include any suitable hardware, such as a computer terminal, personal computer, handheld device (e.g., PDA, Blackberry), cellular telephone, computer network, any other suitable hardware, or any combination thereof. Sender system 2700 is used to generate and/or store a message 2704, which may be, for example, an email message, a binary data file (e.g., graphics, voice, video, etc.), or both. Message 2704 is parsed and split by secure data parser 2702 in accordance with the present invention. The resultant data portions may be communicated across one or more separate communications paths 2706 over network 2708 (e.g., the Internet, an intranet, a LAN, WiFi, Bluetooth, any other suitable hard-wired or wireless communications means, or any combination thereof) to recipient system 2710. The data portions may be communicated parallel in time or alternatively, according to any suitable time delay between the communication of the different data portions. Recipient system 2710 may be any suitable hardware as described above

with respect to sender system 2700. The separate data portions carried along communications paths 2706 are recombined at recipient system 2710 to generate the original message or data in accordance with the present invention.

[0431] FIGURES 28 shows a sender system 2800, which may include any suitable hardware, such as a computer terminal, personal computer, handheld device (e.g., PDA), cellular telephone, computer network, any other suitable hardware, or any combination thereof. Sender system 2800 is used to generate and/or store a message 2804, which may be, for example, an email message, a binary data file (e.g., graphics, voice, video, etc.), or both. Message 2804 is parsed and split by secure data parser 2802 in accordance with the present invention. The resultant data portions may be communicated across a single communications paths 2806 over network 2808 (e.g., the Internet, an intranet, a LAN, WiFi, Bluetooth, any other suitable communications means, or any combination thereof) to recipient system 2810. The data portions may be communicated serially across communications path 2806 with respect to one another. Recipient system 2810 may be any suitable hardware as described above with respect to sender system 2800. The separate data portions carried along communications path 2806 are recombined at recipient system 2810 to generate the original message or data in accordance with the present invention.

[0432] It will be understood that the arrangement of FIGURES 27 and 28 are merely illustrative. Any other suitable arrangement may be used. For example, in another suitable approach, the systems of FIGURES 27 and 28 may be incorporated whereby the multi-path approach of FIGURE 28 is used and in which one or more of communications paths 2706 are used to carry more than one portion of data as communications path 2806 does in the context of FIGURE 29. In general

[0433] The secure data parser may be integrated at any suitable level of a data-in motion system. For example, in the context of an email system, the secure parser may be integrated at the user-interface level (e.g., into Microsoft® Outlook) in which case, the user may have control over the use of the secure data parser features when using email. Alternatively, the secure parser may be implemented in a back-end component such as at the exchange server, in which case, messages

may be automatically parsed, split, and communicated along different paths in accordance with the present invention without any user intervention.

[0434] Similarly, in the case of streaming broadcasts of data (e.g., audio, video), the outgoing data may be parsed and separated into multiple streams each containing a portion of the parsed data. The multiple streams may be transmitted along one or more paths and recombined at the recipient's location in accordance with the present invention. One of the benefits of this approach is that it avoids the relatively large overhead associated with traditional encryption of data followed by transmission of the encrypted data over a single communications channel. The secure parser of the present invention allows data in motion to be sent in multiple parallel streams, increasing speed and efficiency.

[0435] It will be understand that the secure data parser may be integrated for protection of and fault tolerance of any type of data in motion through any transport medium, including, for example, wired, wireless, or physical. For example, voice over Internet protocol (VoIP) applications may make use of the secure data parser of the present invention. Wireless or wired data transport from or to any suitable personal digital assistant (PDA) devices such as Blackberries and SmartPhones may be secured using the secure data parser of the present invention. Communications using wireless 802.11 protocols for peer to peer and hub based wireless networks, satellite communications, point to point wireless communications, Internet client/server communications, or any other suitable communications may involve the data in motion capabilities of the secure data parser in accordance with the present invention. Data communication between computer peripheral device (e.g., printer, scanner, monitor, keyboard, network router, biometric authentication device (e.g., fingerprint scanner), or any other suitable peripheral device) between a computer and a computer peripheral device, between a computer peripheral device and any other suitable device, or any combination thereof may make use of the data in motion features of the present invention.

[0436] The data in motion features of the present invention may also apply to physical transportation of secure shares using for example, separate routes, vehicles, methods, any other suitable physical transportation, or any combination

thereof. For example, physical transportation of data may take place on digital/magnetic tapes, floppy disks, optical disks, physical tokens, USB drives, removable hard drives, consumer electronic devices with flash memory (e.g., Apple IPODs or other MP3 players), flash memory, any other suitable medium used for transporting data, or any combination thereof.

[0437] The secure data parser of the present invention may provide security with the ability for disaster recovery. According to the present invention, fewer than all portions of the separated data generated by the secure data parser may be necessary in order to retrieve the original data. That is, out of m portions stored, n may be the minimum number of these m portions necessary to retrieve the original data, where n <= m. For example, if each of four portions is stored in a different physical location relative to the other three portions, then, if n=2 in this example, two of the locations may be compromised whereby data is destroyed or inaccessible, and the original data may still be retrieved from the portions in the other two locations. Any suitable value for n or m may be used.

[0438] In addition, the n of m feature of the present invention may be used to create a "two man rule" whereby in order to avoid entrusting a single individual or any other entity with full access to what may be sensitive data, two or more distinct entities, each with a portion of the separated data parsed by the secure parser of the present invention may need to agree to put their portions together in order to retrieve the original data.

[0439] The secure data parser of the present invention may be used to provide a group of entities with a group-wide key that allows the group members to access particular information authorized to be accessed by that particular group. The group key may be one of the data portions generated by the secure parser in accordance with the present invention that may be required to be combined with another portion centrally stored, for example in order to retrieve the information sought. This feature allows for, for example, secure collaboration among a group. It may be applied in for example, dedicated networks, virtual private networks, intranets, or any other suitable network.

[0440] Specific applications of this use of the secure parser include, for example, coalition information sharing in which, for example, multi-national friendly

government forces are given the capability to communicate operational and otherwise sensitive data on a security level authorized to each respective country over a single network or a dual network (i.e., as compared to the many networks involving relatively substantial manual processes currently used). This capability is also applicable for companies or other organizations in which information needed to be known by one or more specific individuals (within the organization or without) may be communicated over a single network without the need to worry about unauthorized individuals viewing the information.

[0441] Another specific application includes a multi-level security hierarchy for government systems. That is, the secure parser of the present invention may provide for the ability to operate a government system at different levels of classified information (e.g., unclassified, classified, secret, top secret) using a single network. If desired, more networks may be used (e.g., a separate network for top secret), but the present invention allows for substantially fewer than current arrangement in which a separate network is used for each level of classification.

[0442] It will be understood that any combination of the above described applications of the secure parser of the present invention may be used. For example, the group key application can be used together with the data in motion security application (i.e., whereby data that is communicated over a network can only be accessed by a member of the respective group and where, while the data is in motion, it is split among multiple paths (or sent in sequential portions) in accordance with the present invention).

[0443] The secure data parser of the present invention may be integrated into any middleware application to enable applications to securely store data to different database products or to different devices without modification to either the applications or the database. Middleware is a general term for any product that allows two separate and already existing programs to communicate. For example, in one suitable approach, middleware having the secure data parser integrated, may be used to allow programs written for a particular database to communicate with other databases without custom coding.

[0444] The secure data parser of the present invention may be implemented having any combination of any suitable capabilities, such as those discussed

herein. In some embodiments of the present invention, for example, the secure data parser may be implemented having only certain capabilities whereas other capabilities may be obtained through the use of external software, hardware, or both interfaced either directly or indirectly with the secure data parser.

[0445] FIGURE 30, for example, shows an illustrative implementation of the secure data parser as secure data parser 3000. Secure data parser 3000 is implemented with very few built-in capabilities. As illustrated, secure data parser 3000 may include built-in capabilities for parsing and splitting data into portions (also referred to herein as shares) of data using module 3002 in accordance with the present invention. Secure data parser 3000 may also include built in capabilities for performing redundancy in order to be able to implement, for example, the m of n feature described above (i.e., recreating the original data using fewer than all shares of parsed and split data) using module 3004. Secure data parser 3000 may also include share distribution capabilities using module 3006 for placing the shares of data into buffers from which they are sent for communication to a remote location, for storage, etc. in accordance with the present invention. It will be understood that any other suitable capabilities may be built into secure data parser 3000.

[0446] Assembled data buffer 3008 may be any suitable memory used to store the original data (although not necessarily in its original form) that will be parsed and split by secure data parser 3000. In a splitting operation, assembled data buffer 3008 provides input to secure data parser 3008. In a restore operation, assembled data buffer 3008 may be used to store the output of secure data parser 3000.

[0447] Split shares buffers 3010 may be one or more memory modules that may be used to store the multiple shares of data that resulted from the parsing and splitting of original data. In a splitting operation, split shares buffers 3010 hold the output of the secure data parser. In a restore operation, split shares buffers hold the input to secure data parser 3000.

[0448] It will be understood that any other suitable arrangement of capabilities may be built-in for secure data parser 3000. Any additional features may be built-in and any of the features illustrated may be removed, made more robust, made

less robust, or may otherwise be modified in any suitable way. Buffers 3008 and 3010 are likewise merely illustrative and may be modified, removed, or added to in any suitable way.

[0449] Any suitable modules implemented in software, hardware or both may be called by or may call to secure data parser 3000. If desired, even capabilities that are built into secure data parser 3000 may be replaced by one or more external modules. As illustrated, some external modules include random number generator 3012, cipher feedback key generator 3014, hash algorithm 3016, any one or more types of encryption 3018, and key management 3020. It will be understood that these are merely illustrative external modules. Any other suitable modules may be used in addition to or in place of those illustrated.

[0450] Cipher feedback key generator 3014 may, externally to secure data parser 3000, generate for each secure data parser operation, a unique key, or random number (using for example random number generator 3012), to be used as a seed value for an operation that extends an original session key size (e.g., a value of 128, 256, 512, or 1024 bits) into a value equal to the length of the data to be parsed and split. Any suitable algorithm may be used for the cipher feedback key generation, including, for example, the AES cipher feedback key generation algorithm.

[0451] In order to facilitate integration of secure data parser 3000 and its external modules (i.e., secure data parser layer 3026) into an application layer 3024 (e.g., email application, database application, etc.), a wrapping layer that may make use of, for example, API function calls may be used. Any other suitable arrangement for facilitating integration of secure data parser layer 3026 into application layer 3024 may be used.

[0452] FIGURE 31 illustratively shows how the arrangement of FIGURE 30 may be used when a write (e.g., to a storage device), insert (e.g., in a database field), or transmit (e.g., across a network) command is issued in application layer 3024. At step 3100 data to be secured is identified and a call is made to the secure data parser. The call is passed through wrapper layer 3022 where at step 3102, wrapper layer 3022 streams the input data identified at step 3100 into assembled data buffer 3008. Also at step 3102, any suitable share information, filenames, any

other suitable information, or any combination thereof may be stored (e.g., as information 3106 at wrapper layer 3022). Secure data processor 3000 then parses and splits the data it takes as input from assembled data buffer 3008 in accordance with the present invention. It outputs the data shares into split shares buffers 3010. At step 3104, wrapper layer 3022 obtains from stored information 3106 any suitable share information (i.e., stored by wrapper 3022 at step 3102) and share location(s) (e.g., from one or more configuration files). Wrapper layer 3022 then writes the output shares (obtained from split shares buffers 3010) appropriately (e.g., written to one or more storage devices, communicated onto a network, etc.).

[0453] FIGURE 32 illustratively shows how the arrangement of FIGURE 30 may be used when a read (e.g., from a storage device), select (e.g., from a database field), or receive (e.g., from a network) occurs. At step 3200, data to be restored is identified and a call to secure data parser 3000 is made from application layer 3024. At step 3202, from wrapper layer 3022, any suitable share information is obtained and share location is determined. Wrapper layer 3022 loads the portions of data identified at step 3200 into split shares buffers 3010. Secure data parser 3000 then processes these shares in accordance with the present invention (e.g., if only three of four shares are available, then the redundancy capabilities of secure data parser 3000 may be used to restore the original data using only the three shares). The restored data is then stored in assembled data buffer 3008. At step 3204, application layer 3022 converts the data stored in assembled data buffer 3008 into its original data format (if necessary) and provides the original data in its original format to application layer 3024.

[0454] It will be understood that the parsing and splitting of original data illustrated in FIGURE 31 and the restoring of portions of data into original data illustrated in FIGURE 32 is merely illustrative. Any other suitable processes, components, or both may be used in addition to or in place of those illustrated.

[0455] FIGURE 33 is a block diagram of an illustrative process flow for parsing and splitting original data into two or more portions of data in accordance with one embodiment of the present invention. As illustrated, the original data desired to be parsed and split is plain text 3306 (i.e., the word "SUMMIT" is used as an example). It will be understood that any other type of data may be parsed and split

in accordance with the present invention. A session key 3300 is generated. If the length of session key 3300 is not compatible with the length of original data 3306, then cipher feedback session key 3304 may be generated.

[0456] In one suitable approach, original data 3306 may be encrypted prior to parsing, splitting, or both. For example, as FIGURE 33 illustrates, original data 3306 may be XORed with any suitable value (e.g., with cipher feedback session key 3304, or with any other suitable value). It will be understood that any other suitable encryption technique may be used in place of or in addition to the XOR technique illustrate. It will further be understood that although FIGURE 33 is illustrated in terms of byte by byte operations, the operation may take place at the bit level or at any other suitable level. It will further be understood that, if desired, there need not be any encryption whatsoever of original data 3306.

[0457] The resultant encrypted data (or original data if no encryption took place) is then hashed to determine how to split the encrypted (or original) data among the output buckets (e.g., of which there are four in the illustrated example). In the illustrated example, the hashing takes place by bytes and is a function of cipher feedback session key 3304. It will be understood that this is merely illustrative. The hashing may be performed at the bit level, if desired. The hashing may be a function of any other suitable value besides cipher feedback session key 3304. In another suitable approach, hashing need not be used. Rather, any other suitable technique for splitting data may be employed.

[0458] FIGURE 34 is a block diagram of an illustrative process flow for restoring original data 3306 from two or more parsed and split portions of original data 3306 in accordance with one embodiment of the present invention. The process involves hashing the portions in reverse (i.e., to the process of FIGURE 33) as a function of cipher feedback session key 3304 to restore the encrypted original data (or original data if there was no encryption prior to the parsing and splitting). The encryption key may then be used to restore the original data (i.e., in the illustrated example, cipher feedback session key 3304 is used to decrypt the XOR encryption by XORing it with the encrypted data). This the restores original data 3306.

[0459] FIGURE 35 shows how bit-splitting may be implemented in the example of FIGURES 33 and 34. A hash may be used (e.g., as a function of the cipher feedback session key, as a function of any other suitable value) to determine a bit value at which to split each byte of data. It will be understood that this is merely one illustrative way in which to implement splitting at the bit level. Any other suitable technique may be used.

[0460] It will be understood that any reference to hash functionality made herein may be made with respect to any suitable hash algorithm. These include for example, MD5 and SHA-1. Different hash algorithms may be used at different times and by different components of the present invention.

[0461] After a split point has been determined in accordance with the above illustrative procedure or through any other procedure or algorithm, a determination may be made with regard to which data portions to append each of the left and right segments. Any suitable algorithm may be used for making this determination. For example, in one suitable approach, a table of all possible distributions (e.g., in the form of pairings of destinations for the left segment and for the right segment) may be created, whereby a destination share value for each of the left and right segment may be determined by using any suitable hash function on corresponding data in the session key, cipher feedback session key, or any other suitable random or pseudo-random value, which may be generated and extended to the size of the original data. For example, a hash function of a corresponding byte in the random or pseudo-random value may be made. The output of the hash function is used to determine which pairing of destinations (i.e., one for the left segment and one for the right segment) to select from the table of all the destination combinations. Based on this result, each segment of the split data unit is appended to the respective two shares indicated by the table value selected as a result of the hash function.

[0462] Redundancy information may be appended to the data portions in accordance with the present invention to allow for the restoration of the original data using fewer than all the data portions. For example, if two out of four portions are desired to be sufficient for restoration of data, then additional data from the shares may be accordingly appended to each share in, for example, a

round-robin manner (e.g., where the size of the original data is 4MB, then share 1 gets its own shares as well as those of shares 2 and 3; share 2 gets its own share as well as those of shares 3 and 4; share 3 gets its own share as well as those of shares 4 and 1; and share 4 gets its own shares as well as those of shares 1 and 2). Any such suitable redundancy may be used in accordance with the present invention.

[0463] It will be understood that any other suitable parsing and splitting approach may be used to generate portions of data from an original data set in accordance with the present invention. For example, parsing and splitting may be randomly or pseudo-randomly processed on a bit by bit basis. A random or pseudo-random value may be used (e.g., session key, cipher feedback session key, etc.) whereby for each bit in the original data, the result of a hash function on corresponding data in the random or pseudo-random value may indicate to which share to append the respective bit. In one suitable approach the random or pseudo-random value may be generated as, or extended to, 8 times the size of the original data so that the hash function may be performed on a corresponding byte of the random or pseudo-random value with respect to each bit of the original data. Any other suitable algorithm for parsing and splitting data on a bit by bit level may be used in accordance with the present invention. It will further be appreciated that redundancy data may be appended to the data shares such as, for example, in the manner described immediately above in accordance with the present invention.

[0464] In one suitable approach, parsing and splitting need not be random or pseudo-random. Rather, any suitable deterministic algorithm for parsing and splitting data may be used. For example, breaking up the original data into sequential shares may be employed as a parsing and splitting algorithm. Another example is to parse and split the original data bit by bit, appending each respective bit to the data shares sequentially in a round-robin manner. It will further be appreciated that redundancy data may be appended to the data shares such as, for example, in the manner described above in accordance with the present invention.

[0465] In one embodiment of the present invention, after the secure data parser generates a number of portions of original data, in order to restore the original data, certain one or more of the generated portions may be mandatory. For example, if one of the portions is used as an authentication share (e.g., saved on a

physical token device), and if the fault tolerance feature of the secure data parser is being used (i.e., where fewer than all portions are necessary to restore the original data), then even though the secure data parser may have access to a sufficient number of portions of the original data in order to restore the original data, it may require the authentication share stored on the physical token device before it restores the original data. It will be understood that any number and types of particular shares may be required based on, for example, application, type of data, user, any other suitable factors, or any combination thereof.

[0466] In one suitable approach, the secure data parser or some external component to the secure data parser may encrypt one or more portions of the original data. The encrypted portions may be required to be provided and decrypted in order to restore the original data. The different encrypted portions may be encrypted with different encryption keys. For example, this feature may be used to implement a more secure "two man rule" whereby a first user would need to have a particular share encrypted using a first encryption and a second user would need to have a particular share encrypted using a second encryption key. In order to access the original data, both users would need to have their respective encryption keys and provide their respective portions of the original data. In one suitable approach, a public key may be used to encrypt one or more data portions that may be a mandatory share required to restore the original data. A private key may then be used to decrypt the share in order to be used to restore to the original data.

[0467] Any such suitable paradigm may be used that makes use of mandatory shares where fewer than all shares are needed to restore original data.

[0468] In one suitable embodiment of the present invention, distribution of data into a finite number of shares of data may be processed randomly or pseudo-randomly such that from a statistical perspective, the probability that any particular share of data receives a particular unit of data is equal to the probability that any one of the remaining shares will receive the unit of data. As a result, each share of data will have an approximately equal amount of data bits.

[0469] According to another embodiment of the present invention, each of the finite number of shares of data need not have an equal probability of receiving

units of data from the parsing and splitting of the original data. Rather certain one or more shares may have a higher or lower probability than the remaining shares. As a result, certain shares may be larger or smaller in terms of bit size relative to other shares. For example, in a two-share scenario, one share may have a 1% probability of receiving a unit of data whereas the second share has a 99% probability. It should follow, therefore that once the data units have been distributed by the secure data parser among the two share, the first share should have approximately 1% of the data and the second share 99%. Any suitable probabilities may be used in accordance with the present invention.

[0470] It will be understood that the secure data parser may be programmed to distribute data to shares according to an exact (or near exact) percentage as well. For example, the secure data parser may be programmed to distribute 80% of data to a first share and the remaining 20% of data to a second share.

[0471] According to another embodiment of the present invention, the secure data parser may generate data shares, one or more of which have predefined sizes. For example, the secure data parser may split original data into data portions where one of the portions is exactly 256 bits. In one suitable approach, if it is not possible to generate a data portion having the requisite size, then the secure data parser may pad the portion to make it the correct size. Any suitable size may be used.

[0472] In one suitable approach, the size of a data portion may be the size of an encryption key, a splitting key, any other suitable key, or any other suitable data element.

[0473] As previously discussed, the secure data parser may use keys in the parsing and splitting of data. For purposes of clarity and brevity, these keys shall be referred to herein as "splitting keys." For example, the Session Master Key, previously introduced, is one type of splitting key. Also, as previously discussed, splitting keys may be secured within shares of data generated by the secure data parser. Any suitable algorithms for securing splitting keys may be used to secure them among the shares of data. For example, the Shamir algorithm may be used to secure the splitting keys whereby information that may be used to reconstruct a

splitting key is generated and appended to the shares of data. Any other such suitable algorithm may be used in accordance with the present invention.

[0474] Similarly, any suitable encryption keys may be secured within one or more shares of data according to any suitable algorithm such as the Shamir algorithm. For example, encryption keys used to encrypt a data set prior to parsing and splitting, encryption keys used to encrypt a data portions after parsing and splitting, or both may be secured using, for example, the Shamir algorithm or any other suitable algorithm.

[0475] According to one embodiment of the present invention, an All or Nothing Transform (AoNT), such as a Full Package Transform, may be used to further secure data by transforming splitting keys, encryption keys, any other suitable data elements, or any combination thereof. For example, an encryption key used to encrypt a data set prior to parsing and splitting in accordance with the present invention may be transformed by an AoNT algorithm. The transformed encryption key may then be distributed among the data shares according to, for example, the Shamir algorithm or any other suitable algorithm. In order to reconstruct the encryption key, the encrypted data set must be restored (e.g., not necessarily using all the data shares if redundancy was used in accordance with the present invention) in order to access the necessary information regarding the transformation in accordance with AoNTs as is well known by one skilled in the art. When the original encryption key is retrieved, it may be used to decrypt the encrypted data set to retrieve the original data set. It will be understood that the fault tolerance features of the present invention may be used in conjunction with the AoNT feature. Namely, redundancy data may be included in the data portions such that fewer than all data portions are necessary to restore the encrypted data set.

[0476] It will be understood that the AoNT may be applied to encryption keys used to encrypt the data portions following parsing and splitting either in place of or in addition to the encryption and AoNT of the respective encryption key corresponding to the data set prior to parsing and splitting. Likewise, AoNT may be applied to splitting keys.

[0477] In one embodiment of the present invention, encryption keys, splitting keys, or both as used in accordance with the present invention may be further encrypted using, for example, a workgroup key in order to provide an extra level of security to a secured data set.

[0478] In one embodiment of the present invention, an audit module may be provided that tracks whenever the secure data parser is invoked to parse and/or split data.

[0479] FIGURE 36 depicts an exemplary bit-splitting technique 3600 in accordance with the present disclosure. A session key 3606 may be used for bit-splitting, and may be created as described herein, or in accordance with any technique as understood in the art. For example, a session master key 3604 may be XORed with an initial session key 3602 to create the session key 3606. The session key 3606 may be key expanded, such as by using ANSI X9.82 as a cryptographically secure pseudo-random number generator and an RC4 type technique for randomizing the order. ANSI x9.82 and RC4 are merely exemplary, and any key expansion technique known in the art may be used. The key expansion may be performed in a manner such that if any M of the N expanded keys are recovered, the entire expanded session key 3606 may be reconstructed.

[0480] An exemplary byte of data 3608 to be split by the bit-splitting may be the ASCII character, "S" (*i.e.*, 01010011). A byte of the expanded session key 3606, such as the first session key byte 3610 (82 or 01010010) may optionally be XORed with the byte of data 3608 to produce data 3612. If session key byte 3610 is not XORed with data 3608, data 3608 may be used in subsequent steps as data 3612. Session key byte 3610 may be right shifted to produce a split point. In one exemplary embodiment, session key byte 3610 may be right shifted by five bits to produce a split point of 2 or 00000010. The split point may be used to create two masks that separate byte 3612 into two portions. In this example the split point is two, and the two lowest significant bits may be set to 1 to create mask 3616 (00000011) while the remaining six most significant bits may be set to 1 to create mask 3614 (11111100). The result of ANDing byte 3612 with masks 3614 and 3616 and discarding the 0-mask bytes is to create left split 3618 (six most

significant bits of data 3612) and right split 3620 (two least significant bits of data 3612).

[0481] A feedback value 3622 may be selected, such as by a 4-byte look ahead within session key 3606. An exemplary feedback value 3622 may be 99 or 01100011. The same split point (and masks 3614 and 3616) may be used to separate the feedback value 3622 into a left feedback value 3624 (six most significant bits of feedback value 3622) and a right feedback value 3626 (two least significant bits of feedback value 3622). The left feedback value 3624 may be XORed with the left split 3618 to create split value left 3628. The right feedback value 3626 may be XORed with the right split 3620 to create split value right 3630. Split value left 3628 and split value right 3630 may be distributed to shares as described herein.

[0482] FIGURE 37 depicts a data flow 3700 for distributing the output of the bit-splitting process 3600 (split value right 3630 and split value left 3628) to one or more of shares 3704, 3706, 3708, and 3710. The bytes of DK 3702 may indicate the distribution of data to respective shares 3704, 3706, 3708, and 3710. For example, the first bit of DK 3702 may correspond to share 3704, the second bit of DK 3702 may correspond to share 3706, the third bit of DK 3702 may correspond to share 3708, and the fourth bit of DK 3702 may correspond to share 3710. An exemplary first DK byte 3702 (*e.g.*, 0011) may result in the distribution of split value right 3630 to share 3704 and the distribution of split value left 3628 to share 3706.

[0483] Bit splitting as described herein may be used with various M-of-N share recovery configurations. For example, the distribution may be a 4 of 4 split such that all shares must be recovered for the underlying keys and data to be recovered. The session key 3606 may be divided into 4 parts, with each part distributed to one of the four shares 3704, 3706, 3708, and 3710. Alternatively, the session keys described herein may be expanded such that the resulting bit split distribution will allow the data to be recovered from M shares where M < N, e.g., a 2 of 4 key expansion or 3 of 4 key expansion.

[0484] Another exemplary technique for the distribution of data into shares may be a bit scatter technique as depicted in FIGURE 38. The bit scatter technique may

separate a stream of input bytes into separate output streams by bit. A master session key 3802 may be M of N expanded to create a session key 3804 with N key elements and equal in length to the number of data 3806 bytes times 8. Each session key 3804 element may be associated with a share 3808 and may include an array of integer values. Each integer value may correspond to a bit position within each byte of input data 3806 to be scattered.

[0485] Bits may be scattered to shares by iterating through the integer values of an element of session key 3804. The selection of which bits of data 3806 will be assigned to a share 3808 as well as the order in which they are assigned may be based on the integer value from the element of session key 3804 associated with a particular share as described below. An exemplary session key 3804 element may have integer values 2, 4, 3, 7, and 1 respectively. The integer value of 2 from the session key 3804 element may indicate that the value from the second bit of each byte of data 3806 may be distributed to the first bit location of share 3808. The integer value of 4 from the session key 3804 element may indicate that the value from the fourth bit of data 3806 may be distributed to the next bit of share 3808, and so on for values 3, 7, and 1 of the session key 3804 element. This process may be repeated until each bit of data 3806 has been distributed to the share 3808 based on the session key 3804 element. The process may then be repeated on data 3806 for each respective share and associated session key element.

[0486] FIGURE 39 depicts restoring the portion of a byte of data 3906 that was distributed to a share 3908 using the bit scatter technique. The master session key 3902 may be established or recovered as is described herein, e.g., by recovering a key distributed among shares. Master session key 3902 may be M of N key expanded to create session key 3904 (which may match the session key used to scatter the bits originally) having elements associated with shares as described herein. The integer values of the session key 3904 elements may be used to extract bits from the shares to recreate data 3906. The first integer value of 2 from the session key 3904 element may indicate that the first bit from share 3908 may be distributed to the second bit of data 3906. The second integer value of 4 from the session key 3904 element may indicate that the second bit from share 3908 may be distributed to the fourth bit of data 3906, and so on for the values 3, 7, and 1 of the

session key 3904 element associated with share 3908. This process may be continued for share 3908 until all of the bits from the share 3908 are distributed to data 3906, and then repeated in its entirety for each additional share based on the element of session key 3904 associated with that share.

[0487] Any key expansion technique known in the art may be used to create the expanded session keys associated with the distribution of data to shares and reconstruction of data from shares. An exemplary M of N key expansion utilizing ANSI X9.82 as a cryptographically secure pseudo-random number generator and an RC4 type technique for randomizing the order will be discussed below with respect to performing a 2 of 4 key expansion for use with a bit scatter technique. A master session key may feed the ANSI X9.82 cryptographically secure pseudo-random number generator to create key value k. In an exemplary embodiment the X9.82 technique may be operating in AES-OFB (output feedback) mode. Each resulting k may have a length (K_{len}) equivalent to the length of the plain text data input, padded for AES as necessary, plus 4. The key blocks k may be created based on the master key (MK) and the key length (K_{len}) as represented by k = aes_ofb(MK, aes_pad_length (K_{len})).

[0488] An array of integers S may be instantiated in a manner such that the order of the integers S corresponds to the order of the plain text data. The array may be initialized from S_0, S_1, . . . S_{len}, where the key length is assumed to be equal to the length (len) of the array S. The integer values S may then be randomized based on the key k. Counters i,j, and x may be initially set to 0, and the elements of array S swapped according to the following:

```
for (i … len)
        j = (j + k_x + S_i) mod len
        swap ( S[i], S[j])
                x++;
```

[0489] The resulting randomized S values may be utilized to create the expanded session key elements SK_0 . . . SK_N, each associated with a corresponding share of the N shares. In order to create an M of N share distribution such that there is sufficient overlap of the scattered data for the data can be recovered from any M of N shares, a ratio may be computed as follows: ratio = 1 – (1/N)*(M-1). In the case

of a 2 of 4 key split, the ratio may equal 1 – (1/4)*(2-1) or 75%. The randomized S values may then be allocated to each of session keys $SK_0 \ldots SK_N$ based on the ratio, with each successive copying from the randomized S values beginning where the previous session key SK left off, and looping back to the beginning of the randomized S array as necessary. An example of such an allocation for a 2 of 4 key split with a ratio of 75% is depicted in FIGURE 40. SK1 may be the initial 75% of the S array, SK2 the final 25% and initial 50% of the S array, SK3 the final 50% and initial 25% of the S array, and SK4 the final 75% of the S array. Once the session keys $SK_0 \ldots SK_N$ are created, each may then be re-randomized with a random nonce n in accordance with the following:

```
for (SK0 ... SKN)
        i = j = x =0;
        for (i … len)
                j = (j + nx + Si) mod len
                swap ( S[i], S[j])
                x= (x+1) mod keylen;
```

[0490] The resulting SK values may then be utilized as the expanded session key elements for use in data splitting as described herein.

[0491] Another exemplary technique for the distribution of data into shares may be a block split technique. Data such as a file that is to be split and distributed to shares may include blocks, *i.e.*, consecutive groupings of a fixed number of bits. Examples of block sizes may include 128, 192, or 256. A segment may be a group of blocks that is utilized in the block split technique. If L represents the number of mandatory shares, M represents the number of non-mandatory shares necessary to recover a file, and N represents the total number of non-mandatory shares, a file may be split into L + C(N,M-1) segments, where C(N,M-1) denotes the binomial coefficient N choose M-1. If a file is split into L + C(N,M-1) segments, the file may not be recovered unless all L mandatory shares and at least M non-mandatory shares are recovered.

[0492] Blocks may be assigned to segments based on any appropriate technique. For example, F may be the number of blocks in a file being split. Segmenting values a and b may be calculated according to the following:

$$a = \left\lfloor \frac{F}{\binom{N-1}{M-1} \cdot \left(\frac{N}{N-M+1} + L \right)} \right\rfloor = \left\lfloor \frac{F}{\binom{N}{M-1} + \binom{N-1}{M-1} \cdot L} \right\rfloor \quad b = a \cdot \binom{N}{M-1}$$

[0493] Blocks are assigned to segments such that each ith segment contains blocks (a * i) through (a(i+1)-1) for all i segments where i<C(N,M-1). The remaining L segments may be partitioned evenly from the end of the file and contain blocks b + [(F-b)*(i-C(N,M-1))/L] through b + [(F-b)*((i+1) – C(N,M-1))/L]-1, inclusive.

[0494] The last L segments of the file may be assigned to the L mandatory shares with one segment per share. The first C(N,M-1) segments may be assigned to the N non-mandatory shares by first enumerating all C(N,M-1) possibilities of the (M-1)-element subsets of {0, 1, …, N-1} in lexicographical order. If and only if the ith (M-1)-element subset does not include the element j, then the jth non-mandatory share will contain segment i. Based on this distribution, every possible combination of M-1 non-mandatory shares is missing at least one of the C(N,M-1) segments, while every collection of M non-mandatory shares includes all C(N,M-1) segments.

[0495] Each share may include a preamble. An exemplary preamble may have a first line including six space-separated integers: (1) i; (2) L; (3) M; (4) N; (5) C(N-1,M-1); and (6) the size of a block in bits. Lines 1+i (for i<C(N-1,M-1)) may correspond to each segment stored in the share, and may include three space-separated integers relating to the segment: (1) the segment number; (2) the number of the first block in the segment; and (3) the number of the last block in the segment. If the share is mandatory, the preamble may be the same except it only contains two lines.

[0496] To recover the data, the shares may be joined if all L mandatory shares and at least M non-mandatory shares have been received. This may be determined by examining the share preambles to insure that all L + C(N,M-1) segments are present in the received shares. Shares may be written out based on the offsets indicating the location of segments within the shares.

[0497] Another exemplary technique for the distribution of data into shares may be a bit segment technique. For purposes of the bit segment technique, a segment is

a group of bits that is used for purposes of the splitting and joining process. Splittable data such as a file may split into C(N+L,M-1) segments, such that the file cannot be recovered from any less than L+M shares. Segmenting values a and b may be calculated according to the following:

$$a = \left\lfloor \frac{F}{\binom{N-1}{M-1}\cdot\left(\frac{N}{N-M+1}+L\right)} \right\rfloor = \left\lfloor \frac{F}{\binom{N}{M-1}+\binom{N-1}{M-1}\cdot L} \right\rfloor \quad b = a\cdot\binom{N}{M-1}$$

[0498] An offset S may be equal to C(N,M-1). For i=0 to C(N,M-1)-1, the ith segment may contain bits i, S+i, 2*S+i, …, a*S+i. Segments for the L mandatory shares may be computed by dividing the remaining (b*L) bits such that a mandatory share j may contain bits (a+1)*S+j, (a+1)*S+L+j, (a+1)*S+2L+j, …, (a+1)*S+bL+j.

[0499] The first C(N,M-1) segments may be assigned to the N non-mandatory shares by enumerating all C(N,M-1) possibilities of the (M-1)-element subsets of {0, 1, …, N-1} in lexicographical order. The remaining L segments are then assigned to the L mandatory shares. Bits may be distributed from chunks of C(N,M-1) bits, wherein each chunk contains one bit from each segment. The chunks may be parsed sequentially one bit at a time, with each bit written to the share assigned to its segment.

[0500] Each share i may include a preamble. An exemplary preamble may include a first line including six space-separated integers: (1) i; (2) L; (3) M; (4) N; (5) C(N-1,M-1); and (6) the size of a block in bits. Lines 1+i (for i<C(N-1,M-1)) may each include three space-separated integers for each segment assigned to the share: (1) the segment number; (2) the number of the first bit in the segment; and (3) the number of total bits in the segment. If the share is mandatory, the preamble may be the same except it only contains two lines.

[0501] The shares may be joined if all L mandatory shares and at least M non-mandatory shares have been received. This may be determined by examining the share preambles to insure that all L + C(N,M-1) segments are present in the received shares. Shares may be written out based on the offsets indicating the location of segments within the shares.

[0502] FIGURE 41 shows illustrative overview process 4100 for using the secure data parser of the present invention in some embodiments. The secure data parser may be compliant with Federal Information Processing Standards (FIPS) such as FIPS 140-2, including but not limited to standards relating to data encryption, key storage techniques, and cryptographically secure pseudo-random number generation. As described above, two well-suited functions for secure data parser 4106 may include encryption 4102 of data for storage or transmission and backup 4104 (*e.g.*, backup tapes, mirroring, RAID). As such, secure data parser 4106 may be integrated with a RAID or backup system, a file storage system, a data transmission system, or a hardware or software encryption engine in some embodiments. The secure data parser may be modular in nature, allowing for any known technique to be used within each of the function blocks shown in FIGURE 41. For example, AES encryption could be replaced by other known encryption techniques such as Triple DES (3DES).

[0503] The processes associated with secure data parser 4106 may include one or more of pre-encryption process 4108, encrypt/transform process 4110, key secure process 4112, parse/distribute process 4114, fault tolerance process 4116, share authentication process 4118, and post-encryption process 4120. These processes may be executed in several suitable orders or combinations. The combination and order of processes used may depend on the particular application or use, the level of security desired, whether optional pre-encryption, post-encryption, or both, are desired, the redundancy desired, the capabilities or performance of an underlying or integrated system, or any other suitable factor or combination of factors.

[0504] Pre-encryption process 4108 may operate independently and prior to any encryption of the data splitting process, and may utilize encryption techniques described herein or known in the art, including AES (FIPS 197), DES, and 3DES. Meta-data such as the file name, file length, creation/modification dates, and any other host-specific file information may be pre-pended to the data prior to pre-encryption. The key for pre-encryption may be generated by the system, or may be provided by an external system. Keys may be symmetric or may include public/private key pairs such as RSA public/private key, DSA public private key, and ECDSA public/private key. Pre-encryption process may also include the

generation of a MAC or digital signal for the pre-encrypted data as described herein.

[0505] Encryption/transform 4110 process may receive pre-encrypted or non-encrypted data. Encryption/transform 4110 process may perform key generation, data encryption, and key transform steps as described herein. For example, AES encryption may be used with a cryptographically secure pseudo-random number generator to create a 128, 192, or 256-bit key. That key may be used to encrypt data using AES cipher modes such as AES counter (AES-CTR) or AES cipher block chaining (AES-CBC). Utilizing non-sequential encryption modes such as AES-CTR may allow for parallel processing of data, which may allow faster multi-processing of data. The key may then be transformed for splitting and storage such as with a package transform or AoNT as described herein.

[0506] Key secure process 4112 may control the splitting and distribution of the key to shares, such as through a Shamir key distribution or other key distribution techniques as described herein. Parse/distribute process 4114 may split data according to a technique such as bit split, block segment, bit scatter, or block split. The split data may in turn be assigned to shares as described herein and based on the type of splitting technique used. The operation of the splitting technique and assignment of split data and split keys to shares may also be dependent on the M of N fault tolerance employed by fault tolerance process 4116 in a particular embodiment. A N of N embodiment may provide for a higher level of data security, since all shares must be received to recover the underlying keys and data. A M of N embodiment may provide redundancy. In addition, fault tolerance process 4116 may also implement mandatory shares L that must be recovered even in a M of N embodiment.

[0507] Share authentication process 4118 may provide integrity, authentication and digital signature functionality for information to be distributed to shares. Integrity information may include computing share integrity information as described herein, such as by utilizing a SHA-256 (FIPS 180-2) hash and computing a hash tree. Authentication may include the generating of a MAC for each share, *e.g.*, based on the underlying data, the initialization vector, and any attached meta-data for the share. A shared secret MAC key may be any appropriate key as is

known in the art, which may in turn be used as a key for a MAC technique such as HMAC-SHA1 (FIPS 198) to produce, *e.g.*, a 160-bit MAC tag. Shares may also be signed by a digital signature technique for authentication of the sender. The sending party may utilize FIPS PUB 186-2 signature techniques such as ECDSA using 384/512-bit curves or DSA using a modulus size of 512-1024 bits to sign the share using a private signing key. Other example signature techniques include RSASSA-PSSA.

[0508] Post-encryption process 4120 may optionally operate to further encrypt the shares, including data, meta-data, keys, initialization vector, and any integrity, authentication or signature information. Encryption techniques used by post-encryption process 4120 may include those described herein and known in the art, including AES, DES, and 3DES. The key for post-encryption may be generated by the system, may be provided by a user, or may be provided by an external system, and may include symmetric or public/private key pairs such as RSA public/private key, DSA public private key, and ECDSA public/private key. Each post-encrypted share may also include additional authenticity or integrity information.

[0509] As noted above, pre-encryption process and post-encryption process may be optional. In addition, because data parsing provided by parse/distribute process 4114 provides security unless all required shares are discovered, any encryption performed by the data parser may also be optional. Also, any of the encryption processes may be performed on only some portion of the data, *e.g.*, such that only a subset of the data or shares is encrypted, and thus reduce any burdens of the encryption processes.

[0510] FIGURE 42 depicts an exemplary secure parser 4200. The secure parser core 4202 isolates the functions of data splitting (*e.g.*, share creation, redundancy, and distribution to share buffers) into a callable module. Data may be placed in assembled data buffer 4204 to be split and the secure parser core 4202 may be invoked. The resulting shares may be placed into the split share buffers 4206 to be securely stored (storage 4216) or transmitted (communications 4218) by the host application. Cryptographic functions may be external calls for the secure parser core 4202. This may allow for the custom integration of various cryptographic

libraries, giving flexibility for "bolting on" other encryption modules, key management systems, random number generators, etc. as needed.

[0511] Random number generator 4208 may, for each split operation, generate a unique random value to be used as the basis for the split. Random numbers may be generated in a number of ways, via software program or hardware interface. AES encryption module 4210 may utilize encryption such as AES-CTR or AES-CBC for encryption operations for the secure parser core 4202. Encryption module 4212 may be an external encryption process that may provide functionality for pre-encrypting data prior to splitting or post-encrypting data after splitting. Key management system 4214 may provide for external key management for keys utilized in the encryption and/or splitting operations of the secure parser.

[0512] FIGURE 43 depicts an exemplary integration of the secure parser 4308 into a system 4300 utilizing an Application Programming Interface (API). A secure parser 4308 may include a secure parser core 4302, split share buffers 4310, and assembled data buffer 4312. API/Wrapper Layer 4304 may be an integration layer that interfaces with an application 4306. API/Wrapper Layer 4304 may define the location of shares, such as paths to send the information or storage devices to store the shares. API/Wrapper Layer 4304 may also define the naming convention of the resulting data, or parameters to store with the information such as row, column, and table ID in the case of a database application or the original filename in the case of unstructured data such as documents, images, maps, multimedia, or streaming data. API/Wrapper Layer 4304 may also handle the streaming of data to the secure parser 4308 and secure storage or communications of the resulting shares.

[0513] Application 4306 may select data to be secured and call the secure parser. API/Wrapper layer 4304 may stream input data into assembled data buffer 4312 and save filename and share information relating to the data. Assembled data buffer 4312 may provide data to secure parser core 4302 which may create shares, implement redundancy, and assign shares to locations for distribution as described herein. The shares to be distributed may be output to split share buffer 4310 which may provide the shares to API/Wrapper Layer 4304.

[0514] The various operations described herein may be chosen to match the threat and risk scenario for particular data, creating over a thousand different configuration options for a secure parser. Data may be pre-encrypted before it is parsed into shares, and/or post-encrypted after shares are created. Keys utilized in parsing may be transformed such as by the AoNT transform or package transform. Data parsing can be by various techniques such as bit split, block split, bit scatter, bit segment, block shuffle, or ordered block. The encryption utilized in the parsing technique may include various AES modes as described herein (*e.g.*, AES-CTR) or DES/3DES encryption, and keys used in encryption and or parsing of data may be various lengths such as 128, 296, or 256 bits. Fault tolerance may be implemented in various manners such as N of N, M of N, or parity. Keys may be secured such as with a Shamir key splitting technique or other techniques, including external splitting techniques. Integrity information may be provided and shares may be authenticated utilizing a hash, a MAC and/or a digital signature.

[0515] FIGURE 44 depicts an example configuration of a 2 of 3 share fault tolerance system. Data 4408 may be created locally at Site A 4402. A secure parser may secure and split each block of data 4408 from Site A 4402 and distribute 66% of the split data to each of Site A 4402, Site B 4404, and Site C 4406. The original data may be recovered from any 2 or 3 of shares 4410, 4412, and 4414.

[0516] FIGURE 45 depicts an example configuration of a 2 of 3 share fault tolerance system with a mandatory share 4512. Data 4508 may be created locally at Site A 4502. The secure parser may secure and split each block of data 4508 from Site A 4502, store 1% of the data locally at share 4510, distribute 99% to share 4512 at Site B 4504, and distribute 1% to share 4514 at Site C 4506. In order to recover the original data, share 4512 must be recovered from Site B 4504, and either one of share 4510 from Site A 4502 or share 4514 from Site C 4506 must be recovered. Data may be recovered to cleartext, *e.g.*, at Site B 4504.

[0517] FIGURE 46 depicts a flowchart 4600 of aspects of encrypt/transform process 4110, key secure process 4112, parse/distribute process 4114, fault tolerance process 4116, and share authentication process 4118. Input data 4602 to be split may be received. The received input data 4602 may be un-encrypted data

or may have optionally been pre-encrypted using AES or other encryption techniques as described herein or known in the art. The received input data 4602 may then be encrypted using an encryption technique such as AES. A session key 4604 may be generated using a random number generator such as a cryptographically secure pseudo-random number generator. In the example of AES encryption, the session key 4604 length may be 128, 192, or 256 bits. AES encryption may use any known AES technique such as AES-ENC or AES DEC, and may operate in any known cipher mode such as AES electronic codebook (AES-ECB), AES cipher block chaining (AES-CBC), AES output feedback (AES-OFB), AES Counter (AES-CTR), AES cipher feedback (AES-CFB), or any other cipher mode that is known in the art.

[0518] Depending on the type of AES cipher mode utilized for encryption, input data 4602 may be padded until it is equal in size to an integer number of AES blocks. The padding may consist of a 1-bit followed by 0-bits. The padded input data 4602 may be split into n blocks 4606. An initialization vector (IV) may be generated using a cryptographically secure pseudo-random number generator, and the n blocks 4606 may then be encrypted with the IV and Key 4604 utilizing known AES cipher modes, *e.g.*, AES-CBC or AES-CTR.

[0519] In an exemplary embodiment, AES-CTR mode may use the AES-ENC primitive to implement a stream cipher. For every 128-bit plaintext block to be encrypted, CTR mode may first generate a 128-bit keystream block by calling AES-ENC(K, T), where T is a counter value incremented at each iteration (when T exceeds the maximum counter value, it wraps back to 0). The plaintext block may then be encrypted by XORing it with the keystream block.

[0520] CTR-mode encryption may be defined by the following piece of pseudo-code. K may be an encryption key, and T_0 may be an initial counter value (Initialization Vector). The plaintext may be represented as a series of l28-bit blocks (M_1 , ... , M_n) where M_j represents the ith block of plaintext. AES-CTR may not require plaintext padding: when the plaintext does not divide perfectly into an integer number of blocks, then the final block Mn may be a partial block of size p bits, where $p < 128$. When a p-bit plaintext block is XORed with a normal keystream block, only the first p bits of the two blocks may be considered. The

resulting ciphertext may be represented as a series of blocks (C_1 , ... , C_n) along with the initial counter value T_0. To encrypt a message using AES-CTR:

[0521] $\mathbf{T=T_0}$

For I = 1 to n

$\mathbf{C_i = M_i XOR AES\text{-}ENC(K,T)}$

$\mathbf{T = T + 1}$

[0522] CTR-mode decryption may be identical to encryption, except that the technique operates on ciphertext blocks. To correctly decrypt a CTR-mode ciphertext (T0, C_1 , ... , C_n), compute:

[0523] $\mathbf{T=T_0}$

For I = 1 to n

$\mathbf{C_i = M_i XOR AES\text{-}ENC(K,T)}$

$\mathbf{T = T + 1}$

[0524] CTR mode encryption may require that the 128-bit initial counter value T_0 be initialized to any value between 0 and 2^{128} - 1 inclusive. The default value for T_0 may be 0. This counter may be subsequently incremented for each 128-bit block encrypted or decrypted (if the counter exceeds 2^{128} - 1, it wraps back to 0). To ensure the security of CTR-mode encryptions, it may be necessary that no value of T ever be re-used without re-keying. The technique of choosing the initial counter may be dependent on the implementation.

[0525] CTR mode may be parallelized across multiple processes or processors: after selecting an initial counter T_0, the plaintext may be divided into separate segments and encrypted separately, provided that each encryption process is given the correct counter offset for the first block it encrypts.

[0526] In another exemplary embodiment, AES-CBC mode may use the AES-ENC and AES-DEC primitives to encrypt/decrypt multi-block plaintexts. In addition to the encryption key K, CBC mode may require a 128-bit Initialization Vector (IV), denoted by T_0. Note that for security, this Initialization Vector may be 1) unique for each message encrypted, and 2) generated using a cryptographically-secure random number generator. AES-CBC mode may require that the plaintext consist of an even number of AES blocks, *i.e.*, is a multiple of 128-bits. When this is not the case, the plaintext may be padded by appending a 1 followed by as many

0s as necessary to reach a block boundary. If there is insufficient room to insert the shortest unambiguous padding sequence "10", an additional plaintext block may be added.

[0527] AES-CBC may compute each ciphertext block by XORing a plaintext block with the previous ciphertext block, then encrypting the result using AES-ENC. In the case of the first ciphertext block, the Initialization Vector T_0 replaces the previous ciphertext value. CBC-mode encryption may be defined by the following piece of pseudo-code. The plaintext may be represented as a series of 128-bit blocks (M_1 , ... , M_n) where M_i represents the ith block of plaintext. The resulting ciphertext may be represented as a series of blocks (C_1 , ... , C_n) along with the Initialization Vector T_0. To encrypt a message using AES-CBC:

[0528] $\mathbf{C_1 = AES\text{-}ENC(K, M_1 \, XOR \, T_0)}$

For i = 2 to n

$\mathbf{C_i = AES\text{-}ENC(K, M_1 \, XOR \, C_{i-1})}$

[0529] To correctly decrypt a CBC-mode ciphertext (T_0, C_1 , ... ,. C_n), compute:

[0530] $\mathbf{M_1 = AES\text{-}DEC(K, C_1) \, XOR \, T_0}$

For i = 2 to n

$\mathbf{M_i = AES\text{-}DEC\ (K, C_1) \, XOR \, C_{i-1}}$

[0531] Once the AES encryption is completed, the n encrypted blocks 4608 may then be recombined, with the IV prepended, to be passed to the splitting technique 4610. Before splitting occurs, a meta-data block may also be pre-pended to indicate information such as file length, encryption mode, key size, share ID, L/M/N share values, encryption key ID, encryption IV, hash mode, original buffer size, share buffer size, pre-encryption key ID, pre-encryption IV, pre-signature ID, pre-signature IV, and a flag indicating whether the a key transform such as package or AoNT transform was used to process the key 4604. The data (including IV and metadata) may then be split for distribution to the shares 4614 in accordance with a splitting technique such as bit split, block split, bit segment, or bit scatter as described herein.

[0532] The session key 4604 may optionally be transformed into transform key 4612 such as through a AoNT or a package transform. In the example of a package transform, the session key 4604 may be XORed with the n encrypted

blocks 4608, resulting in a transform key 4612 that cannot be recovered without also recovering all of the n encrypted blocks. The session key 4604 (if no transform takes place) or transform key 4612 may then be split using the Shamir technique or other key-splitting techniques that are well known in the art. For example, the Shamir technique may create L+1 shares, where L is the number of mandatory shares of shares 4614. Each of the L shares may then be distributed to a corresponding mandatory share of shares 4614. The remaining share may then be split into N shares of shares 4614 and distributed in a manner such that the remaining share can be recovered from any M of N shares of shares 4614 as may be required for the particular application. The session key 4604 (if no transform takes place) or transform key 4612 may then be optionally held as a session key, encrypted such as with a public key, or discarded.

[0533] Once the data and/or key has been split for distribution to the shares 4614, each resulting share may further implement integrity protection. As one example, a collision resistant cryptographic hash function (implemented by SHA-256) using hash-tree construction may be used to compute an integrity protection value. A hash value may be calculated for each share using a hashing technique such as SHA-256. If the total number of shares is less than 8, the hash values for all shares may be concatenated and the concatenated result may be stored with each of the shares. If there are 8 or more shares, the integrity protection value may be computed by the following steps:

[0534] 1. Pre-pend 0x00 to each share, and compute a hash value H(0x00 | SHARE) for each share;

[0535] 2. Compute a hash value H(0xFF | A | B) for each consecutive pair of shares, where A and B are the respective outputs of step (1) for each share (*e.g.*, A=H(0x00 | $SHARE_x$); B=H(0x00 | $SHARE_{x+1}$). If the total number of shares is odd, compute a hash value for the final share for (0xFF | A), where A=H(0x00 | $SHARE_{FINAL}$).

[0536] 3. Repeat step (2) on the resulting hash values, until only a single hash result (the hash tree root) remains;

[0537] 4. Distribute to each share $SHARE_i$ the hash of $SHARE_i$ ($H(SHARE_i)$), the tree root, and up to one value from each level of

the tree (*i.e.*, iteration of steps (2) & (3)), as necessary to calculate the tree root from H($SHARE_i$).

[0538] The resulting integrity protection values may be appended to the corresponding share data. Because all hash values are provided to all shares ($n<8$) or a hash tree is provided ($n\geq 8$), The integrity protection as described herein embeds with each share integrity check information about other shares. Thus, if the integrity of any one share in a set is known to be authentic, the integrity of the remaining shares may be evaluated based on the integrity check information of the authentic share.

[0539] The resulting share (including the integrity protection value) may optionally be authenticated (*e.g.*, creating a MAC as described herein) and signed (*e.g.*, a digital signature as described herein). The resulting information may optionally be post-encrypted, for example, using AES or other encryption techniques as described herein and known in the art. The resulting encrypted share may then be distributed, such as to shares for storage or to protect data in motion.

[0540] Data may be recovered from shares (*e.g.*, accessed from storage in shares or received as data in motion) according to the steps of FIGURE 47. Some or all of shares 4702 may be recovered. If the data was post-encrypted prior to distribution to the shares 4702, the data may be decrypted prior to data recovery as described herein. If a share was signed with a digital signature, or includes a MAC, the signature and/or MAC may be confirmed as described herein.

[0541] Each share may have stored a hash value for integrity protection as described above. To confirm the integrity of a received share, a hash value may be computed based on the received data ($SHARE_i$) pre-pended with 0x00, in the same manner as was performed to create the integrity protection value. If the computed hash value from the received $SHARE_i$ data does not match the hash value stored with the share $SHARE_i$, then the integrity of $SHARE_i$ has been compromised and data recovery should be aborted.

[0542] If the total number of shares is less than 8, the computed hash value for $SHARE_i$ may also be compared against the stored hash value for $SHARE_i$ stored in other shares. If the computed hash of $SHARE_i$ fails to match any stored hash of $SHARE_i$, the data recovery should be aborted. This step of checking a computed

hash of $SHARE_i$ against all other stored hashes of $SHARE_i$ may be repeated for all shares. If the total number of shares is 8 or more, then the root of the hash tree may be determined from the computed hash of $SHARE_i$ along with the information stored with the share. This determination may be repeated for each share, and if the hash tree root determined for any individual share does not match, the data recovery may be aborted.

[0543] A key 4706 may be recovered from shares 4702 if all mandatory shares are available as well at least M of N non-mandatory shares. The split data from the shares 4702 may be recovered by recovery technique 4704 utilizing the appropriate recovery technique associated with the data-splitting technique used to create the shares, *e.g.*, bit split, block split, bit segment, or bit scatter as described herein. Data recovered by recovery technique 4704 may include the AES-encrypted data and the initialization vector.

[0544] If a transform such as a package transform or AoNT was used to protect the original session key, the session key 4708 may be recovered from the key 4706 by reversing the transform process. In the example of a package transform, the encrypted data portion of the recovered data from recovery technique 4704 may be split into blocks 4710 of equal length to the key 4706 and XORed with the key 4706 to create the session key 4708. The session key 4708 and initialization vector may then be used as inputs to decrypt the data as data blocks 4712 which may be combined as data 4714. Any padding that was originally necessary to match the data to the AES block size may be discarded. If data 4714 was pre-encrypted, decryption may be performed as described herein.

[0545] A Parsed File System (PFS) is a distributed file system which incorporates a directory, shared among file servers, which is itself parsed. The PFS directory is the clients' view of all file assets. The set of files visible to an individual client is controlled by that client's group keys. The PFS may maintain a directory that contains information about the locations of the shares (for example, the file server location) and the names of the files at the share locations that include the share data. The PFS directory may store information about files including M of N properties, URLs or other globally unique identifiers (GUID) of the shares, a key-id of the key that was used to parse the file, client access times of the key

referenced by the key-id, validity check data, and any other data relating to the clients, users, files, or shares. This PFS directory of files may itself be parsed to prevent unauthorized access. The directory data may be parsed with separate, replaceable group keys to allow keys to be rescinded and replenished as necessary (for example, when there are personnel changes or suspected security breaches).

[0546] The underlying distribution of shares may be hidden from users/clients by the PFS such that files appear as a file storage system based on the PFS directory. The PFS provides an interface that allows users to access parsed files without knowledge of the location of shares. Clients working on a device may enter login credentials. Each client may have group keys associated with that user's login credentials, the group keys determining which files within the directory a client may access. An example set of group keys that might be suitable for a government application may include unclassified, secret, top secret, special 1, special 2, and special 3. Similar group key categories could be set up for various entities based on the shared interests, credentials, position, or other characteristics of the groups. A data set such as a file or a group of files may be associated with a group key. Based on the group keys available to a user, a user may be able to access files associated with that group key. For example, the PFS may display only unclassified files in the directory when the PFS is accessed by a user with only unclassified clearance. Each client may access any files that are authorized by workgroup keys held by that client. Workgroups may be tiered such that a higher classification or clearance level allows access to all lower classification or clearance levels. For example, a user with a top secret workgroup key may receive access to all top secret, secret, and unclassified files.

[0547] The PFS may also monitor events relating to file access and usage. For example, the PFS may audit any file open and close operations as well as any attempts to modify data or move data between files. The auditing process may monitor any attempts to move data from a higher security level to a lower security level. One example of a data monitoring technique is to create a signature of any data that is read from a file (*e.g.*, a cut or copy operation). Signature generators may be available for different file types such as .txt, .wrd, .doc, .xls, .jpg, etc. through a plug-in interface. The signature may be stored by the PFS with a file's

group key until all of the following are met: 1) the file is closed; 2) all processes running when the file was opened are terminated; and 3) all processes which were started after the file was opened but while there was data in the clipboard are terminated. If an attempt to move information from a higher security level to a lower security level is detected, the client may be told that the data will be sequestered for declassification review and may be asked whether they wish to continue the operation. If the user does complete the operation, the data may be sequestered for review by an appropriate party such as an administrator. An exemplary use case for the PFS is outlined below:

[0548] 1) USER1 logs in to the network and is granted {USER1,SAP1, SECRET, UNCLASS} keys.

[0549] 2) USER1 opens Notepad and types "The quick fox jumped over the lazy brown dog."

[0550] 3) USER1 saves the file as TEST1.TXT.

[0551] 4) A dialog box appears asking what secure parser group key should be used: USER1, SAP1, SECRET, or UNCLASS.

[0552] 5) USER1 chooses SECRET and TESTl.TXT is saved.

[0553] 6) USER2 logs in and is granted {USER2, UNCLASS} keys.

[0554] 7) TEST1.TXT is not visible when USER2 opens Explorer.

[0555] 8) USER3 logs in and is granted {USER3, TS_SCI, SAPl, SECRET, UNCLASS} keys.

[0556] 9) USER3 sees TEST1.TXT and opens it.

[0557] 10) USER3 copies "quick fox" to clipboard.

[0558] 11) USER3 pastes clipboard ("quick fox") to a new file.

[0559] 12) USER3 saves the new file as·TEST2.TXT and picks the UNCLASS group key.

[0560] 13) A warning dialog box appears with the message "TEST2.TXT will be sequestered for declassification
review."

[0561] 14) USER3 cancels the warning - the new file is not saved.

[0562] 15) USER3 saves TEST2.TXT using SAP1 key. Since SAP1 includes SECRET, which was TEST1.TXT's key, no warning is issued.

[0563] 16) USER1 sees and reads TEST2.TXT (since he has the SAP1 key), but USER2 cannot.

[0564] 17) USER3 copies/pastes "brown dog" to a new file and saves the new file as TEST1.TXT using key UNCLASS.

[0565] 18) The declassification warning appears and USER3 OKs it.

[0566] 19) ADMIN logs in and is granted all keys.

[0567] 20) ADMIN receives a message to review TEST3.TXT for possible declassification.

[0568] 21) ADMIN shows Details>>> File TEST3.TXT, written by USER3 using key UNCLASS. It contains "brown dog", which may have been copied from TESTl.TXT (key SECRET).

[0569] 22) ADMIN OKs the save.

[0570] 23) USERl, USER2, and USER3 all see and can access TEST3.TXT.

[0571] A secure parser may also be implemented at the device driver level. An exemplary device driver level implementation may be a parsed fabric, wherein specific logical unit numbers (LUNs) or drives are parsed. In the parsed fabric environment, any applications and servers may access and store files to the LUN or drive and issue commands as if the data were stored at the LUN or drive. The secure parser may access a key manager and LUN map which includes a mapping from application visible LUNs to the split physical location of the corresponding shares. The parsed fabric option may allow application and operating system software to operate normally because the parsing is transparent to the programs which can read and write to the LUNs.

[0572] A secure parser may also be implemented at the host bus adapter (HBA) level or the switch level. HBA and switch level implementations may be transparent to the existing software and file systems. HBA and switch level implementations may offload parsing, distribution, and LUN processing from the servers or file system.

[0573] A secure parser may also be implemented within applications, such as through custom integration into the application. A secure parser may be implemented through APIs, function calls, libraries, etc., *e.g.*, as described with respect to FIGURES 30-32 and 42-43, to allow applications to directly or

indirectly utilize the functionality of a secure parser to store, access, or communicate data.

[0574] Although a number of specific implementation points have been described, the secure parser may be implemented at any level or device, such as application servers, storage fabric switches and directors, storage arrays, tape devices, virtualization abstraction layers, remote mirroring/replication storage applications, routing and communications, backup and recovery software, storage management software and interfaces, remote storage management access points, notebook computers, storage network management software or storage MAN/WAN connectivity. For example, the secure parser may be implemented at the application level such as in database software to create hardware-independent implementations, at the SAN controller lever to create disk and application independent implementations, at the switch or router level such as in the router IOS to create hardware and software independent implementation, or at the embedded hardware or controller level for application independent implementations.

[0575] An exemplary API may provide an interface for developing applications for use with a secure parser. The API may include setup files, installer programs, dynamic link libraries, header files, standard libraries such as C++ libraries, visual C++ project files, executables, source code, a ReadMe file, a test harness program, and/or additional or similar files as necessary for a particular platform. The secure parser may utilize several data types and structures, such as those depicted in the table below:

Type	**Description**
Parser	Structure for holding the state and associated I/O data.
Key	Structure for holding a generic key.
Share	Structure for holding a generic buffer.
ParserParams	Structure for holding parser parameters.
HeaderInfo	Structure for holding header information.
FooterInfo	Structure for holding footer information.
EncContext	Structure for storing various encryption contexts.
SigContext	Structure for storing various signature contexts.
HashingContext	Structure for storing various hash contexts.

SplitContext	Structure for storing the split context.
ERROR_TYPE	Enumerator indicating a specific error type.
SPLIT_TYPE	Enumerator identifying the type of split algorithm to utilize.
ENC_TYPE	Enumerator identifying the encryption mode to use.
AUTH_TYPE	Enumerator identifying the authentication mode to use.
HASH_TYPE	Enumerator identifying the hashing mode to use.
TRANFORM_TYPE	Enumerator identifying the transform type to use.
KEY_TYPE	Enumerator indicating a specific key type.
uint8	An unsigned 8 bit integer.
uint16	An unsigned 16 bit integer.
uint32	An unsigned 32 bit integer.

[0576] As is depicted in FIGURE 48, Panel A, and FIGURE 48, Panel B, various enumerators may indicate parameters used in parsing operations such as operating modes, encryption techniques, etc. For example, encryption type 4802 options may include no encryption, AES 128 bit in CTR mode, AES 192 bit in CTR mode, AES 256 bit in CTR mode, AES 128 bit in CBC mode, AES 192 bit in CBC mode, AES 256 bit in CBC mode, or 3DES in CBC mode. Authentication type 4804 options may include a RSA-PSS technique, a DSA digital signature technique, a _generateFooters function 5230 may generate share footer information for each Message Authentication Code. Hash type 4806 options may include no hashing technique or SHA-256. Split type 4808 options may include no split, block level split as determined by the splitting technique, byte level split, bit level split, or bit scattering. Key type 4810 options may include symmetric keys, RSA public key, RSA private key, DSA public key, DSA private key, ECDSA public key, or ECDSA private key. Error type 4812 options may include no error, no master key, invalid callback, invalid parse split technique, no target set to parse, target buffer has no length, unable to restore because not enough shares are present, invalid share was set, invalid key was set, an integrity check failure occurred, or out of memory.

[0577] FIGURE 49, Panel A and FIGURE 49, Panel B depict data structures for the parser, keys and shares. Parser data structure 4902 may include information related to the data to be split and the splitting process, such as originalShare,

shares, shareCount, splitEncContext, and finalFlag. ParserParams data structure 4904 may include information relating to the parameters used in the parsing process, such as L (# of mandatory shares), N (total # of non-mandatory shares), M (# of non-mandatory shares necessary to recover data), splitType, splitEncMode, preEncMode, postEncMode, splitHashMode, preAuthMode, preEncKey, postEncKey, preAuthKey, postAuthKey, maxOrigBufSize, and maxShareBufSize.

[0578] KeyId data structure 4906 may include information for identifying a key, such as id and idLen. KeyShare data structure 4908 may include information relating to the key share data for a share, such as a data field and dataLen. Key data structure 4910 may include additional key information, including keyID (of type keyID 4906), type, data, and dataLen. Share data structure 4912 may include information relating to the status of a share, including data, dataLen, encContext, authContext, and hashContext.

[0579] FIGURE 50, Panel A and FIGURE 50, Panel B depict data structures relating to encryption, authentication, and hashing functionality. EncContext data structure 5002 may be utilized in various other data structures, and may include information relating to the type of encryption being used and encryption contexts as described below. EncContext_AESCBC data structure 5004 may include information relating to AES-CBC encryption, including encKeyId, currentIV (initialization vector) and currentIVLen. EncContext_AESCTR data structure 5006 may include information relating to AES-CTR encryption, including encKeyId, currentIV (initialization vector) and currentIVLen.

[0580] AuthContext data structure 5008 may include information relating to the type of authentication being used and information relating to the various authentication contexts as described below. AuthContext_RSAPSS data structure 5010 may include information relating to a RSA_PSS digital signature, including a pubKeyId, privKeyId, and hashContext. AuthContext_DSA data structure 5012 may include information relating to a DSA digital signature, including a pubKeyId, privKeyId, and hashContext. AuthContext_ECSA data structure 5014 may include information relating to a ECDSA digital signature, including a pubKeyId, privKeyId, and hashContext. AuthContext_HMACSHA1 data structure 5016 may

include information relating to a HMAC-SHA1 type MAC, including a macContext pointer to the OpenSSL mac context data type.

[0581] hashContext data structure 5018 may include information relating to the type of hashing being utilized, such as a hashMode and any appropriate hash contexts. An example of hash context may be HashContext_SHA data structure 5020 which may include a pointer to the OpenSSL hash context data type.

[0582] FIGURE 51, Panel A and FIGURE 51, Panel B depict data formats including share data 5102, post-encrypted footer 5104, post-encrypted header 5106, and encrypted footer 5108. Share data 5102 may include a post-encryption key id, post-signature key id, post-encrypted header 5106, post-encrypted footer 5104, and post-signature data. Post-encrypted footer 5104 may include encrypted footer 5108. Encrypted footer 5108 may include split-hash data, and pre-signature data. Post-encrypted header 5106 may include a key share, share id, L, M, N, split mode, split-encryption key, split-encryption IV, split-hash mode, original buffer, share buffer, pre-encryption key, and pre-signature key.

[0583] The secure parser API may include a function library with various functions as depicted in FIGURE 52A, Panel A, FIGURE 52A, Panel B, FIGURE 52B, Panel A, and FIGURE 52B, Panel B. A number of functions may relate to initializing and ending parser operations. A parser_createParser function 5202 may be called to allocate a secure parser context and set default values for the parser, while a parser_destroyParser function 5204 may be passed a Parser data structure and may destroy the secure parser context, including parser parameter objects and share buffers. A parser_createKey function 5206 may construct the key structure, while a parser_destroyKey function 5208 may destroy the key. A parser_createShare function 5210 may create a share data structure for use with the secure parser, while a parser_destroyShare function 5212 may destroy a share, including all encryption and authentication keys. A parser_initParameters function 5214 may initialize the ParserParams data structure to the default parameter set, while a parser_setParameters 5216 may set any ParserParames settings for the current Parser data structure. A parser_setFinalize function 5218 may set the internal state of the Parser to finalize the output stream during the next split session.

[0584] Other functions may relate to the creation and splitting of shares, and the creation of the headers and footers associated with shares. parser_getOriginalShare function 5220 may return a share structure representing the original buffer used by the Parser. parser_getShare function 5222 may return a share containing the share structure for a share matching a share ID. parser_doSplit function 5224 may perform the secure parser split. parser_doRestore function 5226 may restore shares into reconstructed original data, while parser_getRestoreStatus function 5236 may return the status of the prior restore process. parser_generateHeaders function 5228 and parser_generateFooters function 5230 may generate header and footer information, while parser_restoreHeaders function 5232 and parser_restoreFooters function 5234 may restore header and footer information from shares.

[0585] parser_generateHeaders function 5228 may generate share header information for each share based on any meta-data that must necessarily be communicated to the secure parser when later performing a restore technique. The header information may only contain data that is available to the secure parser prior to the start of the data splitting process. The parser generateHeaders routine creates the header blocks for each share and places them within each Share buffer. A call to parser_generateHeaders may be made prior to any calls to parser_doSplit. The parser_generateHeaders function involves the following steps:

1. Split key using Shamir splitting algorithm.
2. Create a temporary buffer.
3. For each share…
    - 3.1 Include key share information in temporary buffer.
    - 3.2 Include share ID in temporary buffer.
    - 3.3 Include L, M and N in temporary buffer.
    - 3.4 Include split mode in temporary buffer.
    - 3.5 Include split-encryption key ID in temporary buffer.
    - 3.6 Include split-encryption IV in temporary buffer.
    - 3.7 Include split-hash mode in temporary buffer.
    - 3.8 Include original buffer size in temporary buffer.
    - 3.9 Include share buffer size in temporary buffer.

3.10 Include pre-encryption key ID in temporary buffer.

3.11 Include pre-encryption IV in temporary buffer.

3.12 Include pre-signature key ID in temporary buffer.

3.13 Include pre-signature IV in temporary buffer.

3.14 Replace key share information in temporary buffer with Share i's key share.

3.15 Replace share ID in temporary buffer with Share i's ID.

3.16 Begin split-hash on the data in temporary buffer and store context for later.

3.17 Encrypt temporary buffer with post-encryption key and post-encryption IV and include resulting ciphertext in Share i's output buffer. Maintain i's post-encryption context for later use.

3.18 Begin post-signature on Share i's output buffer and store context for later.

[0586] The parser_doSplit function 5224 may split all data from the target buffer into share buffers to be later handled by the calling function. A series of steps may be taken to provide confidentiality, integrity, authenticity and data partitioning for the data that is split, before and after the data is split. These steps may include:

1. Test if pre-encrypt is on.

   If Yes,

   1.1 Encrypt target buffer under pre-encrypt key and pre-encrypt IV.

2. Test if pre-sign is on.

   If Yes,

   2.1 Sign target buffer under pre-sign key.

   2.2 Test if finalize has been set.

   If Yes,

   2.2.1 Finalize pre-signature context.

3. Do split-encryption using split-encryption context. (Should be initialized during the first call to this function.)

4. Call appropriate split algorithm…

5. Test if hashing is on.

   If Yes,

5.1 For each output share…

5.1.1 Continue hash for share i's buffer.

6. Test if post-encrypt is on.

If Yes,

6.1 For each output share…

6.1.1 Encrypt share i's buffer using share i's post-encryption key and post-encryption context.

7. Test if post-sign is on.

If Yes,

7.1 For each output share…

7.1.1 Continue signature for share i's output buffer under share i's post-signature context.

[0587] parser_generateFooters function 5230 may generate share footer information for each share based on any meta-data that must necessarily be communicated to the secure parser when later performing a restore technique. The footer information may typically only available to the secure parser after the body of the data has been parsed. The parser_generateFooters routine creates the footer blocks for each share and places them within each Share buffer. parser_generateFooters may be called following all calls to parser_doSplit and parser_setFinalize. parser_generateFooters function 5230 may perform the following steps:

1. Create temporary buffer 1 for unencrypted footer information.
2. Create temporary buffer 2 for partially encrypted footer information.
3. For each share…

3.1 Include pre-signature data in unencrypted buffer.

3.2 Encrypt temporary buffer 1 using split-key and split-encryption context and include resulting ciphertext in temporary buffer 2.

3.3 Continue split-hash data in temporary buffer 2.

3.4 Include split-hash data in temporary buffer 2.

3.5 Encrypt temporary buffer 2 using share i's post-encryption key and post-encryption context and place resulting ciphertext in share i's output buffer.

3.6 Continue post-authentication signature over share i's output buffer using share i's post-signature context.

3.7 Finalize share i's post-signature context.

3.8 Include share i's post-signature in share i's output buffer.

[0588] parser_restoreHeaders function 5232 may restore header information for each share based on any meta-data that was stored by the secure parser for later restoration. The header information may contain data that is required for future calls to the parser_doRestore process to function properly. The parser_restoreHeaders routine may require that the header blocks for each share be placed within each Share buffer. A call to parser_restoreHeaders may be made prior to any calls to parser_doRestore. Steps of parser_restore headers function 5232 may include the following:

1. For each share…
   - 1.1 Create a temporary buffer for share i.
   - 1.2 Begin signature over share i's buffer using share i's post-signature key and post signature IV. Maintain post-signature context for share i.
   - 1.3 Decrypt share i's buffer using share i's post-encryption key and post-encryption IV and place contents into share i's temporary buffer.
   - 1.4 Recover key share information for share i from share i's temporary buffer.
   - 1.5 Test if this is share 0.

     If no,

     - 1.5.1 Compare share i's header information in temporary buffer with share 0's header information in temporary buffer. If there is a mismatch, return an error.
2. Recover split-encryption key, based on all key share information in each share's temporary buffer.
3. Recover parser state based on header information found in share 0's temporary buffer.

[0589] parser_doRestore function 5226 may restore all shares to their original single source. A series of steps verify that the data has not been tampered with

before and after data restoration has completed. Steps for parser_doRestore function 5226 may include the following:

1. Test if post-sign is on.
   If Yes,
   1.1 For each output share…
      1.1.1 Sign share i's output buffer under share i's post-signature key.
2. Test if post-encrypt is on.
   If Yes,
   2.1 For each output share…
      2.1.1 Decrypt share i's buffer using key post-decrypt i and IV i.
3. Test if hashing is on.
   If Yes,
   3.1 For each output share…
      3.1.1 Continue hash for share i's buffer.
4. Call appropriate restore algorithm.
5. Do split-decryption using split-decryption key and split-decryption context. (Should be initialized during first call to this function.)
6. Test if pre-sign is on.
   If Yes,
   6.1 Sign original buffer under pre-sign key using pre-signature context or pre-signature IV.
   6.2 Test if finalize has been set.
      If Yes,
      6.2.1 Finalize pre-signature context.
7. Test if pre-encrypt is on.
   If Yes,
   7.1 Decrypt original buffer under pre-decryption key.

[0590] parser_restoreFooters function 5234 may restore footer information for each share based on any meta-data that was stored by the secure parser for later restoration. The footer information may contain data that is needed for valid completion of the restore process. The parser_restoreFooters routine may require

that the footer blocks for each share be placed within each Share buffer. A call to parser_restoreFooters may be after all calls to parser_doRestore and parser_setFinalize. Steps for parser_restoreFooters function 5234 may include the following:

1. Create a temporary pre-signature buffer.
2. For each share…
    - 2.1 Create a temporary buffer for share i.
    - 2.2 Continue post-signature over share i's buffer using share i's post-signature key and post-signature context.
    - 2.3 Finalize share i's post-signature context.
    - 2.4 Compare share i's post-signature result with expected post-signature result and return an error on mismatch.
    - 2.5 Decrypt share i's buffer using share i's post-decryption key and post-decryption context and place contents into share i's temporary buffer.
    - 2.6 Continue split-hash over share i's encrypted footer portion of share i's temporary buffer using share i's split-hash context.
    - 2.7 Finalize share i's split hash context.
    - 2.8 Compare share i's split-hash result with expected split-hash result found in remaining portion of share i's temporary buffer and return an error on mismatch.
    - 2.9 Decrypt the footer portion of share i's temporary buffer using the split-decryption key and split-decryption context and place resulting plaintext in to the temporary pre-signature buffer.
    - 2.10 Compare temporary pre-signature buffer with finalized pre-signature result and return an error on mismatch.

[0591] FIGURE 53 depicts an exemplary implementation of a secure parser within a hardware system such as a data storage control node. The secure parser may operate on a processor 5302. The secure parser may be in communication with various forms of internal memory such as SDRAM (*e.g.*, 5304), hard drives (*e.g.*, 5310), and flash memory (*e.g.*, 5306). The secure parser may also be in

communication with other internal circuitry and functionality and may also communicate over networks, *e.g.*, utilizing Ethernet connectivity 5308.

[0592] FIGURE 54 depicts an exemplary implementation of a secure parser for data masking. It may be desirable to store certain information of a set of information securely. For example, a healthcare record for an individual may include less sensitive information such as name, address, height, and weight. The healthcare record may also include sensitive information such as a social security number 5404, medical ID number 5406, and employer phone number 5408. The less sensitive information may be stored locally, *e.g.*, at local server 5402. The sensitive information 5404, 5406, and 5408 may be parsed and distributed to multiple locations, *e.g.*, to local server 5402 and remote servers 5410 and 5412.

[0593] FIGURE 55 depicts an exemplary data record in a data masking implementation. As described above, the local server may not have local access to records that have been parsed and distributed to multiple locations, and thus the sensitive records 5502, 5504, and 5506 may not be visible. To the extent that local information 5508 relating to the sensitive records exists, it may not be in a human readable form.

[0594] An exemplary set of workgroup keys is depicted in FIGURE 56. For example, four groups may include top secret / sensitive compartmented information (TS/SCI) 5602, secret 5604, secret SAP 5606, and coalition 5608. Each group may include a plurality of users who are associated with that group. When a user logs into the system from a device, the login may include credentials, username, password, or other authenticating information that provides access to one or more workgroup keys associated with one or more of workgroups 5602, 5604, 5606, and 5608.

[0595] Accordingly, if the login credentials match a member of an appropriate group, the user may access parsed files, drives, and data associated with that workgroup, or in some embodiments any information associated with groups having a lower classification.

[0596] FIGURE 57 depicts the use of workgroup keys in an example application of military use. Command operations headquarters 5702, deployed headquarters 5706, tactical team 5708, and tactical base 5710 may all have access to information

stored as described herein via a satellite link 5704. Data may be stored at one or more of locations 5702, 5706, 5708, and/or 5710, as well as additional offsite storage locations. Data may be stored in distributed shares as described herein and/or may be transmitted on satellite link 5704 as shares as described herein. Individuals located at locations 5702,5706, 5708, and/or 5710 may submit login credentials to gain access to information associated with one or more of workgroup keys TS/SCI, secret, secret SAP, or coalition.

[0597] Workgroup keys may be implemented as in a MLS solution as depicted in FIGURE 58. Example workgroup keys may include TS/SCI 5802, secret 5804, coalition 5806, and unclassified 5808. The types, names, and number of workgroups are exemplary only, and may be modified based on the particular application. Workgroup keys may be managed and stored as described herein (*e.g.*, locally, remotely, in shares). Clients may access information associated with a workgroup through a parser server 5812.

[0598] Parser server 5812 may include one or more servers, and may include client partition 5814, TS/SCI partition 5816, secret partition 5818, coalition partition 5820, and unclassified partition 5822. Partitions may be based on workgroup keys and may be logical, or as in the example of FIGURE 58, may be physical. Client-facing aspects of the parser server may be implemented at client partition 5814. Client partition 5814 may also interface with local storage area network 5824, which may provide storage of information for parser server 5812.

[0599] A secure parser may support backup applications. For example, a conventional file system may be maintained while a backup of the files is parsed to multiple backup locations in accordance with the present invention. For backup applications parsing may provide additional security as well as redundancy through M on N parsing. A backup application may also utilize one or more mandatory shares while maintaining M of N parsing for the non-mandatory shares. It may also be possible to use public key cryptography to further secure backup data. Any storage operations for backup data may utilize a public key to encrypt the data. Only the holder of the private key may recover the backup data.

[0600] A secure parser may also be used for secure deletion of data. When one or more mandatory shares are utilized in the splitting and distribution process, the

underlying data may not be recoverable without all of the mandatory shares. The permanent deletion of any mandatory shares may therefore result in the effective deletion of the underlying data.

[0601] A secure parser may also be used to create flexible security policies. For example, utilizing an M-of-N data split, a backup operator may produce N shares (*e.g.*, as backup tapes), with each accessible to distinct individuals or departments. A quorum of M individuals may therefore be required to combine their shares to reconstruct data.

[0602] An embodiment of the present invention for a backup application is depicted at FIGURE 59. Server 5902 and server 5904 may be MSCS clustered servers running an application. Servers 5902 and 5904 may each include a LUN map associating a LUN with shares used for storage of parsed drives, files, or other data. Each of server 5902 and 5904 may be in communication with key manager 5906 to access keys for encryption and parsing of data. Parser enabled HBA 5908 may implement parsing, distribution, recovery, and access of parsed data to shares 5912 and 5914 as provided in the LUN map of server 5902. Communication between HBA 5908 and shares 5912 and 5914 may be implemented through storage area network (SAN) 5920. Parser enabled HBA 5910 may implement parsing, distribution, recovery, and access of parsed data to shares 5916 and 5918 as provided in the LUN map of server 5904. Communication between HBA 5910 and shares 5916 and 5918 may be implemented through SAN 5922.

[0603] Backup protection may be provided by SafeGuard appliance 5924 and SafeGuard appliance 5926. As depicted in FIGURE 59, SafeGuard appliance 5924 may capture parsed data that is written to shares 5912 and 5914 and route complete copies of the parsed data for storage at shares 5916 and 5918 through SafeGuard appliance 5926 and SAN 5922. Similarly, SafeGuard appliance 5926 may capture parsed data that is written to shares 5916 and 5918 and route complete copies of the parsed data for storage at shares 5912 and 5914 through SafeGuard appliance 5924 and SAN 5920. In the event of a disaster or other event, the data split between shares 5912 and 5914 may be fully recovered from shares 5916 and 5918. Similarly, the data split between shares 5916 and 5918 may be fully recovered from shares 5912 and 5914.

[0604] An embodiment of the present invention for backup applications is depicted at FIGURE 60. Server 6002 and server 6004 may be MSCS clustered servers running an application. Server 6002 may be in communication with parser enabled switch 6006 and server 6004 may be in communication with parser enabled switch 6008. Each of parser enabled switch 6006 and 6008 may be in communication with key manager / LUN map 6010. Key manager / LUN map 6010 may provide access to keys for encryption and parsing of data, and a LUN map associating a LUN with shares used for storage of parsed drives, files, or other data. Parser enabled switch 6006 may implement parsing, distribution, recovery, and access of parsed data to shares 6012 and 6014 as provided in the key manager / LUN map 6010. Communication between parser enabled switch 6006 and shares 6012 and 6014 may be implemented through storage area network (SAN) 6020. Parser enabled switch 6008 may implement parsing, distribution, recovery, and access of parsed data to shares 6016 and 6018 as provided in the key manager / LUN map 6010. Communication between parser enabled switch 6008 and shares 6016 and 6018 may be implemented through SAN 6022.

[0605] Disaster recovery protection may be provided by SafeGuard appliance 6024 and SafeGuard appliance 6026. As depicted in FIGURE 60, SafeGuard appliance 6024 may capture parsed data that is written to shares 6012 and 6014 and route complete copies of the parsed data for storage at shares 6016 and 6018 through SafeGuard appliance 6026 and SAN 6022. Similarly, SafeGuard appliance 6026 may capture parsed data that is written to shares 6016 and 6018 and route complete copies of the parsed data for storage at shares 6012 and 6014 through SafeGuard appliance 6024 and SAN 6020. In the event of a disaster or other event, the data split between shares 6012 and 6014 may be fully recovered from shares 6016 and 6018. Similarly, the data split between shares 6016 and 6018 may be fully recovered from shares 6012 and 6014.

[0606] A secure parser may include a variety of techniques such as FIPS standard techniques for managing keys. These include systems for encrypting key data, use of protected memory for key material, and "split-knowledge" techniques which allow keys to be safely divided among multiple participants. Authenticated key agreement techniques may also be provided to rapidly establish connections

between secure parser modules in a manner that is compliant with industry standards such as IPSEC, TLS and SSL.

[0607] A secure data parser may communicate with the electronic storage locally or remotely. The secure data parser may be implemented through any network or communication protocol such as IPV4 and IPV6. Shares used to reconstruct files, file systems, or any other data distributed over shares may be accessed over one or more transmission medium, including physical delivery of a drive, disk, or other storage medium, delivery via physical networks such as twisted pair, coaxial cable, optical fiber, or wireless delivery such as via AM radio, shortwave, FM/TV broadcast, cellular technology, satellites, microwave, terrestrial, or any other known wireless medium.

[0608] A secure parser may be implemented in any number of environments, from servers to desktops, cell phones to PDAs, and dedicated appliances to smartcards.

[0609] Pricing for usage of the secure parser may be accomplished in a number of ways. For example, a user could be charged based on storage or data processing (*e.g.*, throughput), *e.g.*, on a per-Gigabyte basis. Pricing could be on an enterprise bases, server, basis, client basis, or site license basis. Charges may also be on a percentage of effort on value basis, *e.g.*, based on a measure of the security improvement in the system.

[0610] Additionally, other combinations, additions, substitutions and modifications will be apparent to the skilled artisan in view of the disclosure herein. Accordingly, the present invention is not intended to be limited by the reaction of the preferred embodiments but is to be defined by a reference to the appended claims.

What is claimed is:

1. A method of presenting a virtual disk to a client device, the method comprising:

receiving client credentials from a client device, the client credentials including a client identifier;

authenticating the client device at a secure storage device;

determining a volume is associated with the client device based upon the client identifier, the volume associated with a plurality of shares stored on a corresponding plurality of physical storage devices; and

upon determining the volume is associated with the client device, presenting the volume to the client device.

SECURE DATA PARSER METHOD AND SYSTEM

Abstract of the Invention

[0611] A secure data parser is provided that may be integrated into any suitable system for securely storing and communicating data. The secure data parser parses data and then splits the data into multiple portions that are stored or communicated distinctly. Encryption of the original data, the portions of data, or both may be employed for additional security. The secure data parser may be used to protect data in motion by splitting original data into portions of data that may be communicated using multiple communications paths.

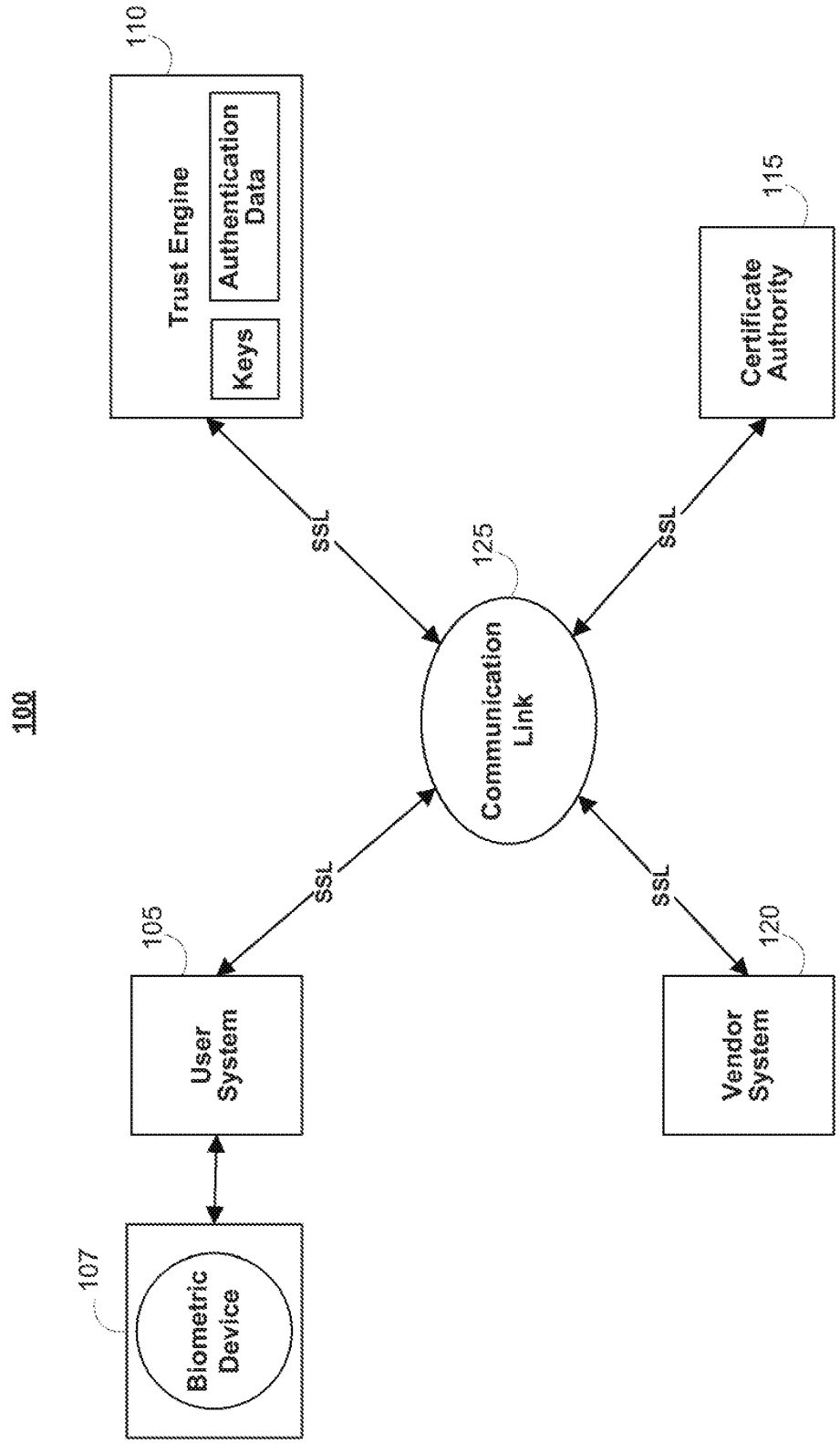

100
110
Trust Engine
Authentication Data
Keys
115
Certificate Authority
SSL
SSL
125
Communication Link
SSL
SSL
105
User System
120
Vendor System
107
Biometric Device

FIG. 1

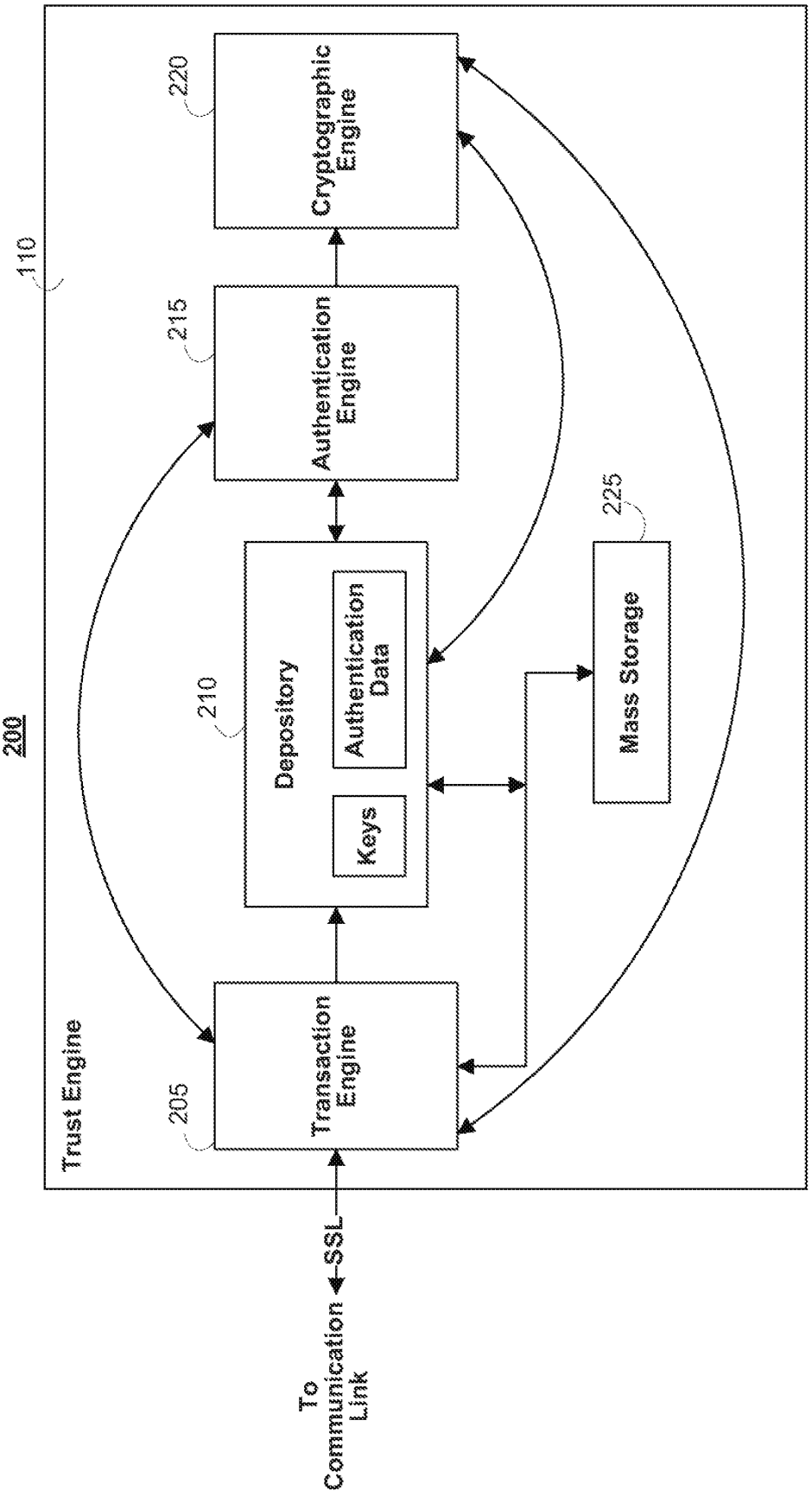

200
110
Trust Engine
205
Transaction Engine
210
Depository
Keys
Authentication Data
215
Authentication Engine
220
Cryptographic Engine
225
Mass Storage
SSL
To Communication Link

FIG. 2

EX1002 - Page 457

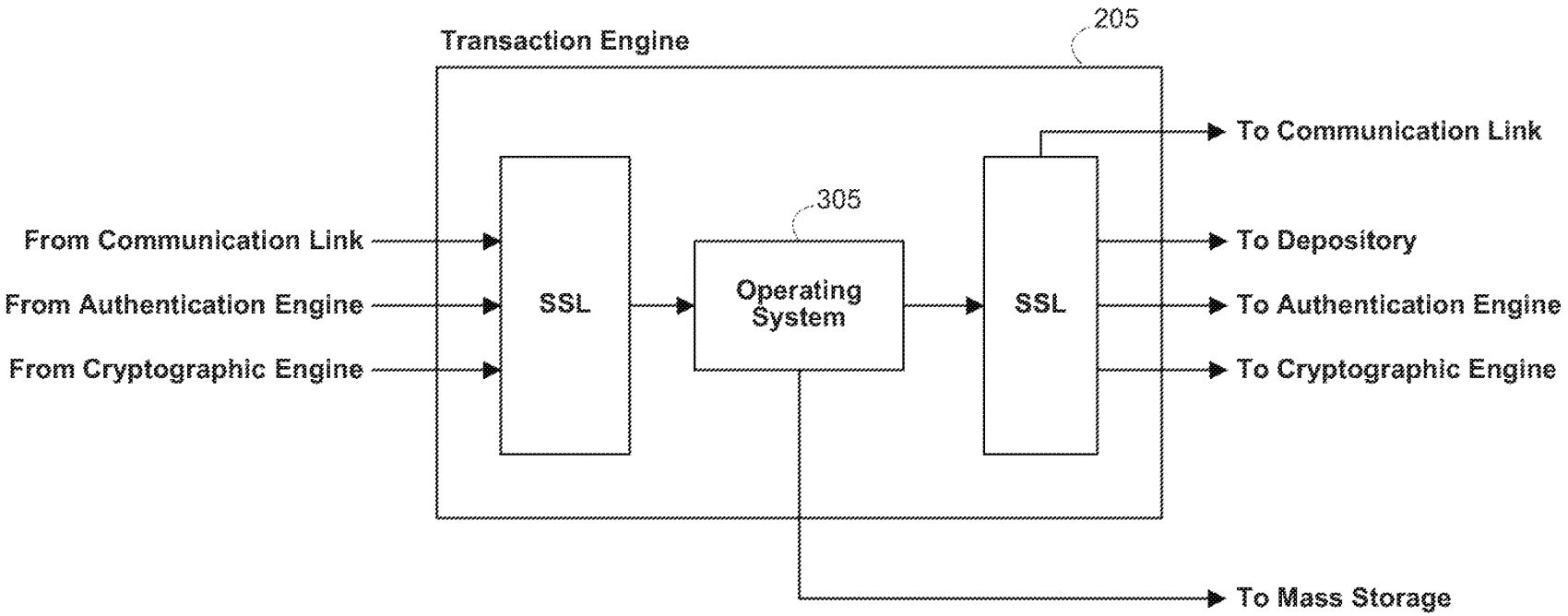


FIG. 3

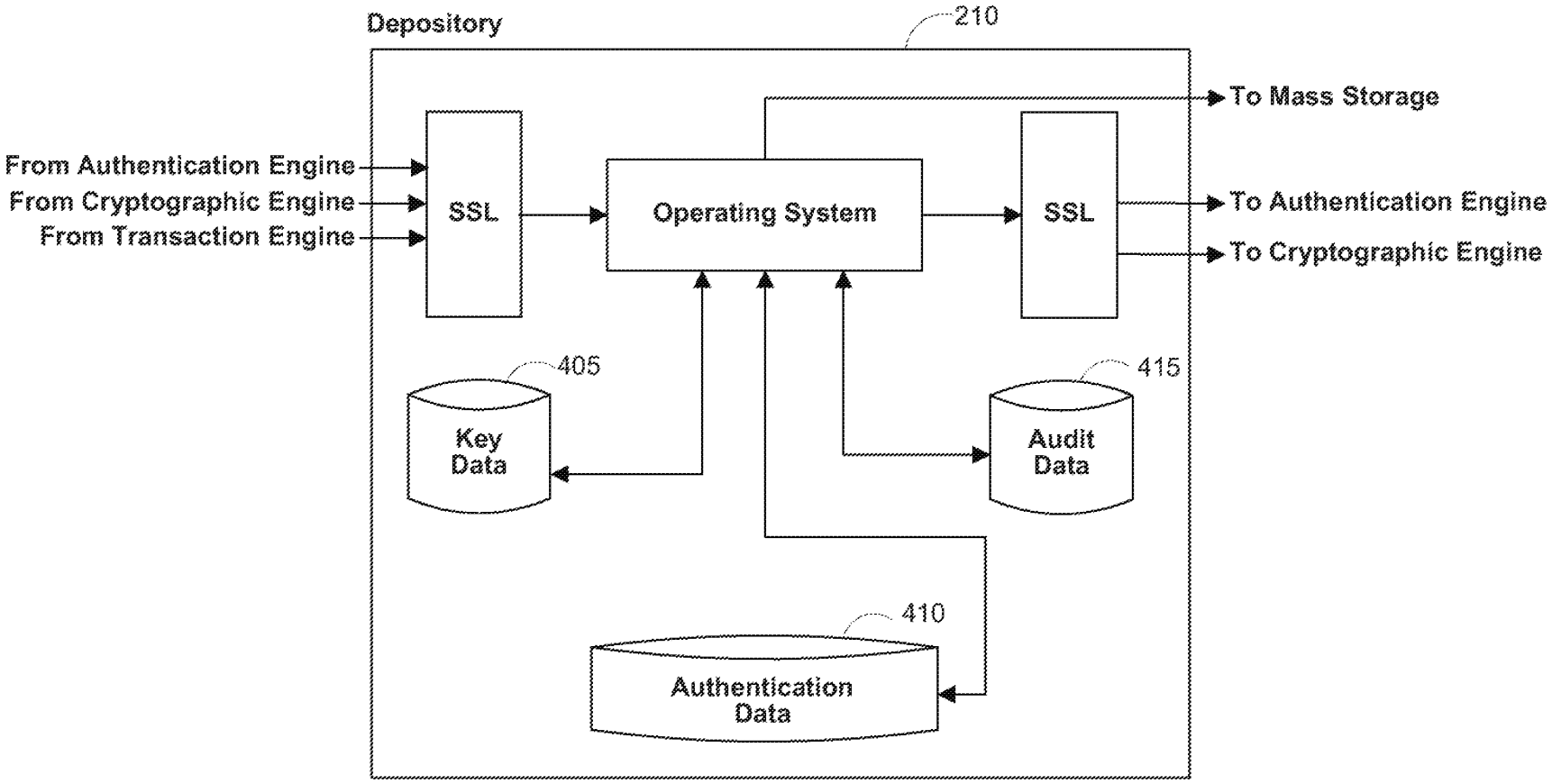


FIG. 4

EX1002 - Page 458

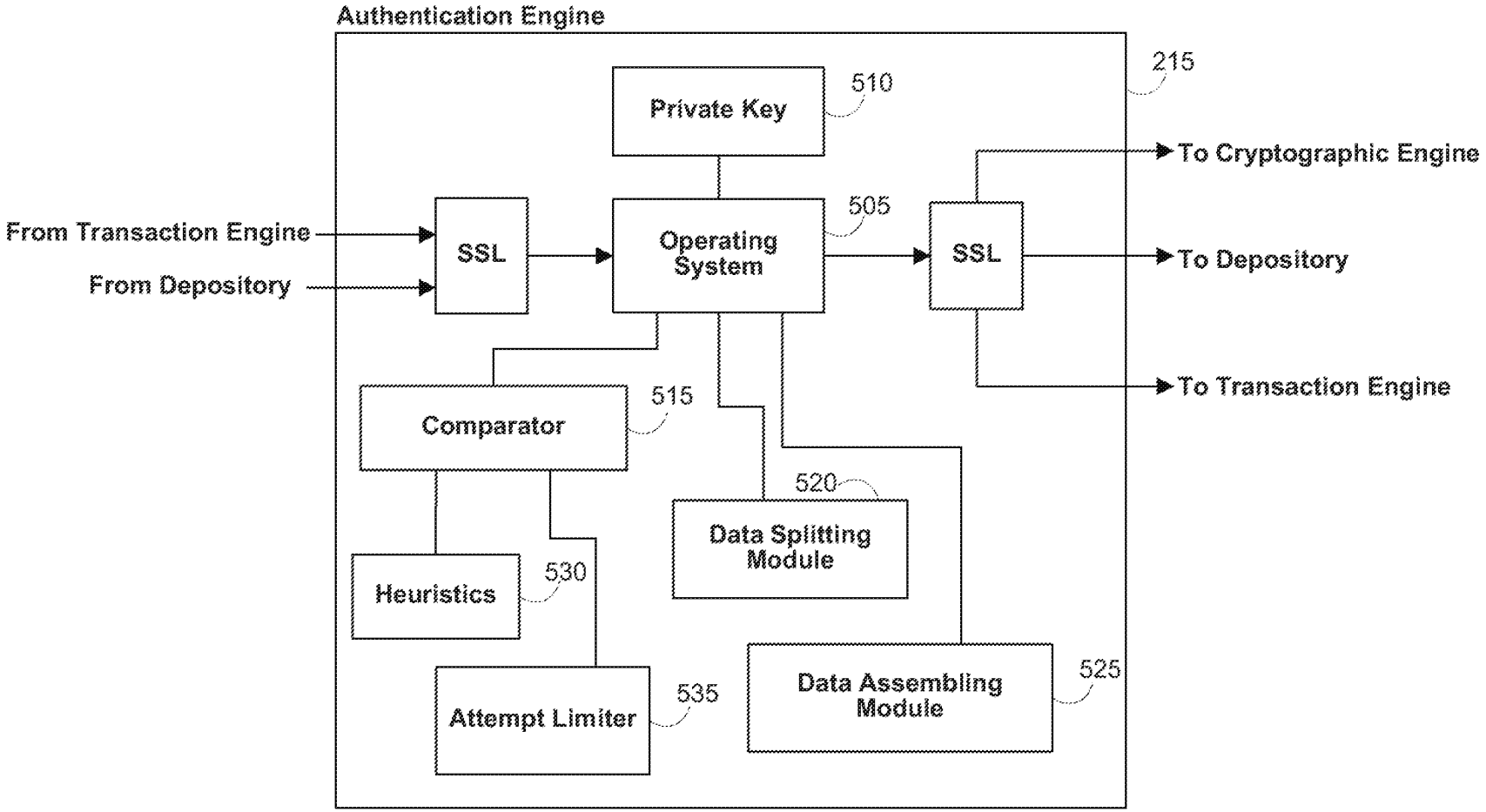


FIG. 5

EX1002 - Page 459

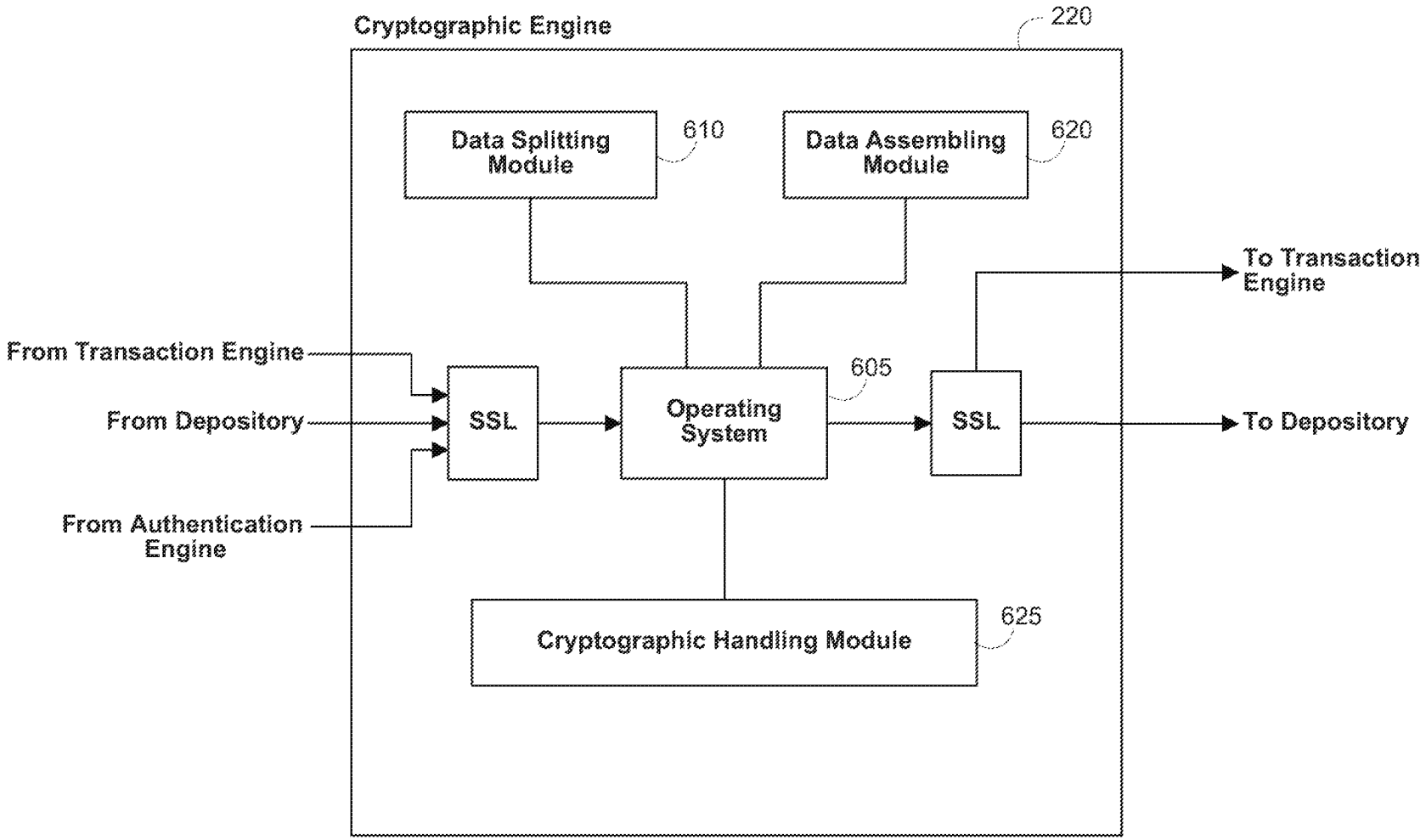


FIG. 6

EX1002 - Page 460

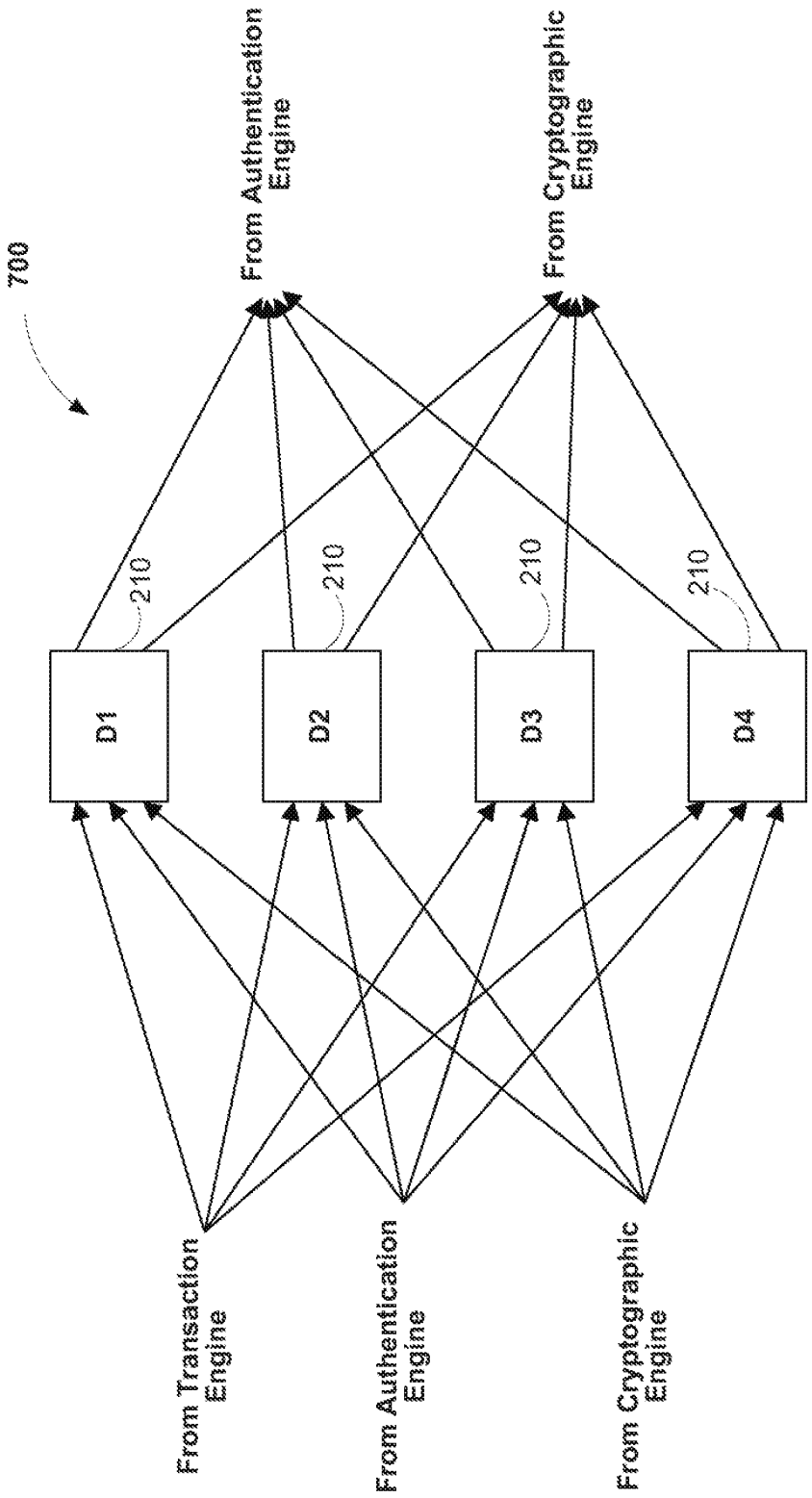

700
From Authentication Engine
From Cryptographic Engine
210
210
210
210
D1
D2
D3
D4
From Transaction Engine
From Authentication Engine
From Cryptographic Engine

FIG. 7

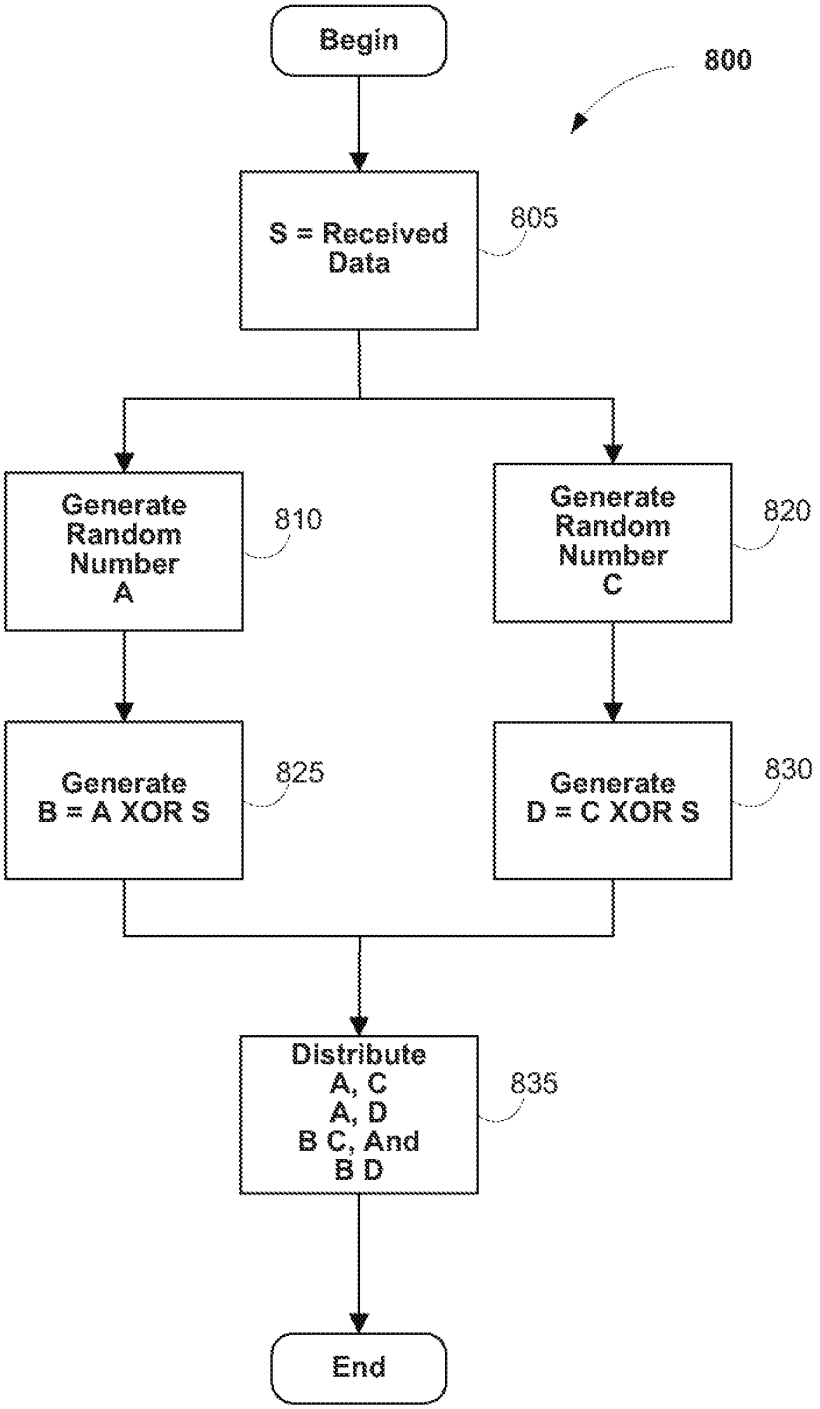

Begin
800
S = Received Data
805
Generate Random Number A
810
Generate Random Number C
820
Generate B = A XOR S
825
Generate D = C XOR S
830
Distribute A, C A, D B C, And B D
835
End

FIG. 8

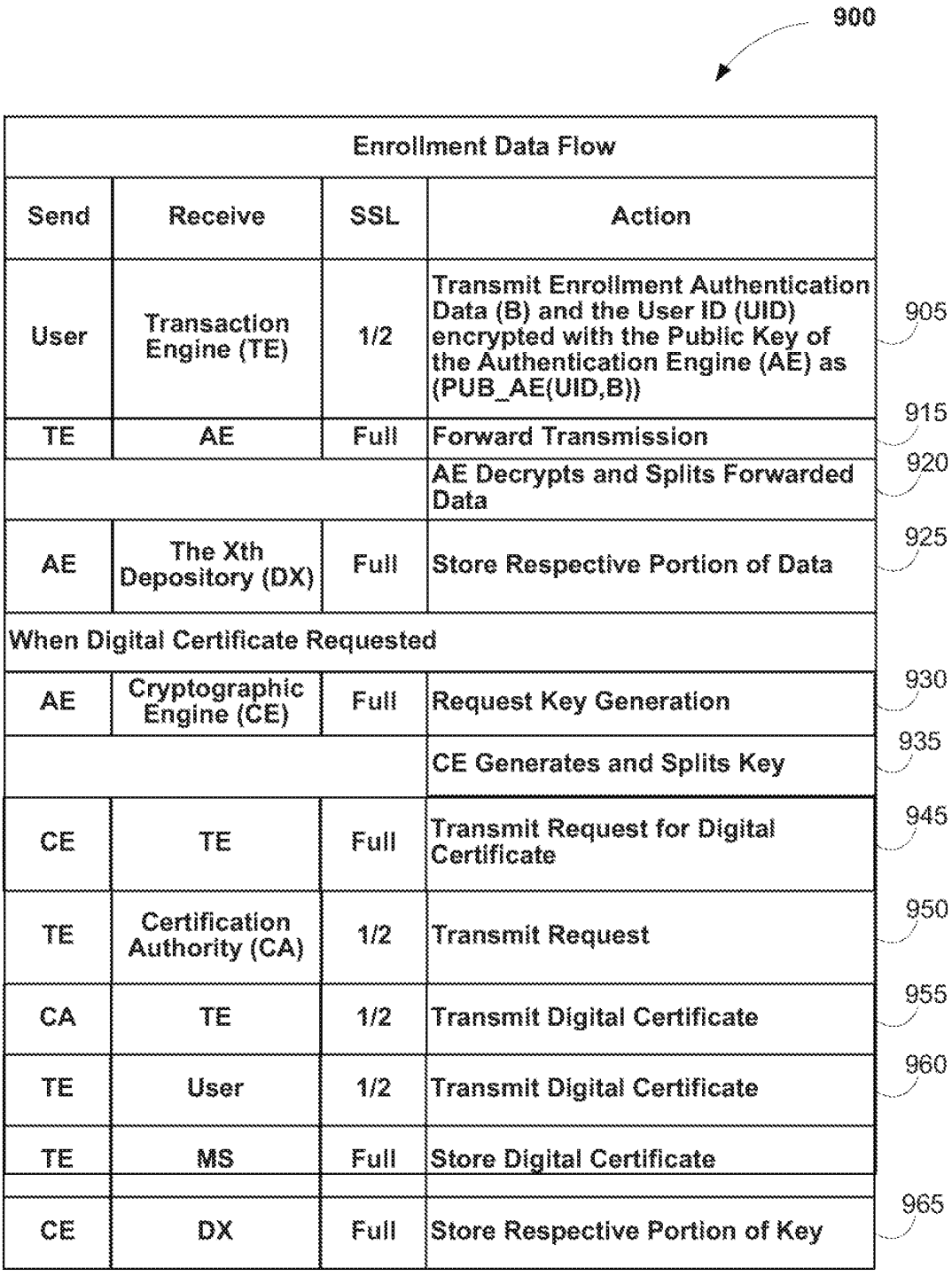

900
Enrollment Data Flow
Send
Receive
SSL
Action
User
Transaction Engine (TE)
1/2
Transmit Enrollment Authentication Data (B) and the User ID (UID) encrypted with the Public Key of the Authentication Engine (AE) as (PUB_AE(UID,B))
905
TE
AE
Full
Forward Transmission
915
AE Decrypts and Splits Forwarded Data
920
AE
The Xth Depository (DX)
Full
Store Respective Portion of Data
925
When Digital Certificate Requested
AE
Cryptographic Engine (CE)
Full
Request Key Generation
930
CE Generates and Splits Key
935
CE
TE
Full
Transmit Request for Digital Certificate
945
TE
Certification Authority (CA)
1/2
Transmit Request
950
CA
TE
1/2
Transmit Digital Certificate
955
TE
User
1/2
Transmit Digital Certificate
960
TE
MS
Full
Store Digital Certificate
CE
DX
Full
Store Respective Portion of Key
965

FIG. 9, Panel A

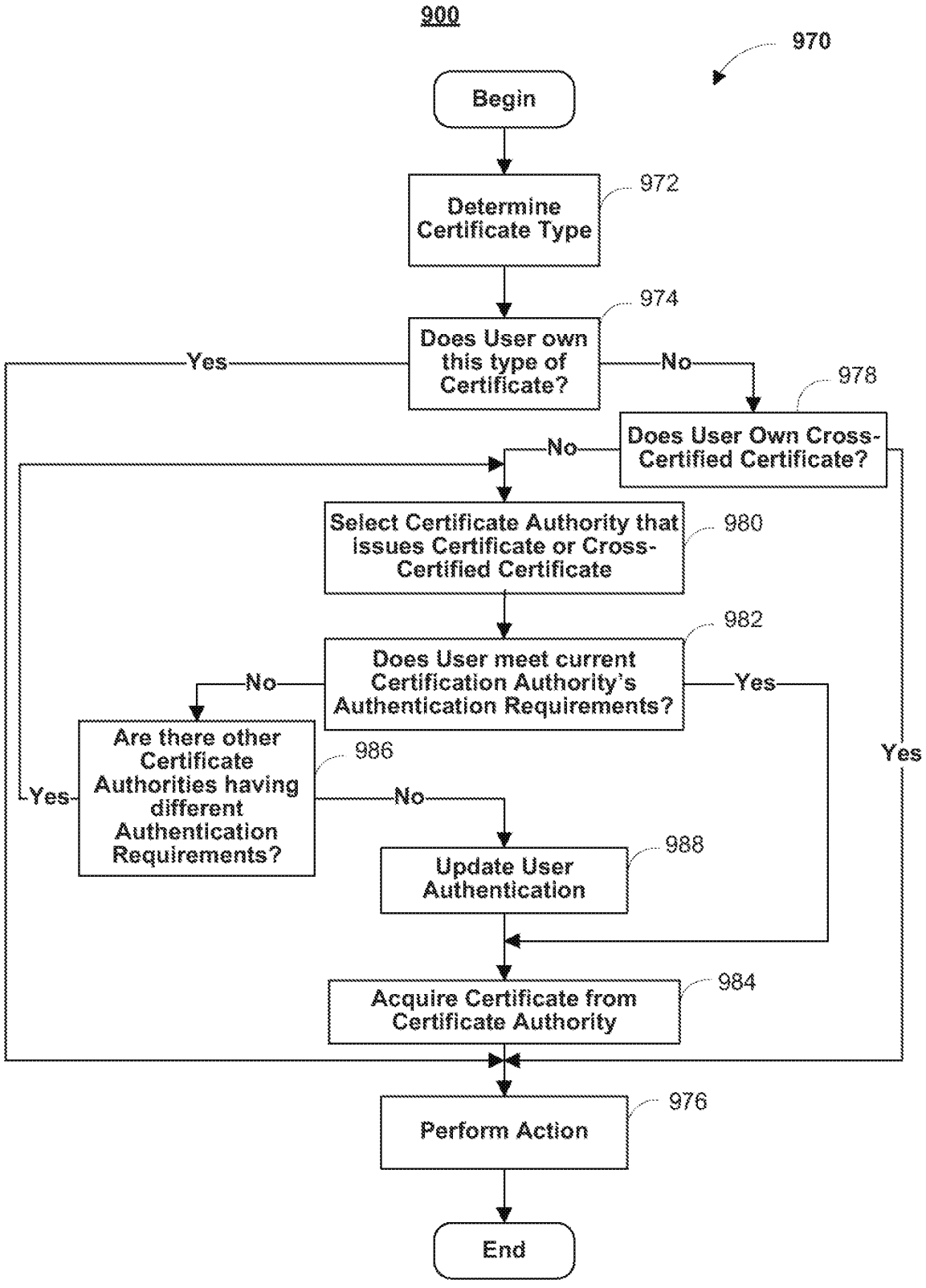

900
970
Begin
Determine Certificate Type
972
Does User own this type of Certificate?
974
Yes
No
Does User Own Cross-Certified Certificate?
978
No
Yes
Select Certificate Authority that issues Certificate or Cross-Certified Certificate
980
Does User meet current Certification Authority's Authentication Requirements?
982
No
Yes
Are there other Certificate Authorities having different Authentication Requirements?
986
Yes
No
Update User Authentication
988
Acquire Certificate from Certificate Authority
984
Perform Action
976
End

FIG. 9, Panel B

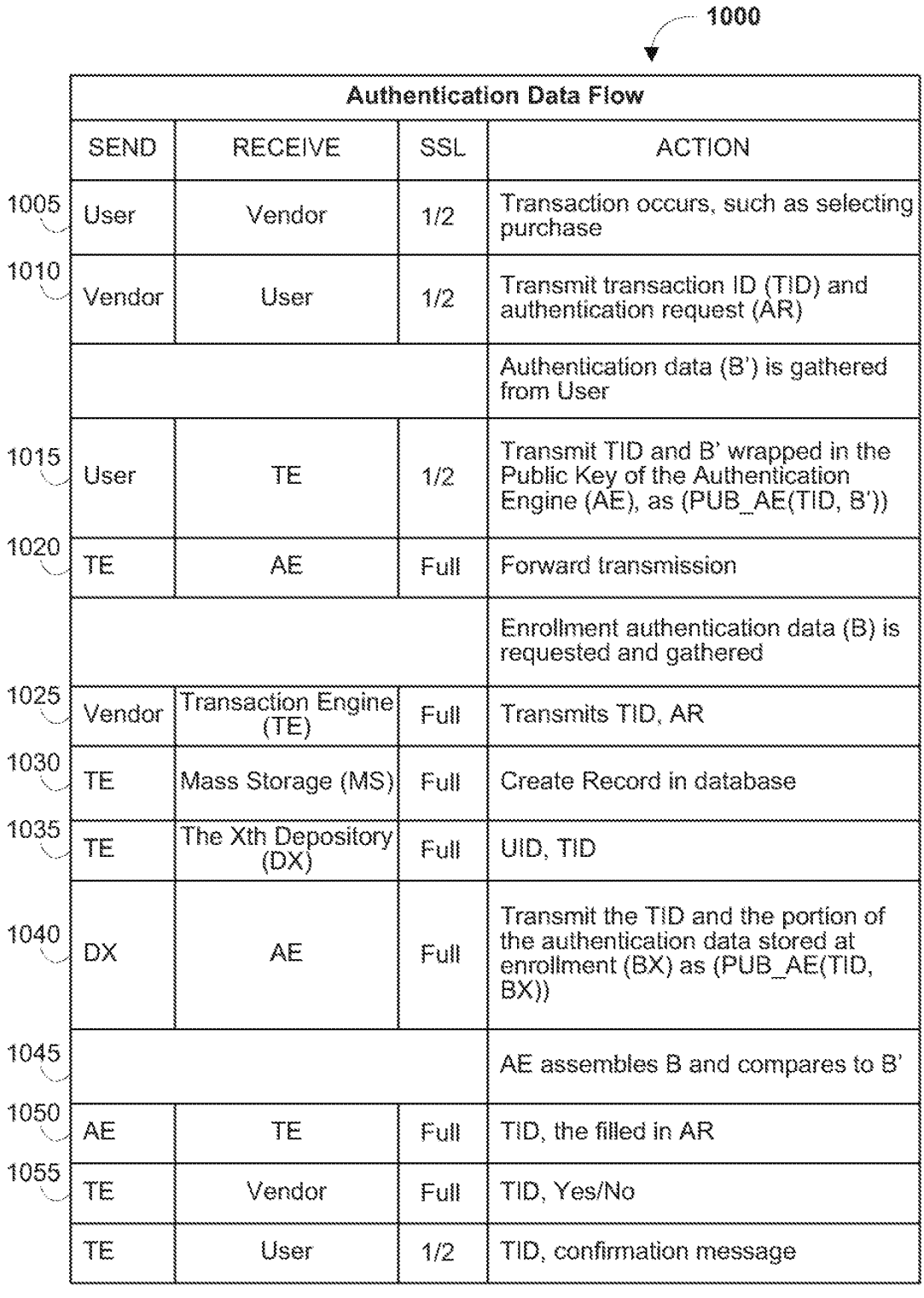

1000
Authentication Data Flow
SEND
RECEIVE
SSL
ACTION
1005
User
Vendor
1/2
Transaction occurs, such as selecting purchase
1010
Vendor
User
1/2
Transmit transaction ID (TID) and authentication request (AR)
Authentication data (B') is gathered from User
1015
User
TE
1/2
Transmit TID and B' wrapped in the Public Key of the Authentication Engine (AE), as (PUB_AE(TID, B'))
1020
TE
AE
Full
Forward transmission
Enrollment authentication data (B) is requested and gathered
1025
Vendor
Transaction Engine (TE)
Full
Transmits TID, AR
1030
TE
Mass Storage (MS)
Full
Create Record in database
1035
TE
The Xth Depository (DX)
Full
UID, TID
1040
DX
AE
Full
Transmit the TID and the portion of the authentication data stored at enrollment (BX) as (PUB_AE(TID, BX))
1045
AE assembles B and compares to B'
1050
AE
TE
Full
TID, the filled in AR
1055
TE
Vendor
Full
TID, Yes/No
TE
User
1/2
TID, confirmation message

FIG. 10



Signing Data Flow			
SEND	RECEIVE	SSL	ACTION
User	Vendor	1/2	Transaction occurs, such as agreeing on a deal
Vendor	User	1/2	Transmit transaction identification number (TID), authentication request (AR), and agreement or message (M)
			Current authentication data (B') and a hash of the message received by the User (h(M')) is is gathered from User
User	TE	1/2	Transmit TID, B', AR, and h(M') wrapped in the Public Key of the Authentication Engine (AE), as (PUB_AE(TID, B', h(M'))
TE	AE	Full	Forward transmission
			Gather enrollment authentication data
Vendor	Transaction Engine (TE)	Full	Transmits UID, TID, AR, and a hash of the message (h(M')).
TE	Mass Storage (MS)	Full	Create Record in database
TE	The Xth Depository (DX)	Full	UID, TID
DX	AE	Full	Transmit the TID and the portion of the authentication data stored at Enrollment (BX), as (PUB_AE(TID, BX))
			The original vendor message is transmitted to the AE
TE	AE	Full	Transmit h(M)
			AE assembles B, compares to B' and compares h(M) to h(M')
AE	Cryptographic Engine (CE)	Full	Request for digital signature and a message to be signed, for example, the hashed message
AE	DX	Full	TID, signing UID
DX	CE	Full	Transmit the portion of the Crypto-graphic Key corresponding to the signing party
			CE assembles key and signs
CE	AE	Full	Transmit the digital signature (S) of signing party
AE	TE	Full	TID, the filled in AR, h(M), and S
TE	Vendor	Full	TID, a receipt=(TID, Yes/No, and S), and the digital signature of the trust engine, for example, a hash of the receipt encrypted with the trust engine's Private Key (Priv_TE(h(receipt)))
TE	User	1/2	TID, confirmation message

1103
1105
1110
1115
1120
1125
1130
1135
1140

FIG. 11

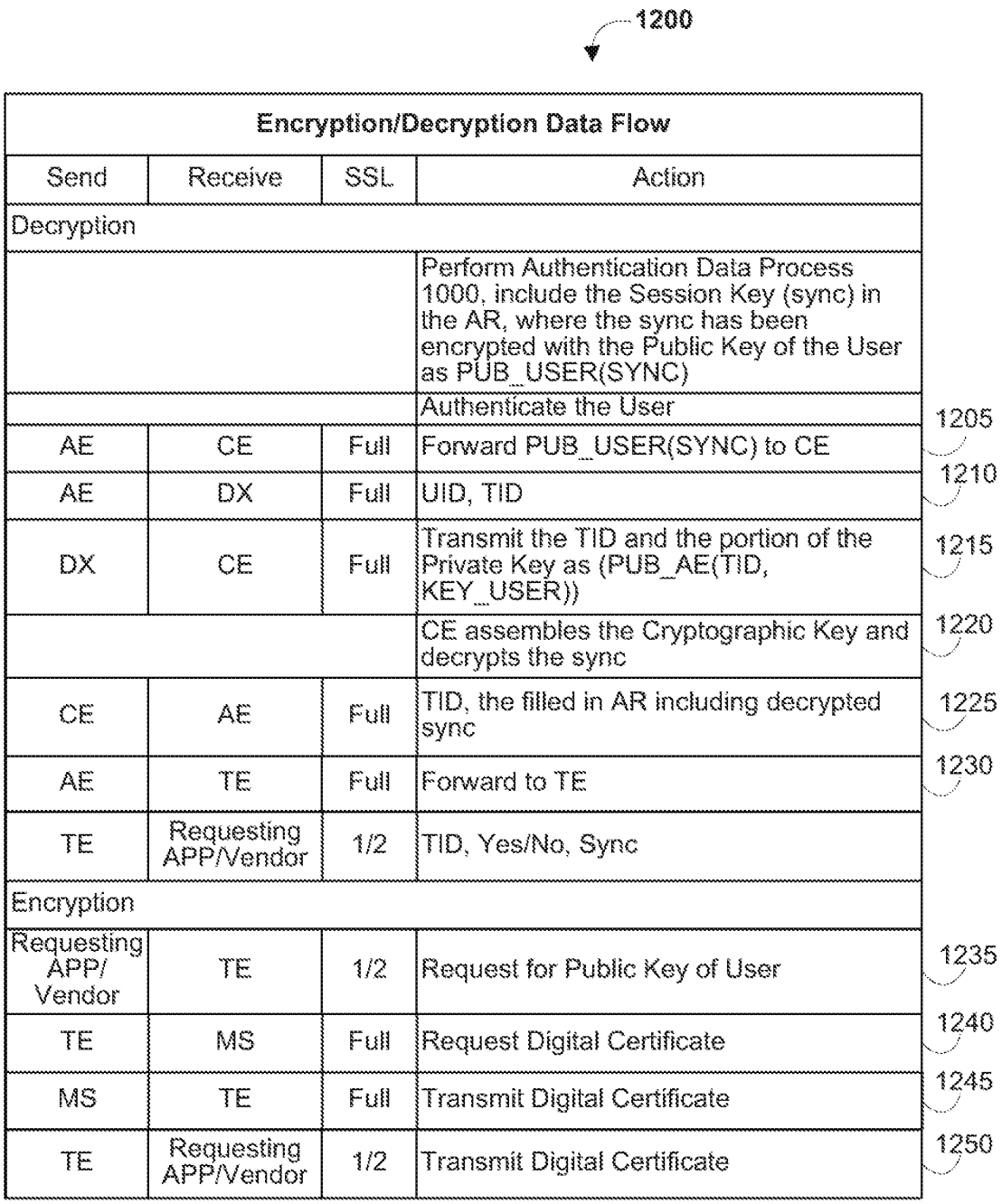

1200
Encryption/Decryption Data Flow
Send
Receive
SSL
Action
Decryption
Perform Authentication Data Process 1000, include the Session Key (sync) in the AR, where the sync has been encrypted with the Public Key of the User as PUB_USER(SYNC)
Authenticate the User
1205
AE
CE
Full
Forward PUB_USER(SYNC) to CE
1210
AE
DX
Full
UID, TID
1215
DX
CE
Full
Transmit the TID and the portion of the Private Key as (PUB_AE(TID, KEY_USER))
1220
CE assembles the Cryptographic Key and decrypts the sync
1225
CE
AE
Full
TID, the filled in AR including decrypted sync
1230
AE
TE
Full
Forward to TE
TE
Requesting APP/Vendor
1/2
TID, Yes/No, Sync
Encryption
1235
Requesting APP/ Vendor
TE
1/2
Request for Public Key of User
1240
TE
MS
Full
Request Digital Certificate
1245
MS
TE
Full
Transmit Digital Certificate
1250
TE
Requesting APP/Vendor
1/2
Transmit Digital Certificate

FIG. 12

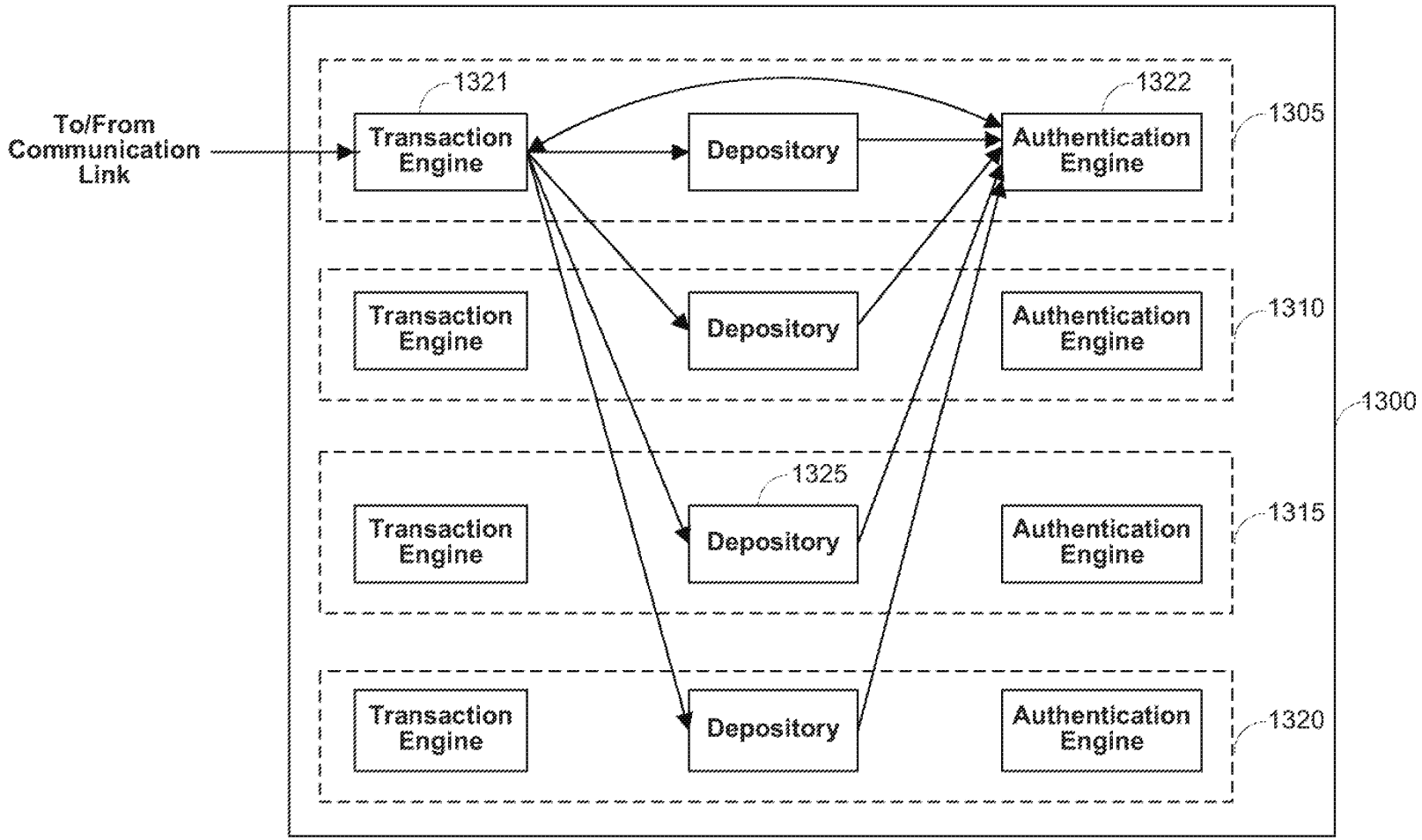


FIG. 13

EX1002 - Page 468

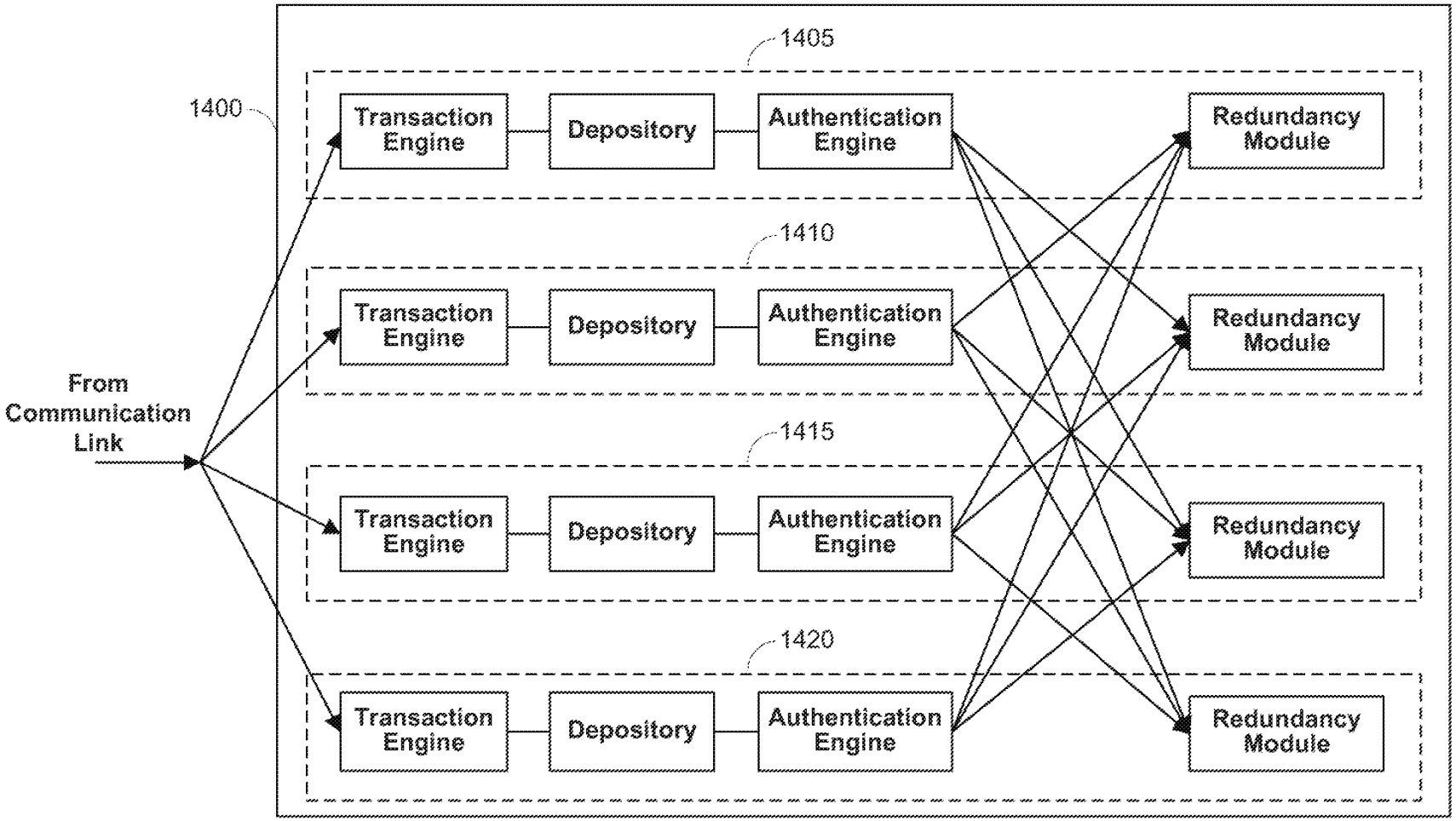


FIG. 14

EX1002 - Page 469

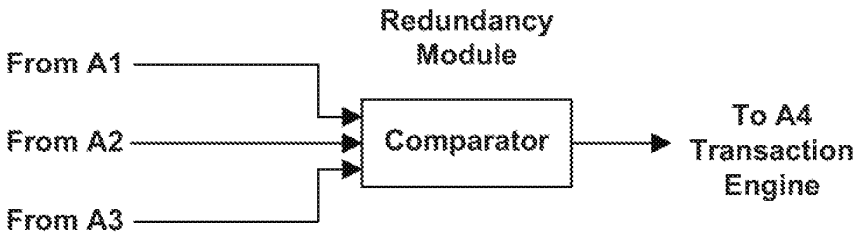

Redundancy
Module
From A1
From A2
From A3
Comparator
To A4
Transaction
Engine

FIG. 15

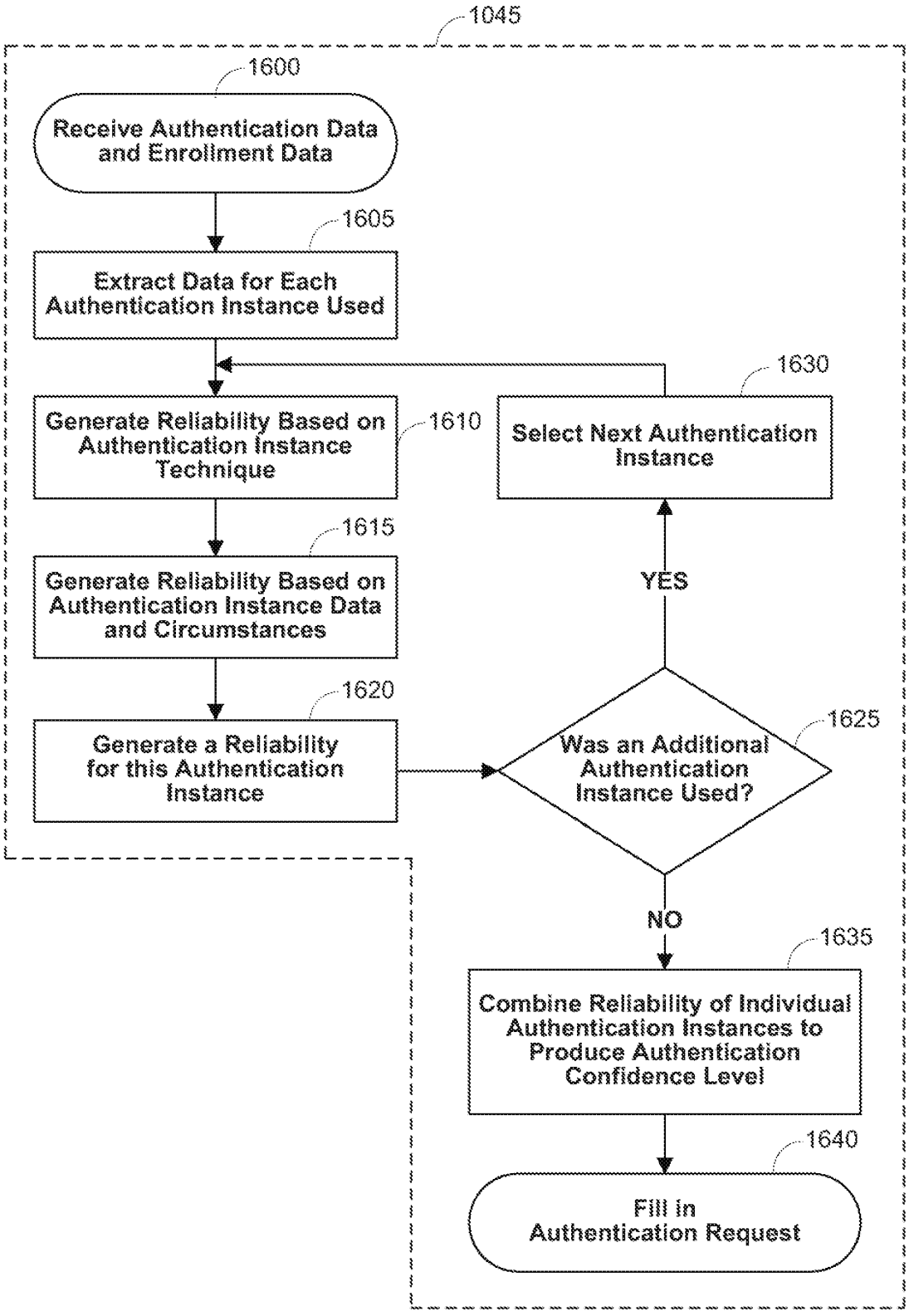

1045
1600
Receive Authentication Data and Enrollment Data
1605
Extract Data for Each Authentication Instance Used
1630
Generate Reliability Based on Authentication Instance Technique
1610
Select Next Authentication Instance
1615
Generate Reliability Based on Authentication Instance Data and Circumstances
YES
1620
Generate a Reliability for this Authentication Instance
Was an Additional Authentication Instance Used?
1625
NO
1635
Combine Reliability of Individual Authentication Instances to Produce Authentication Confidence Level
1640
Fill in Authentication Request

FIG. 16

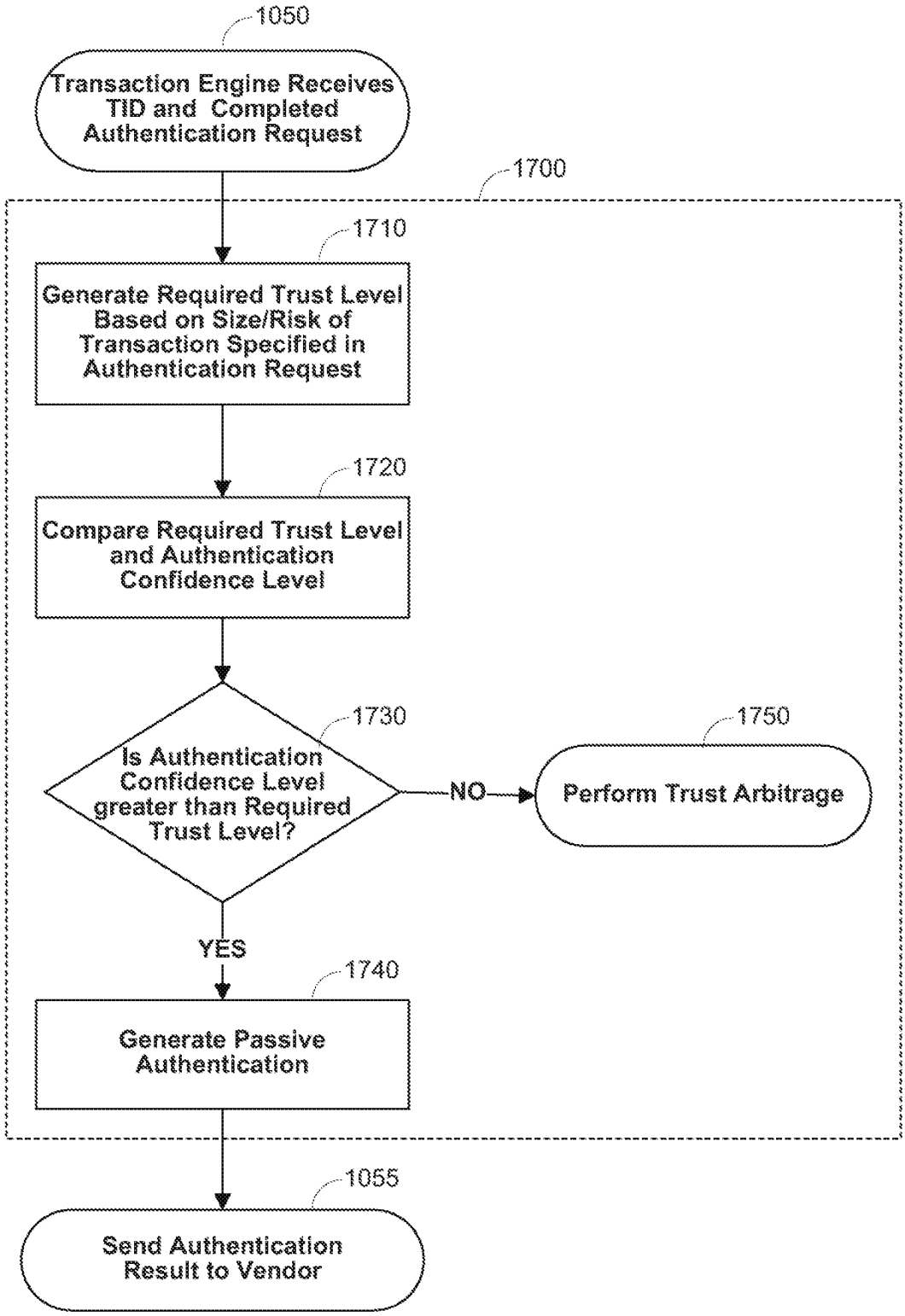

1050
Transaction Engine Receives TID and Completed Authentication Request
1700
1710
Generate Required Trust Level Based on Size/Risk of Transaction Specified in Authentication Request
1720
Compare Required Trust Level and Authentication Confidence Level
1730
Is Authentication Confidence Level greater than Required Trust Level?
NO
1750
Perform Trust Arbitrage
YES
1740
Generate Passive Authentication
1055
Send Authentication Result to Vendor

FIG. 17

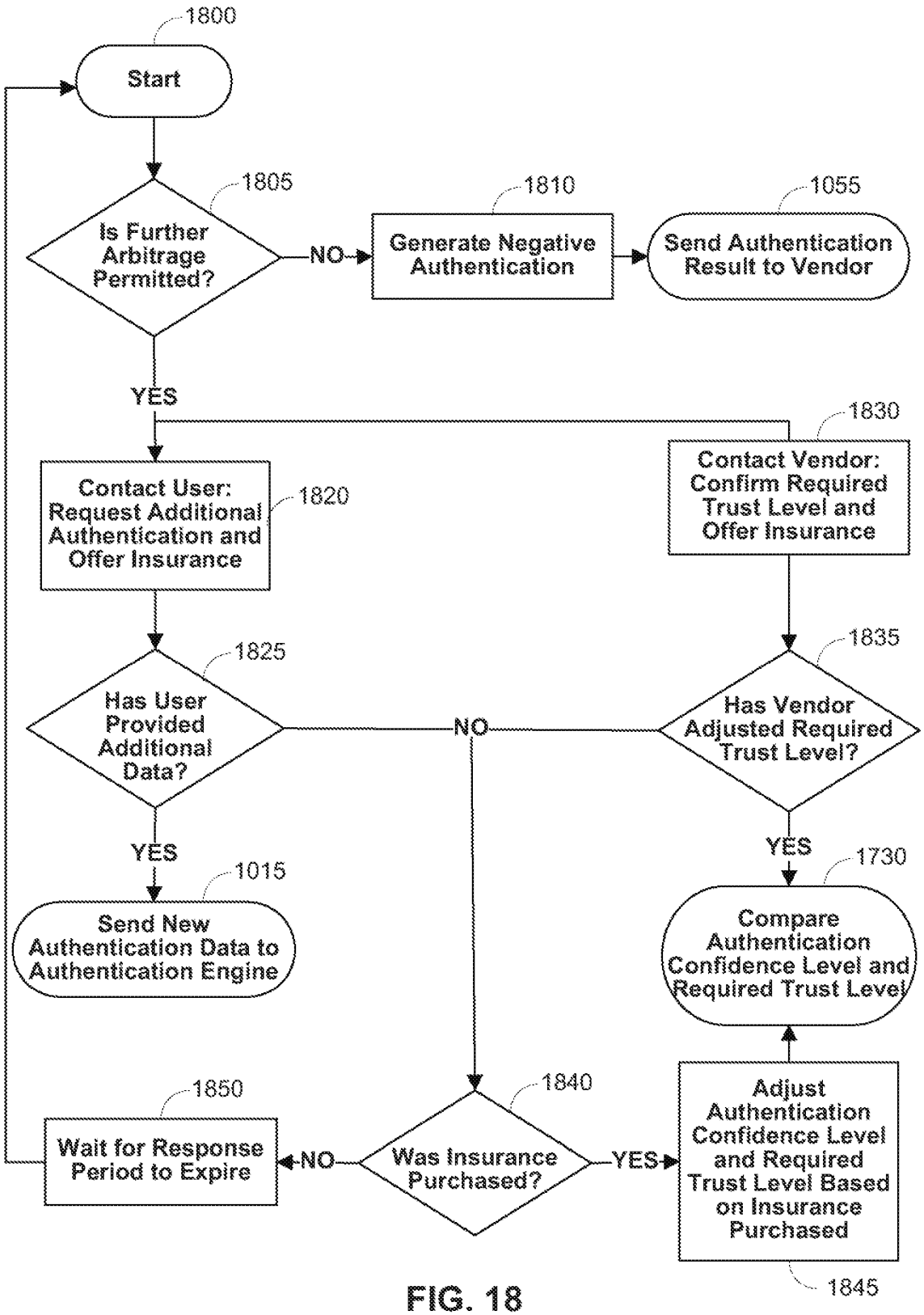

1800
Start
1805
Is Further Arbitrage Permitted?
NO
1810
Generate Negative Authentication
1055
Send Authentication Result to Vendor
YES
1830
Contact Vendor: Confirm Required Trust Level and Offer Insurance
Contact User: Request Additional Authentication and Offer Insurance
1820
1825
Has User Provided Additional Data?
NO
1835
Has Vendor Adjusted Required Trust Level?
YES
1015
Send New Authentication Data to Authentication Engine
YES
1730
Compare Authentication Confidence Level and Required Trust Level
1850
Wait for Response Period to Expire
NO
1840
Was Insurance Purchased?
YES
Adjust Authentication Confidence Level and Required Trust Level Based on Insurance Purchased
1845

FIG. 18

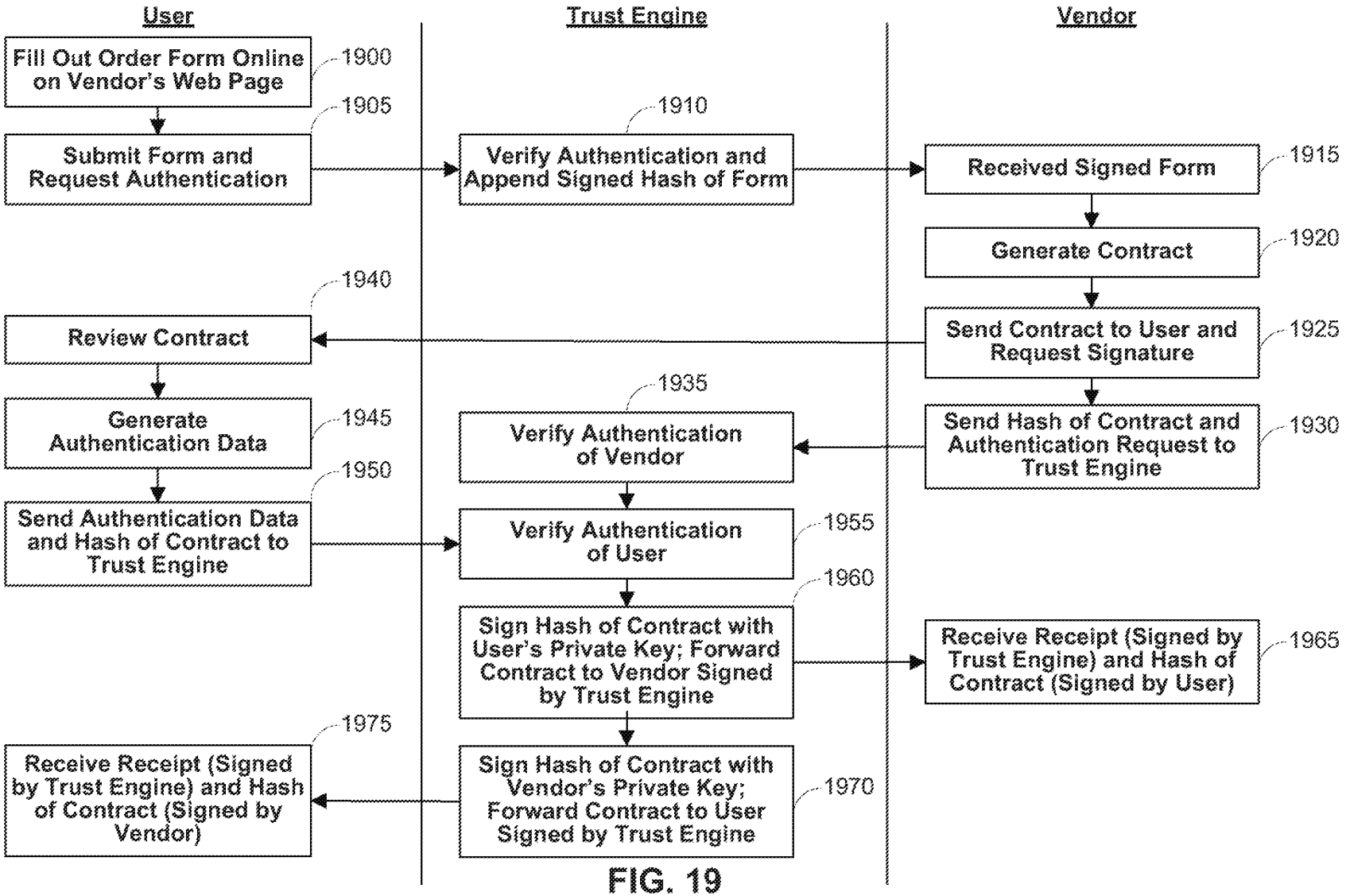


FIG. 19

EX1002 - Page 474

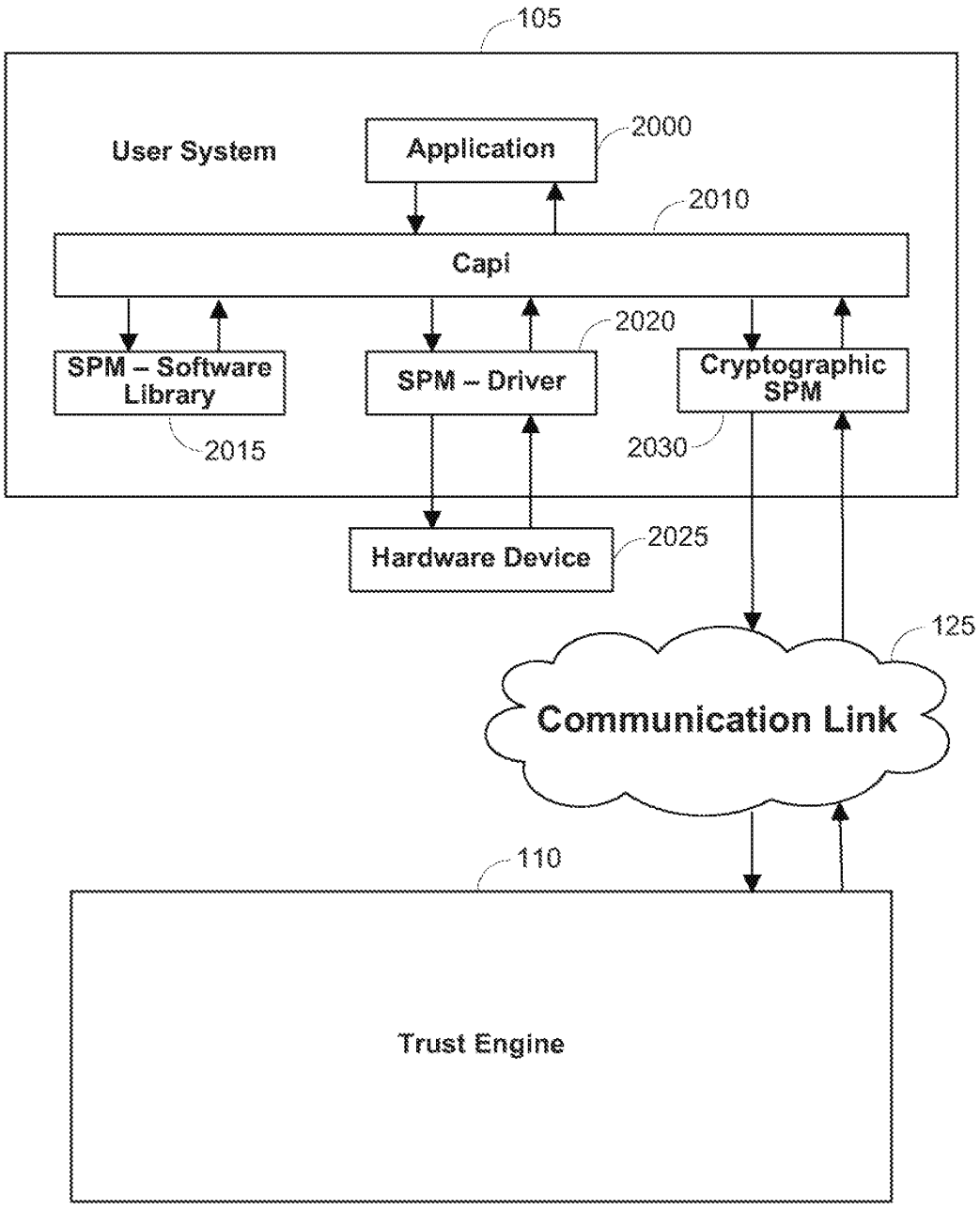

105
User System
Application
2000
2010
Capi
2020
SPM – Software Library
SPM – Driver
Cryptographic SPM
2015
2030
Hardware Device
2025
125
Communication Link
110
Trust Engine

FIG. 20

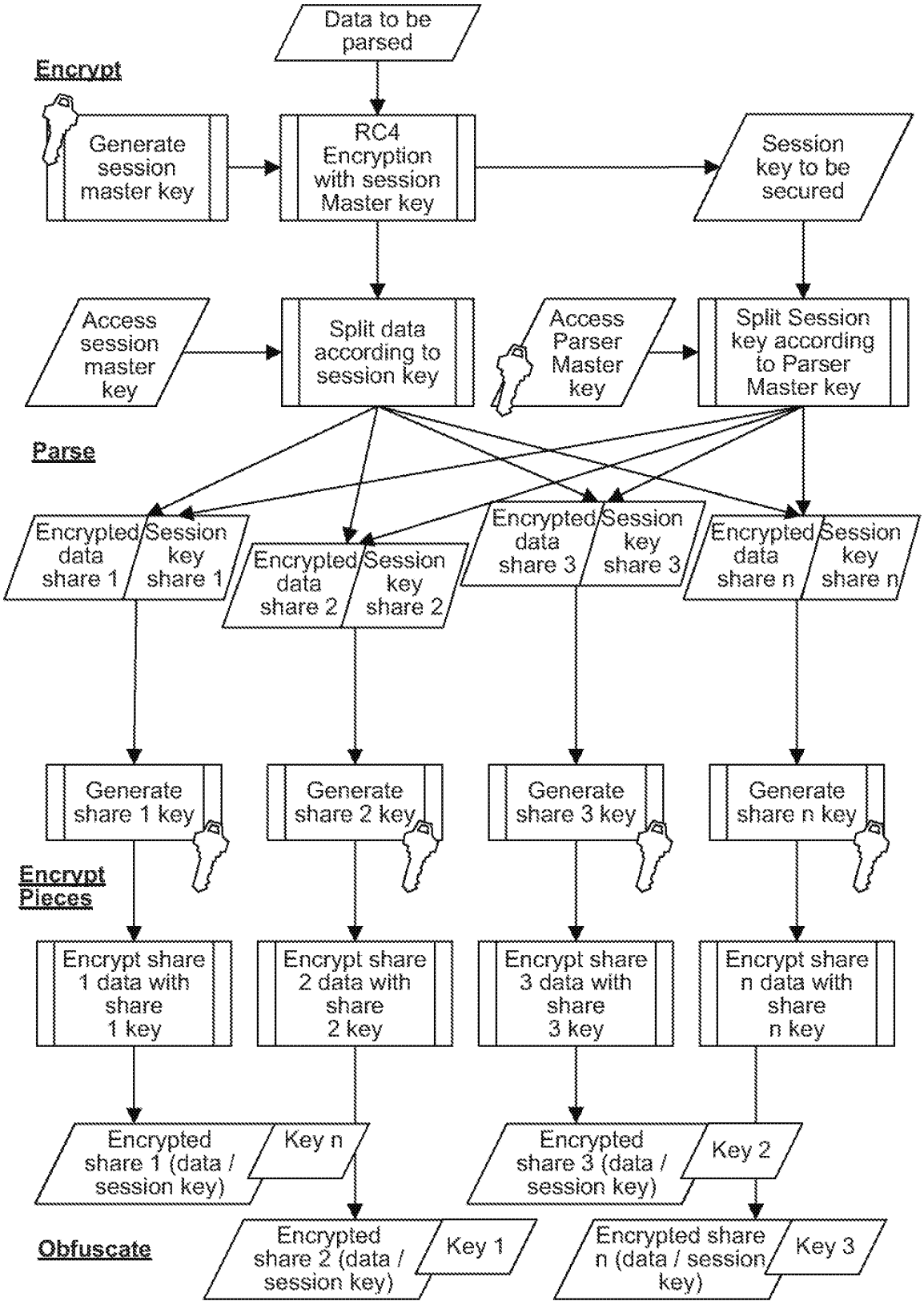

Data to be parsed
Encrypt
Generate session master key
RC4 Encryption with session Master key
Session key to be secured
Access session master key
Split data according to session key
Access Parser Master key
Split Session key according to Parser Master key
Parse
Encrypted data share 1
Session key share 1
Encrypted data share 2
Session key share 2
Encrypted data share 3
Session key share 3
Encrypted data share n
Session key share n
Generate share 1 key
Generate share 2 key
Generate share 3 key
Generate share n key
Encrypt Pieces
Encrypt share 1 data with share 1 key
Encrypt share 2 data with share 2 key
Encrypt share 3 data with share 3 key
Encrypt share n data with share n key
Encrypted share 1 (data / session key)
Key n
Encrypted share 3 (data / session key)
Key 2
Obfuscate
Encrypted share 2 (data / session key)
Key 1
Encrypted share n (data / session key)
Key 3

FIG. 21

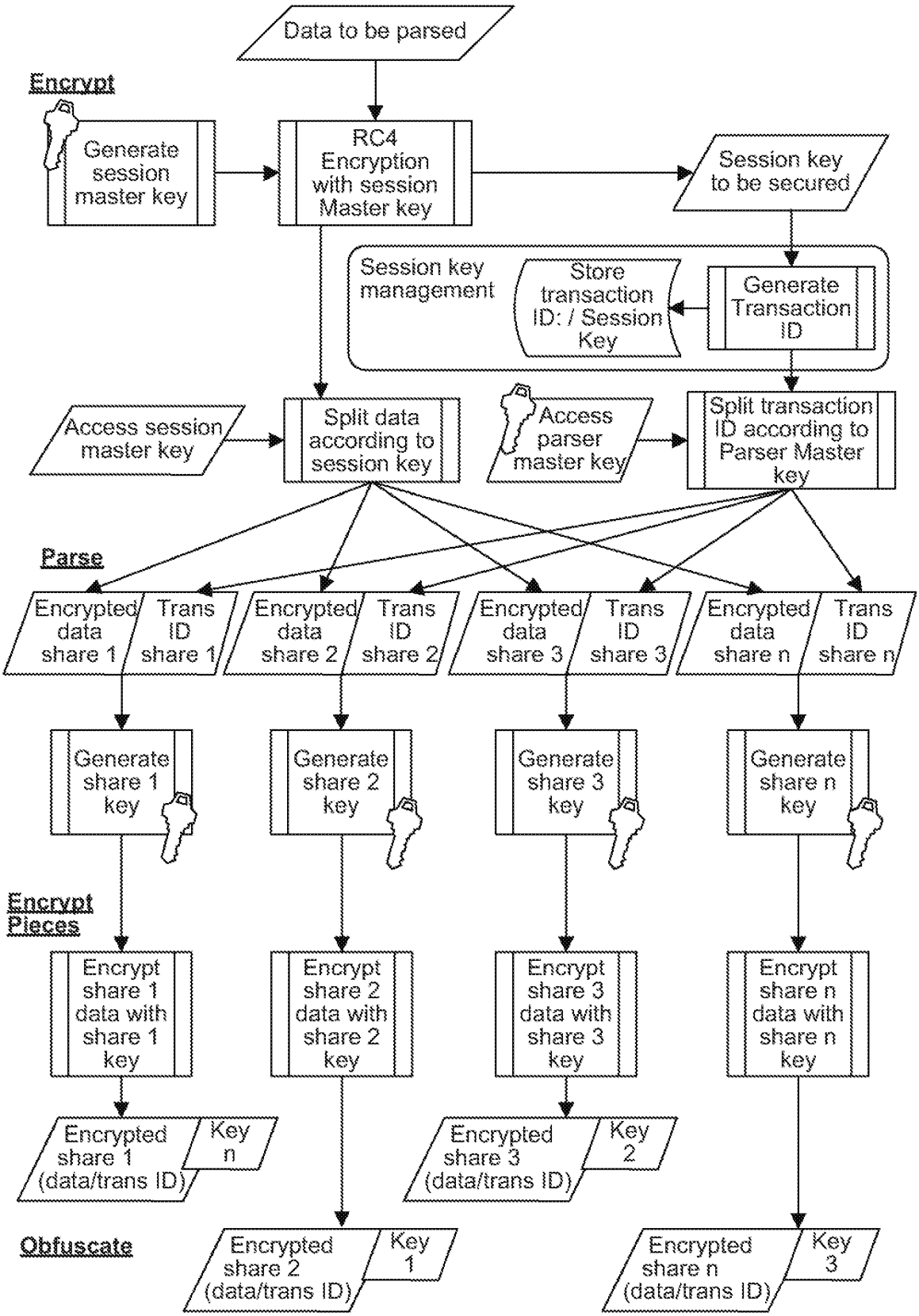

Data to be parsed
Encrypt
Generate session master key
RC4 Encryption with session Master key
Session key to be secured
Session key management
Store transaction ID: / Session Key
Generate Transaction ID
Access session master key
Split data according to session key
Access parser master key
Split transaction ID according to Parser Master key
Parse
Encrypted data share 1
Trans ID share 1
Encrypted data share 2
Trans ID share 2
Encrypted data share 3
Trans ID share 3
Encrypted data share n
Trans ID share n
Generate share 1 key
Generate share 2 key
Generate share 3 key
Generate share n key
Encrypt Pieces
Encrypt share 1 data with share 1 key
Encrypt share 2 data with share 2 key
Encrypt share 3 data with share 3 key
Encrypt share n data with share n key
Encrypted share 1 (data/trans ID)
Key n
Encrypted share 3 (data/trans ID)
Key 2
Obfuscate
Encrypted share 2 (data/trans ID)
Key 1
Encrypted share n (data/trans ID)
Key 3

FIG. 22

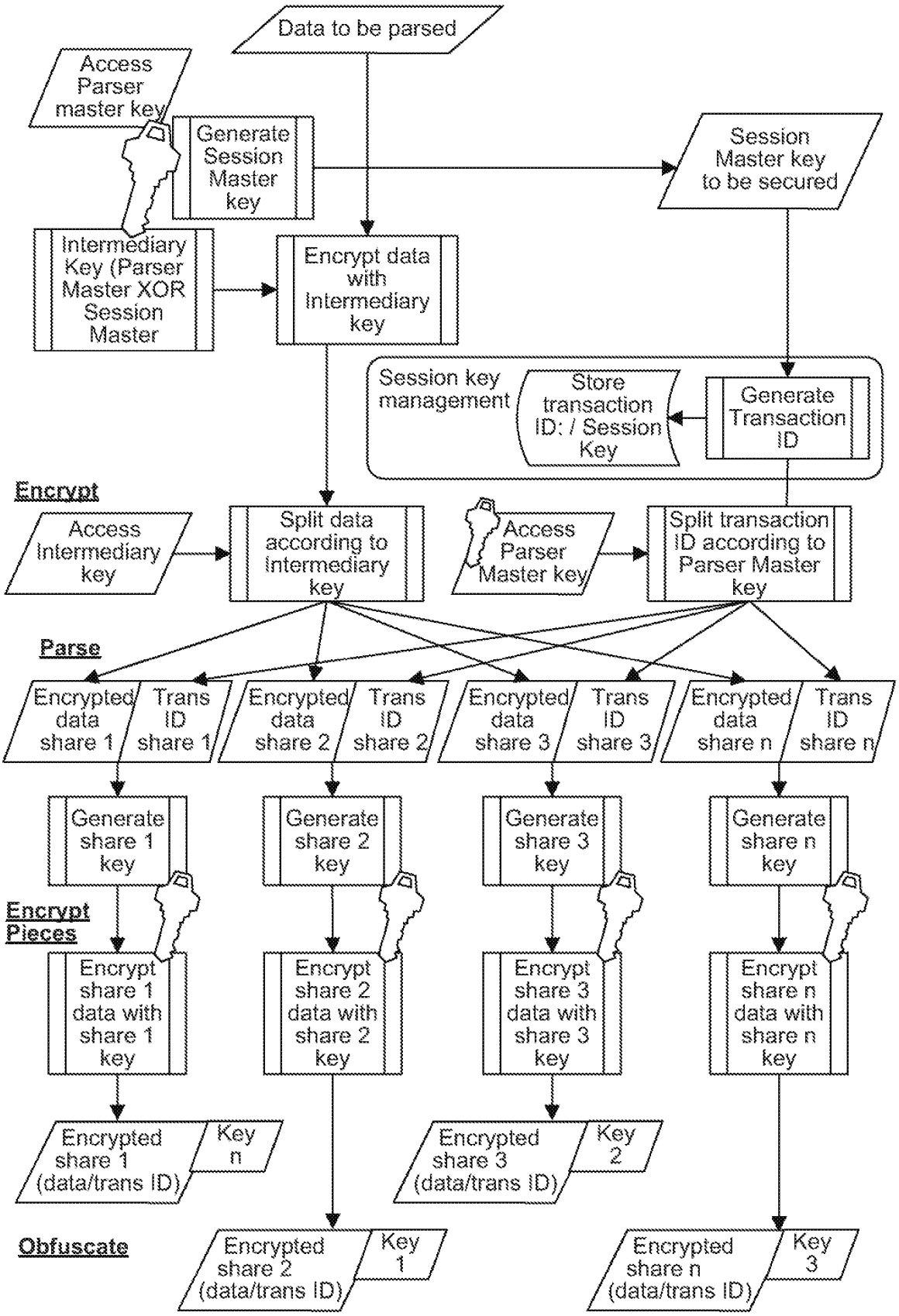

Data to be parsed
Access Parser master key
Generate Session Master key
Session Master key to be secured
Intermediary Key (Parser Master XOR Session Master
Encrypt data with Intermediary key
Session key management
Store transaction ID: / Session Key
Generate Transaction ID
Encrypt
Access Intermediary key
Split data according to Intermediary key
Access Parser Master key
Split transaction ID according to Parser Master key
Parse
Encrypted data share 1
Trans ID share 1
Encrypted data share 2
Trans ID share 2
Encrypted data share 3
Trans ID share 3
Encrypted data share n
Trans ID share n
Generate share 1 key
Generate share 2 key
Generate share 3 key
Generate share n key
Encrypt Pieces
Encrypt share 1 data with share 1 key
Encrypt share 2 data with share 2 key
Encrypt share 3 data with share 3 key
Encrypt share n data with share n key
Encrypted share 1 (data/trans ID)
Key n
Encrypted share 3 (data/trans ID)
Key 2
Obfuscate
Encrypted share 2 (data/trans ID)
Key 1
Encrypted share n (data/trans ID)
Key 3

FIG. 23

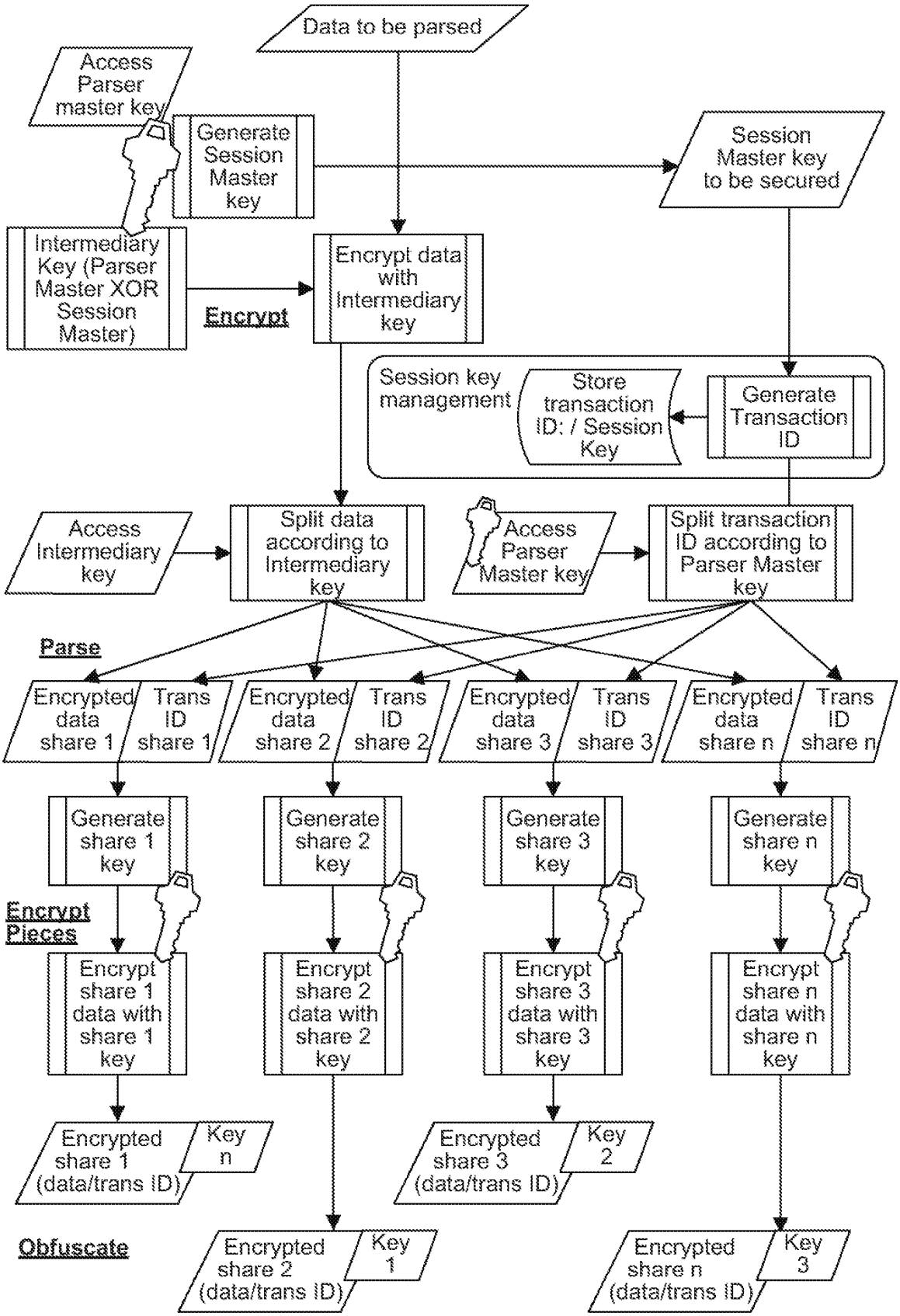

Data to be parsed
Access Parser master key
Generate Session Master key
Session Master key to be secured
Intermediary Key (Parser Master XOR Session Master)
Encrypt
Encrypt data with Intermediary key
Session key management
Store transaction ID: / Session Key
Generate Transaction ID
Access Intermediary key
Split data according to Intermediary key
Access Parser Master key
Split transaction ID according to Parser Master key
Parse
Encrypted data share 1
Trans ID share 1
Encrypted data share 2
Trans ID share 2
Encrypted data share 3
Trans ID share 3
Encrypted data share n
Trans ID share n
Generate share 1 key
Generate share 2 key
Generate share 3 key
Generate share n key
Encrypt Pieces
Encrypt share 1 data with share 1 key
Encrypt share 2 data with share 2 key
Encrypt share 3 data with share 3 key
Encrypt share n data with share n key
Encrypted share 1 (data/trans ID)
Key n
Encrypted share 3 (data/trans ID)
Key 2
Obfuscate
Encrypted share 2 (data/trans ID)
Key 1
Encrypted share n (data/trans ID)
Key 3

FIG. 24

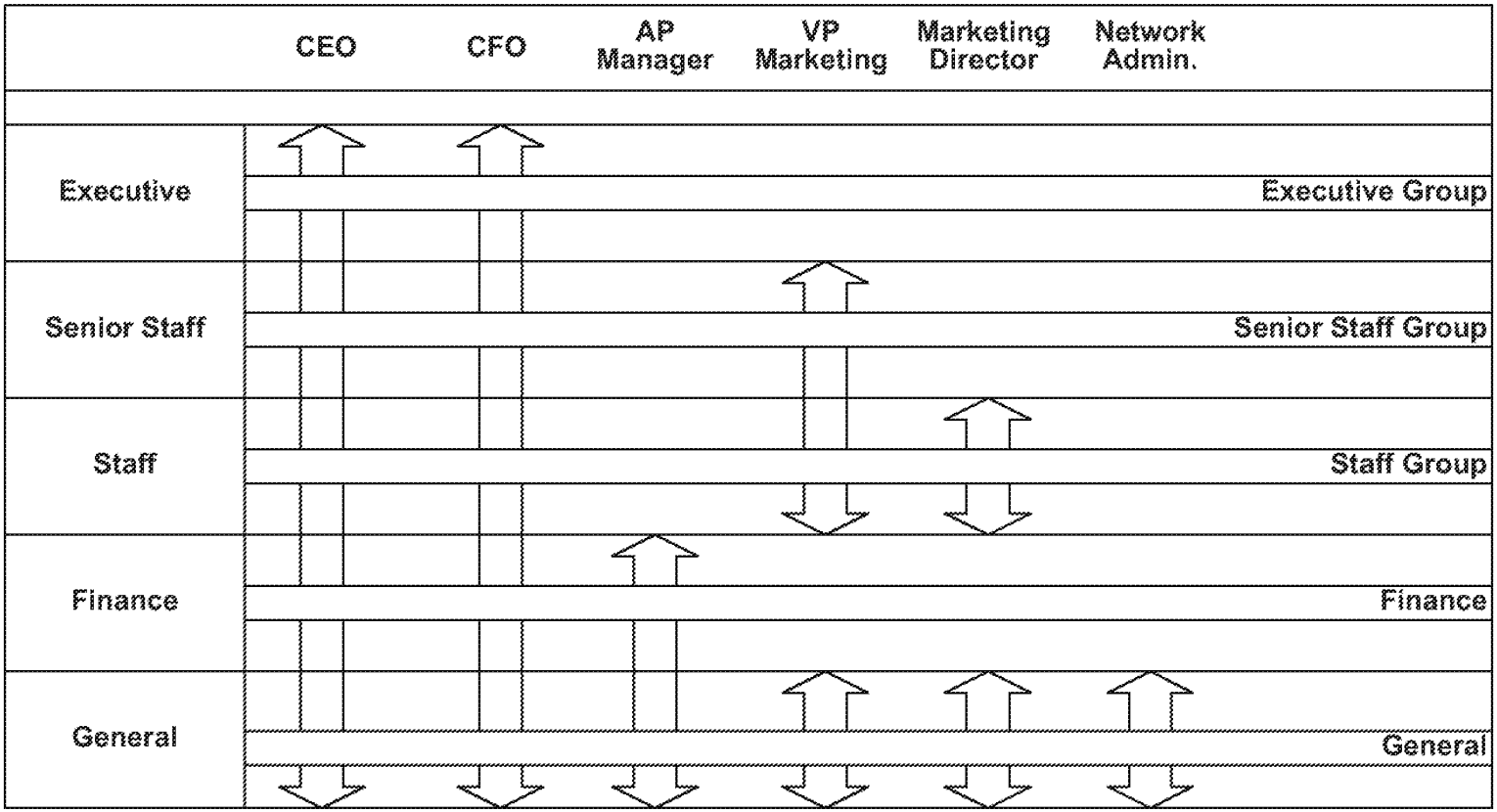


FIG. 25

EX1002 - Page 480

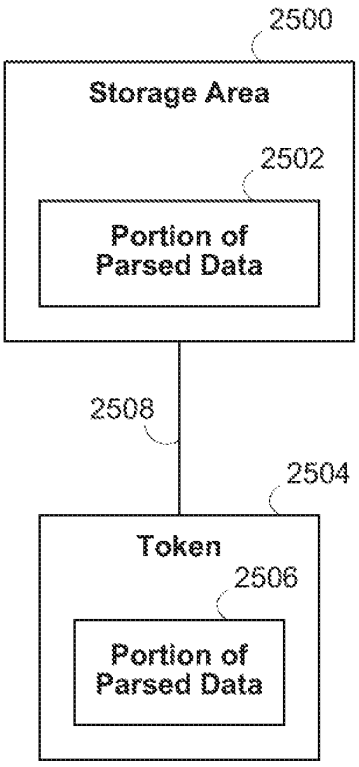

2500
Storage Area
2502
Portion of Parsed Data
2508
2504
Token
2506
Portion of Parsed Data

FIG. 26

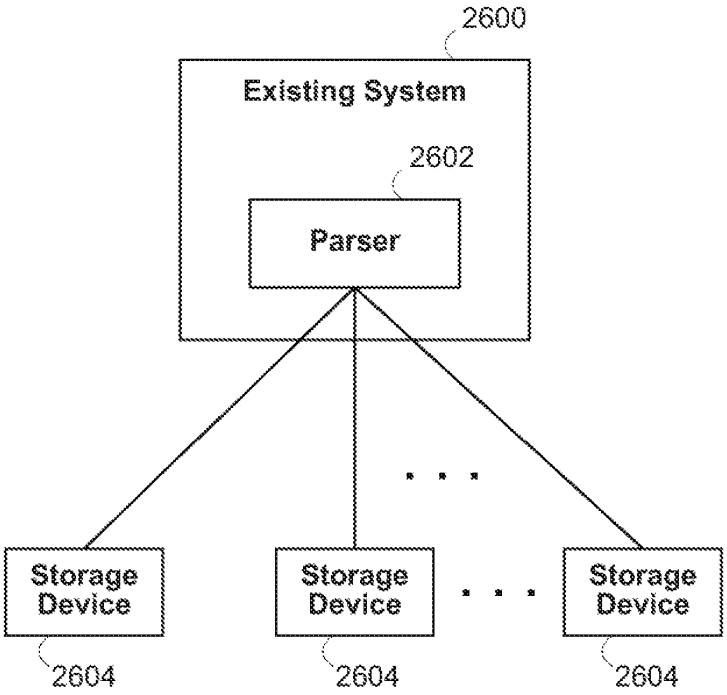

2600
Existing System
2602
Parser
Storage Device
2604
Storage Device
2604
Storage Device
2604

FIG. 27

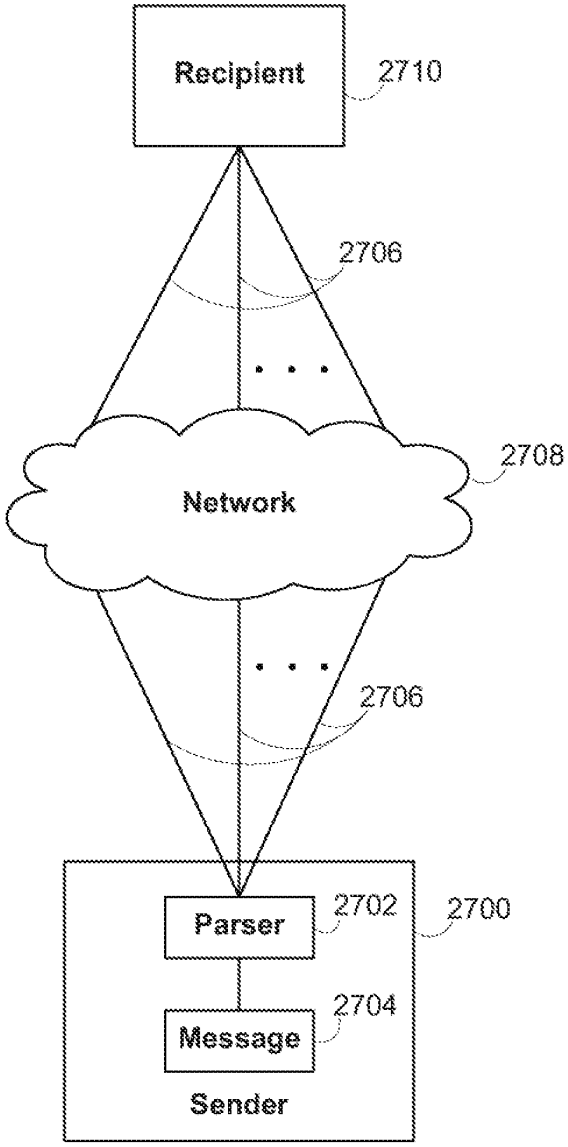

Recipient
2710
2706
2708
Network
2706
Parser
2702
2700
2704
Message
Sender

FIG. 28

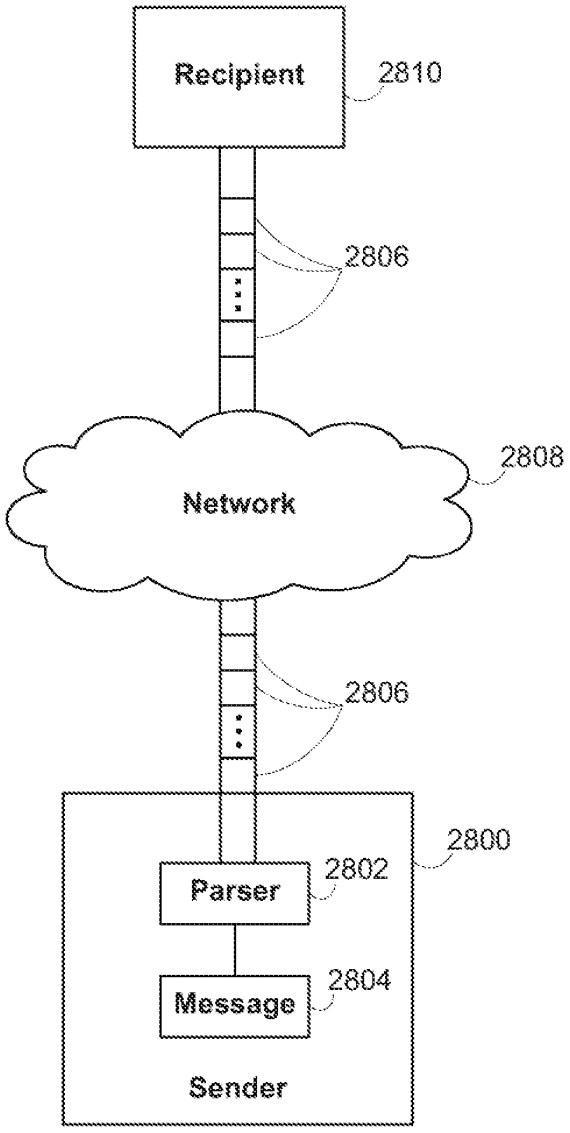

Recipient
2810
2806
Network
2808
2806
2800
Parser
2802
Message
2804
Sender

FIG. 29

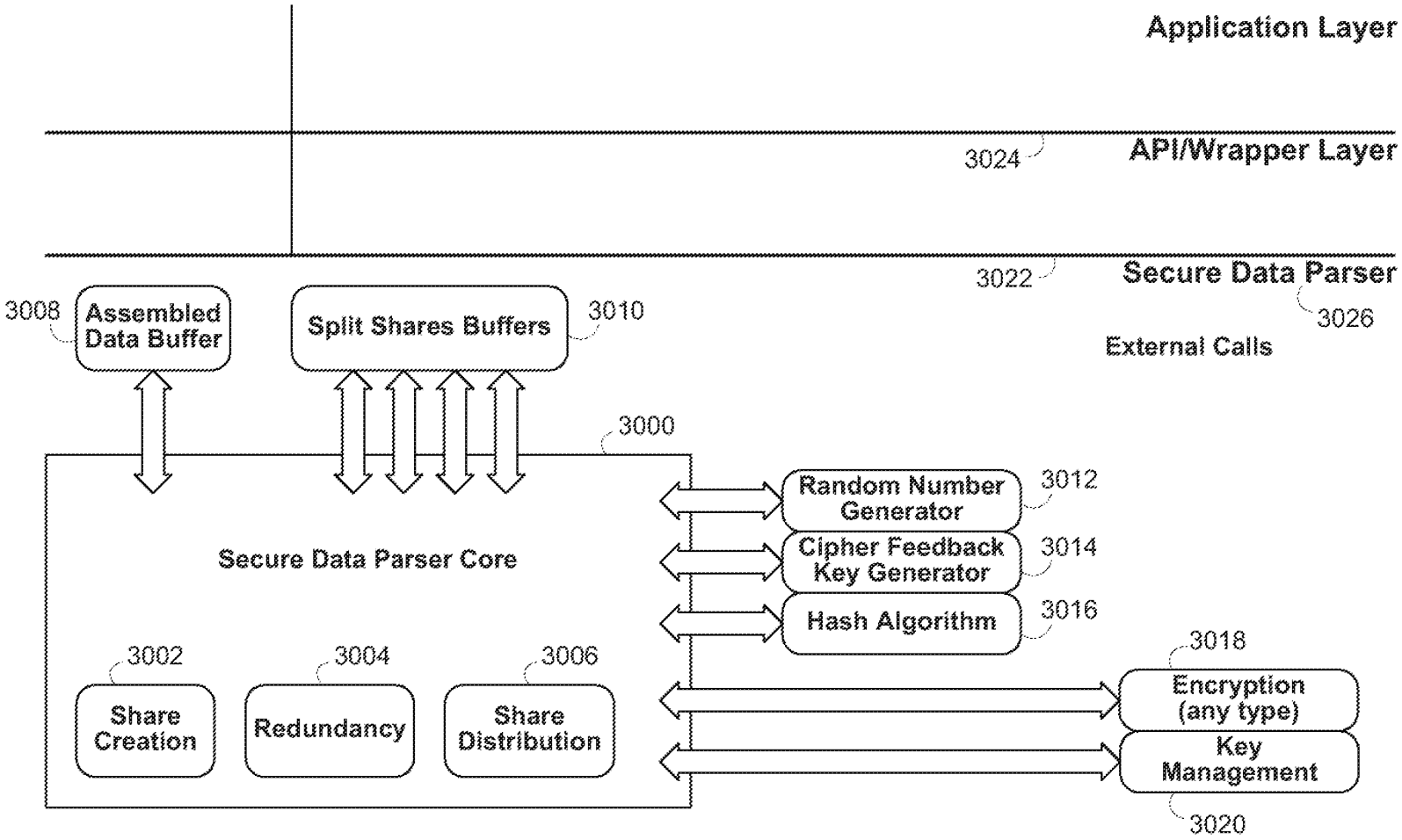


FIG. 30

EX1002 - Page 485

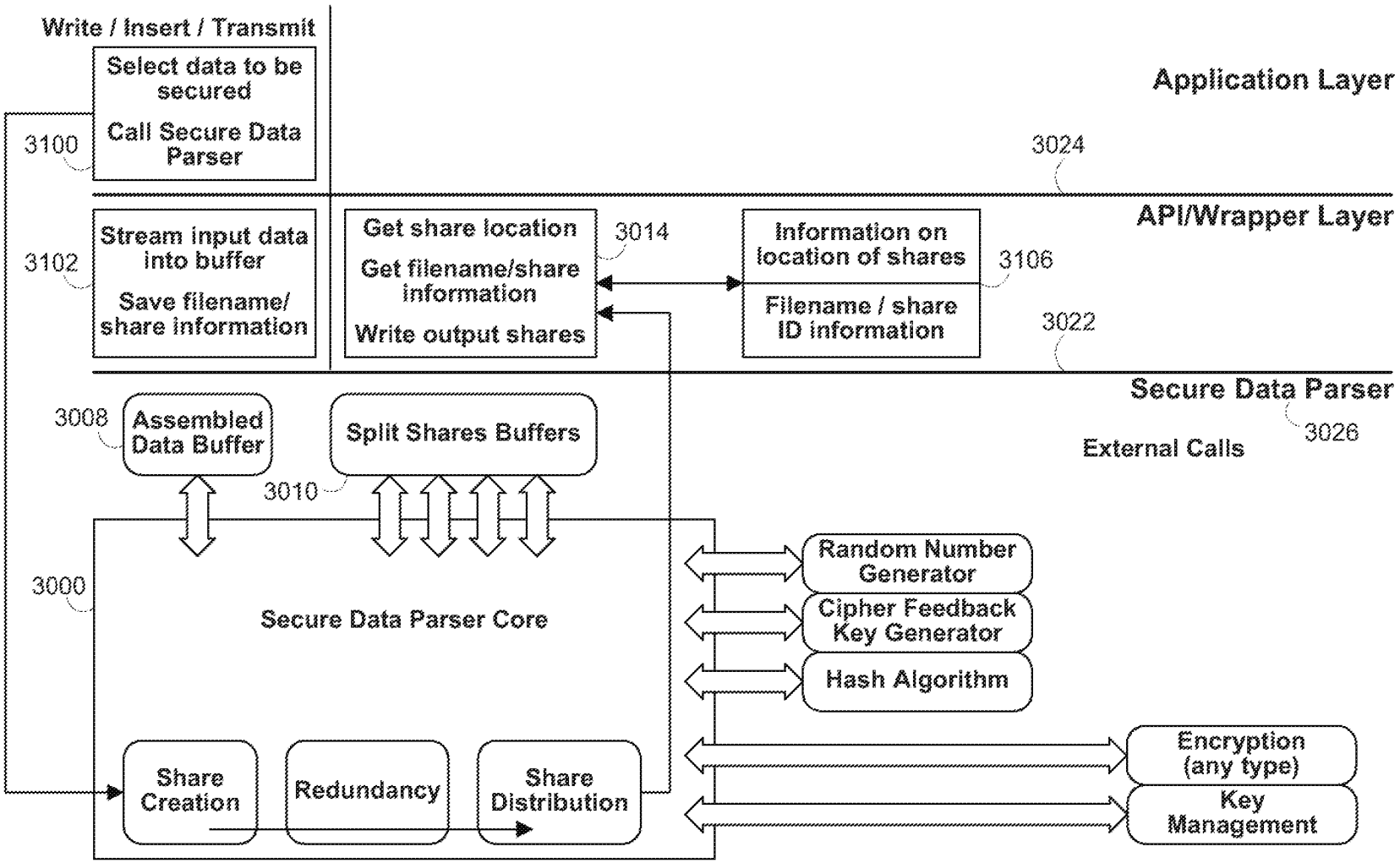


FIG. 31

EX1002 - Page 486

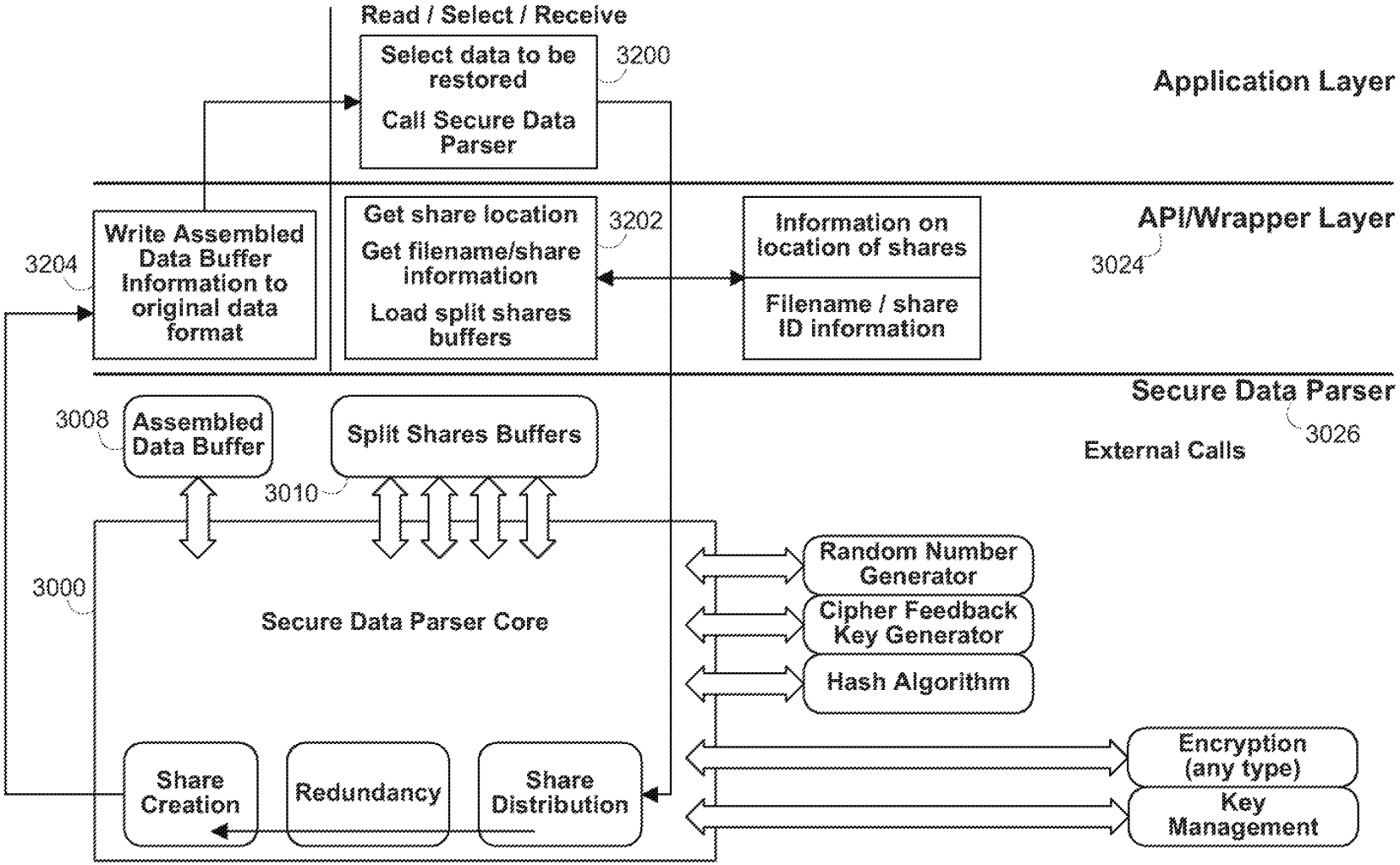


FIG. 32

EX1002 - Page 487

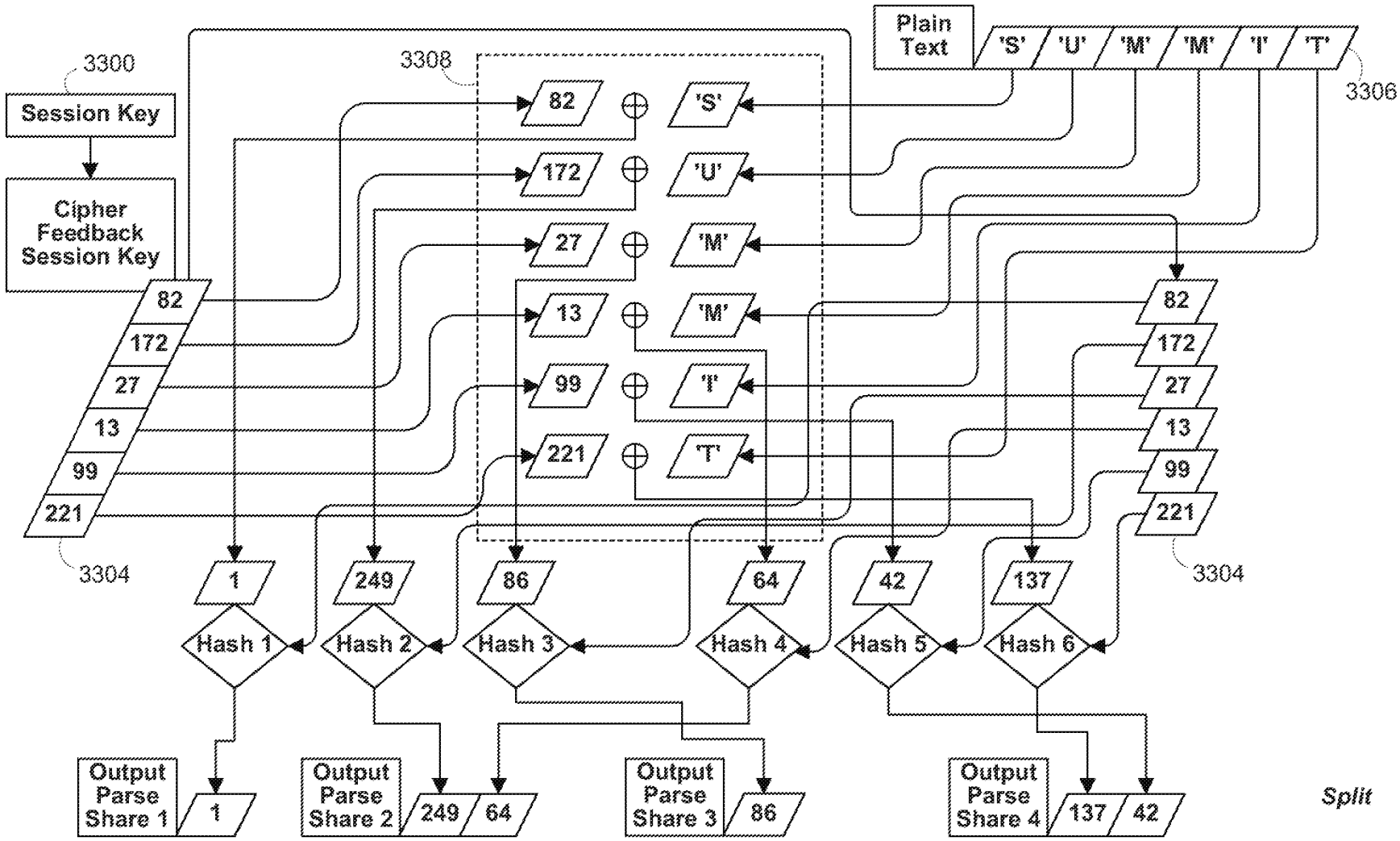


FIG. 33

EX1002 - Page 488

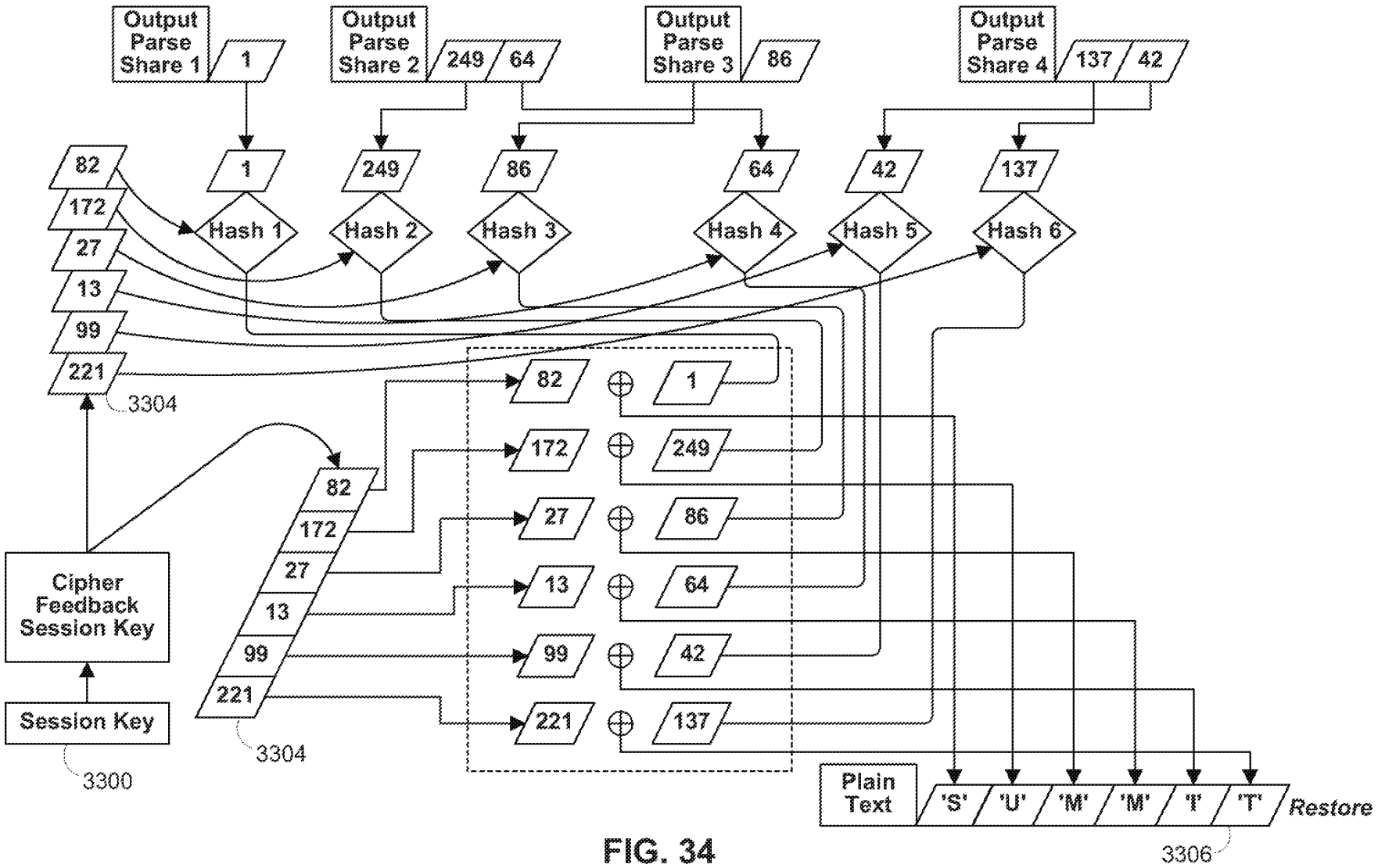


FIG. 34

EX1002 - Page 489

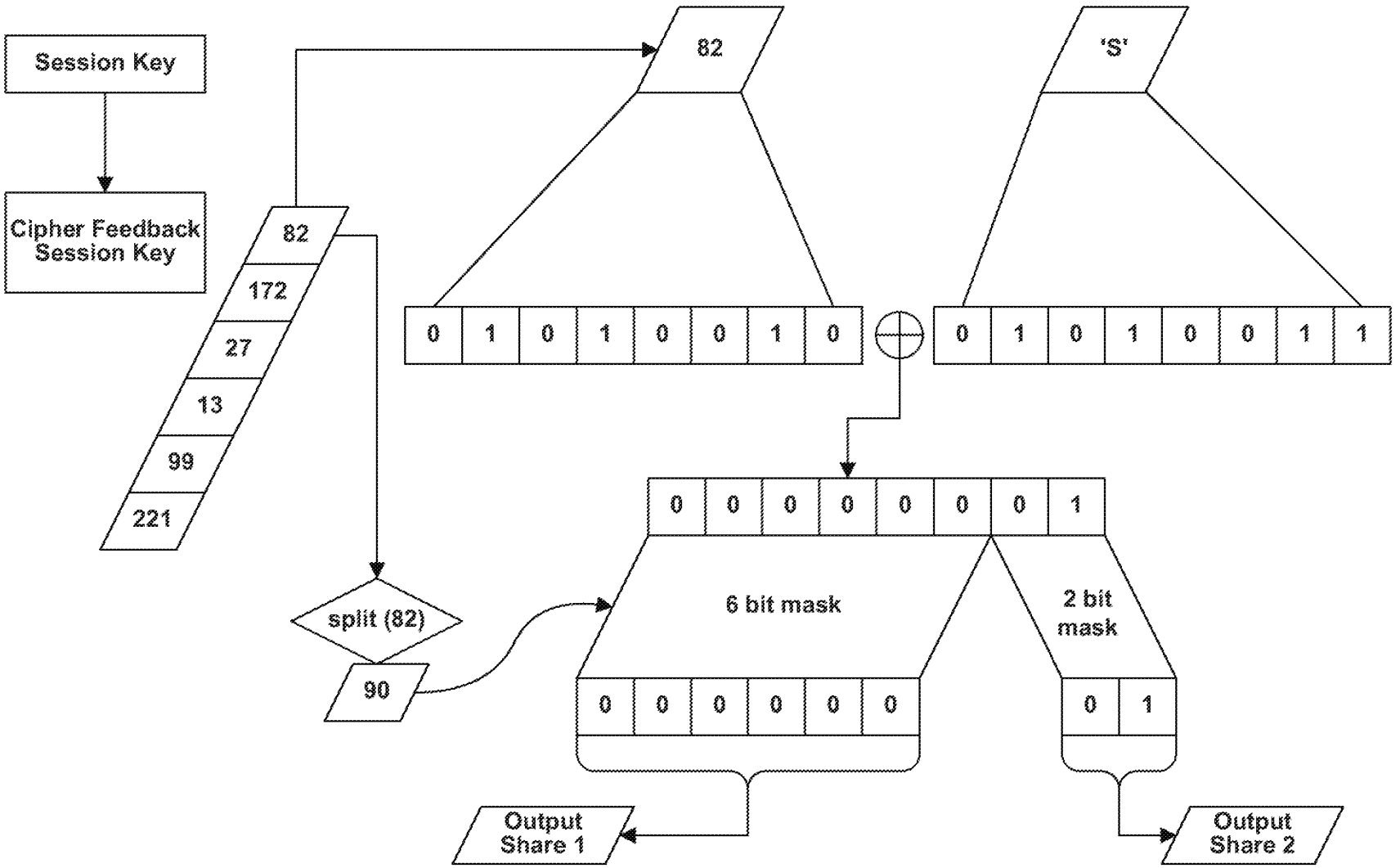


FIG. 35

EX1002 - Page 490

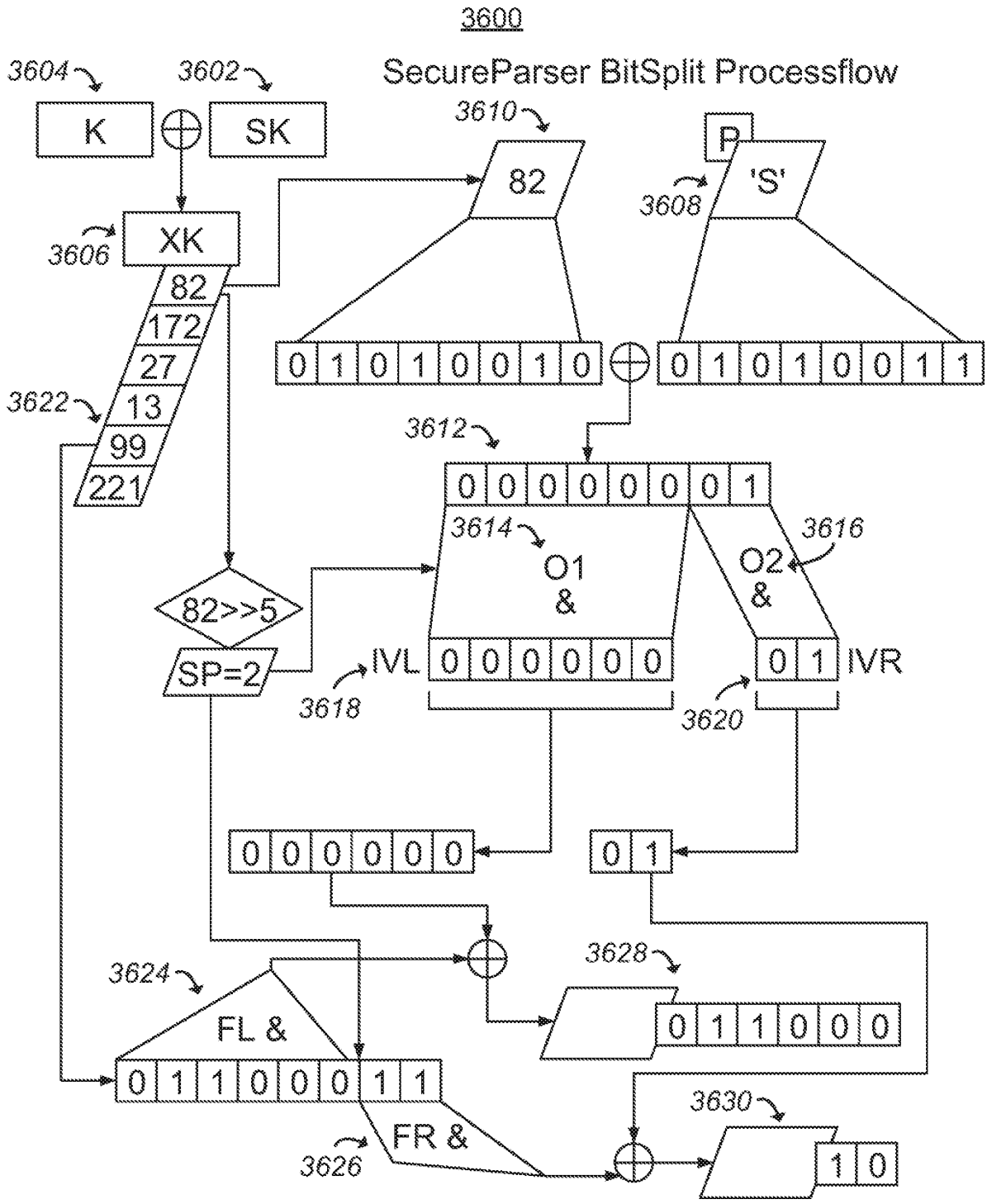

3600
SecureParser BitSplit Processflow
3604
3602
K
SK
3610
82
P
'S'
3608
3606
XK
82
172
27
13
99
221
3622
0 1 0 1 0 0 1 0
0 1 0 1 0 0 1 1
3612
0 0 0 0 0 0 0 1
3614
O1
&
3616
O2
&
82>>5
SP=2
IVL
0 0 0 0 0 0
0 1
IVR
3618
3620
0 0 0 0 0 0
0 1
3624
FL &
3628
0 1 1 0 0 0
0 1 1 0 0 0 1 1
3630
FR &
3626
1 0

FIG. 36

EX1002 - Page 492

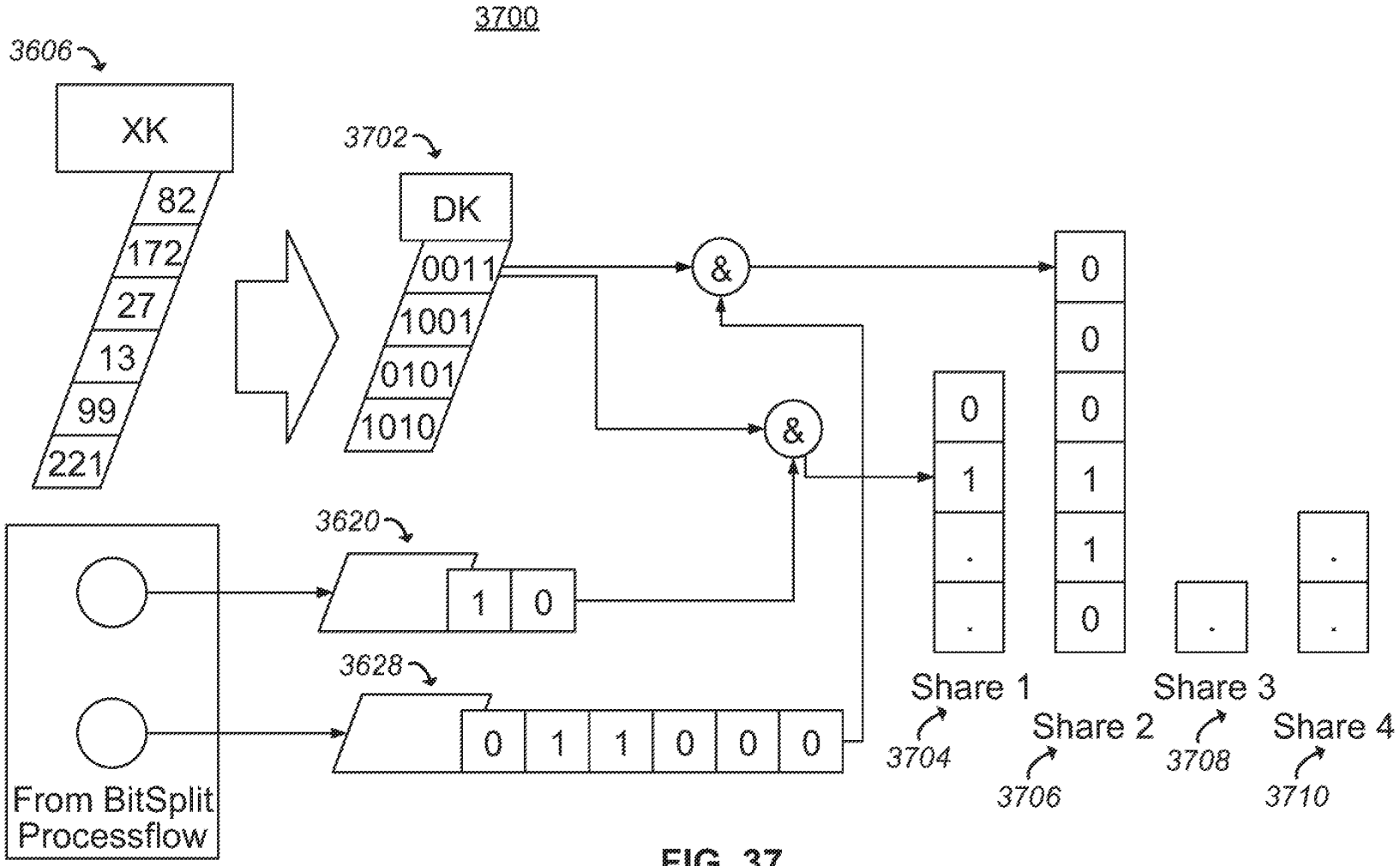


FIG. 37

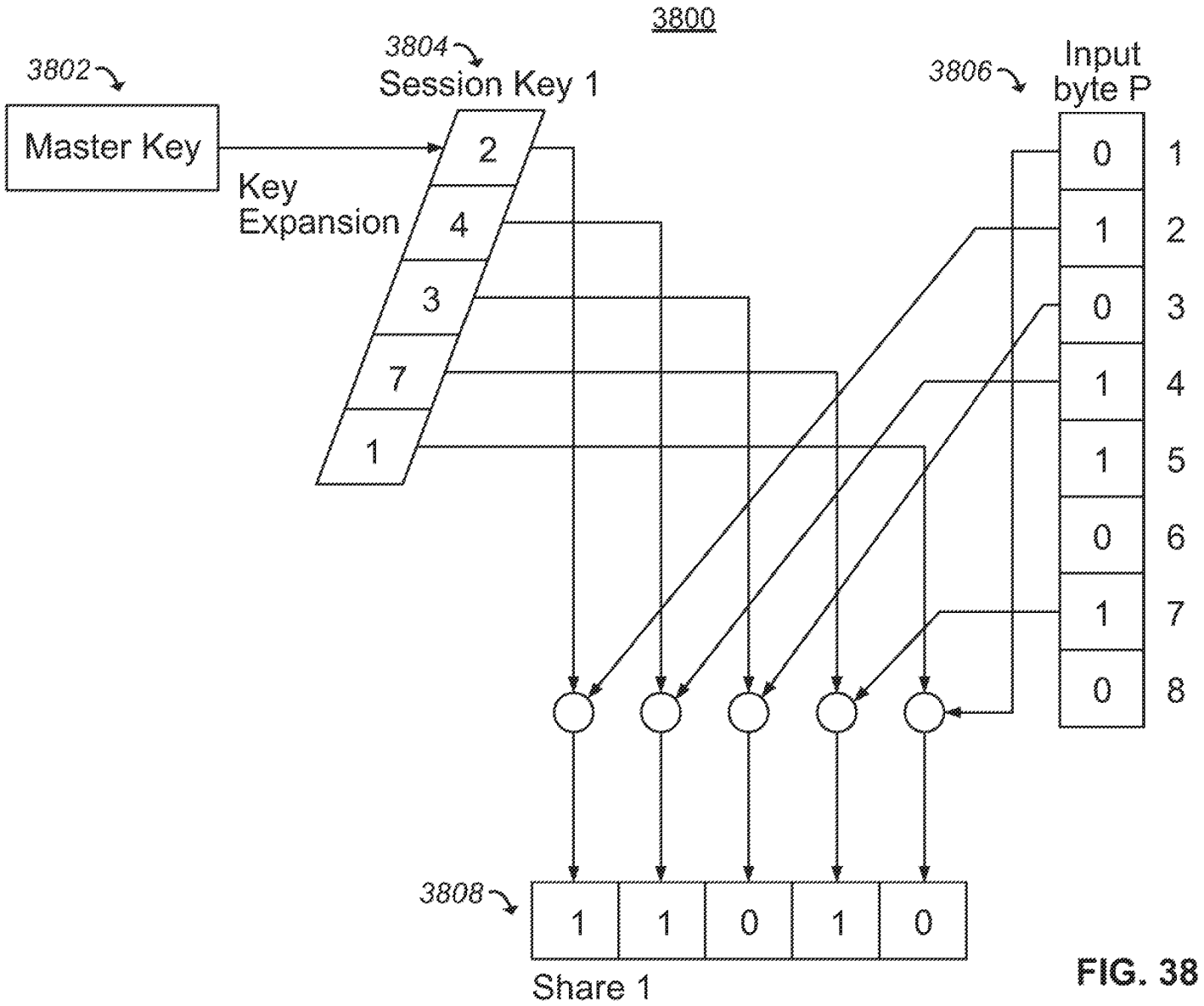


FIG. 38

EX1002 - Page 493

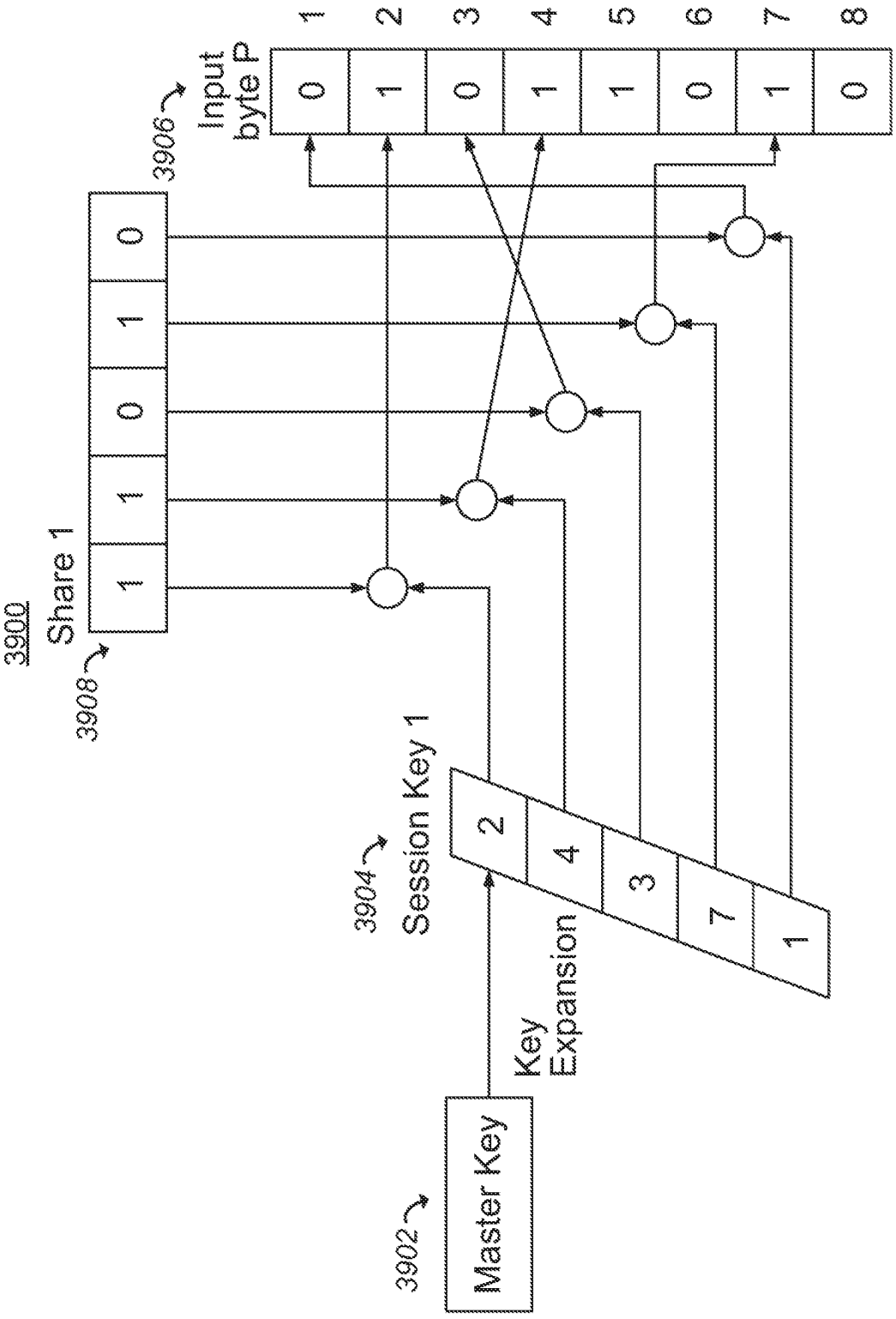

3900
Share 1
3908
1 1 0 1 0
3906
Input byte P
1 2 3 4 5 6 7 8
0 1 0 1 1 0 1 0
3904
Session Key 1
2 4 3 7 1
Key Expansion
3902
Master Key

FIG. 39

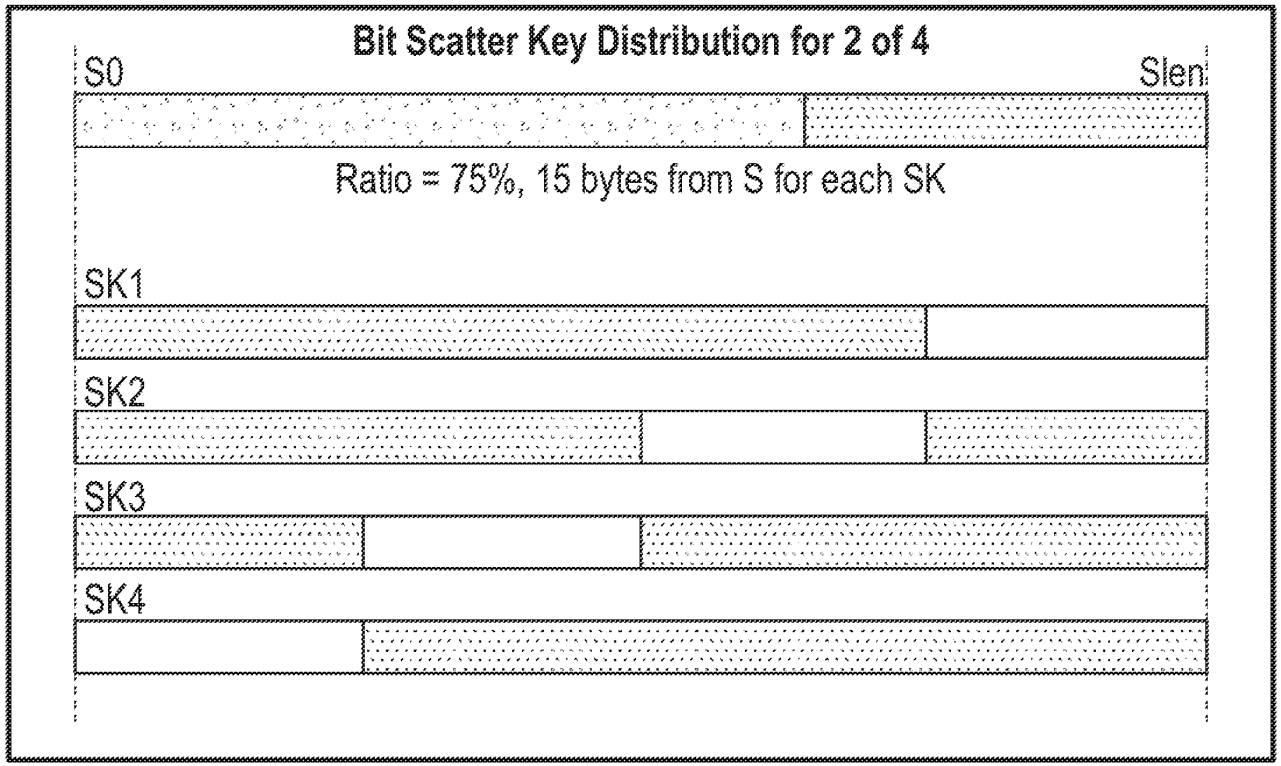


FIG. 40

EX1002 - Page 495

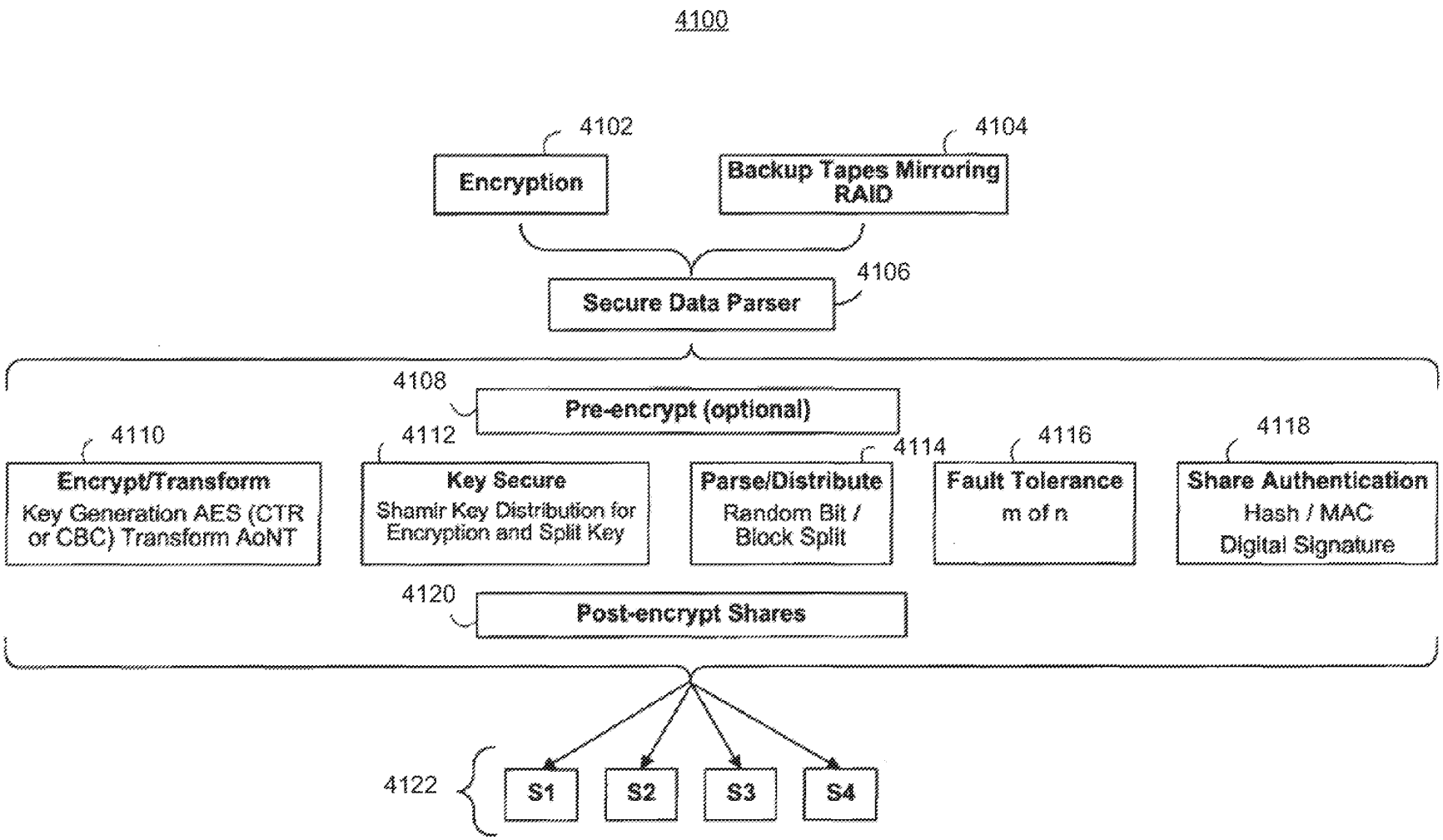

4100
4102
Encryption
4104
Backup Tapes Mirroring
RAID
4106
Secure Data Parser
4108
Pre-encrypt (optional)
4110
Encrypt/Transform
Key Generation AES (CTR or CBC) Transform AoNT
4112
Key Secure
Shamir Key Distribution for Encryption and Split Key
4114
Parse/Distribute
Random Bit / Block Split
4116
Fault Tolerance
m of n
4118
Share Authentication
Hash / MAC
Digital Signature
4120
Post-encrypt Shares
4122
S1
S2
S3
S4

FIG. 41

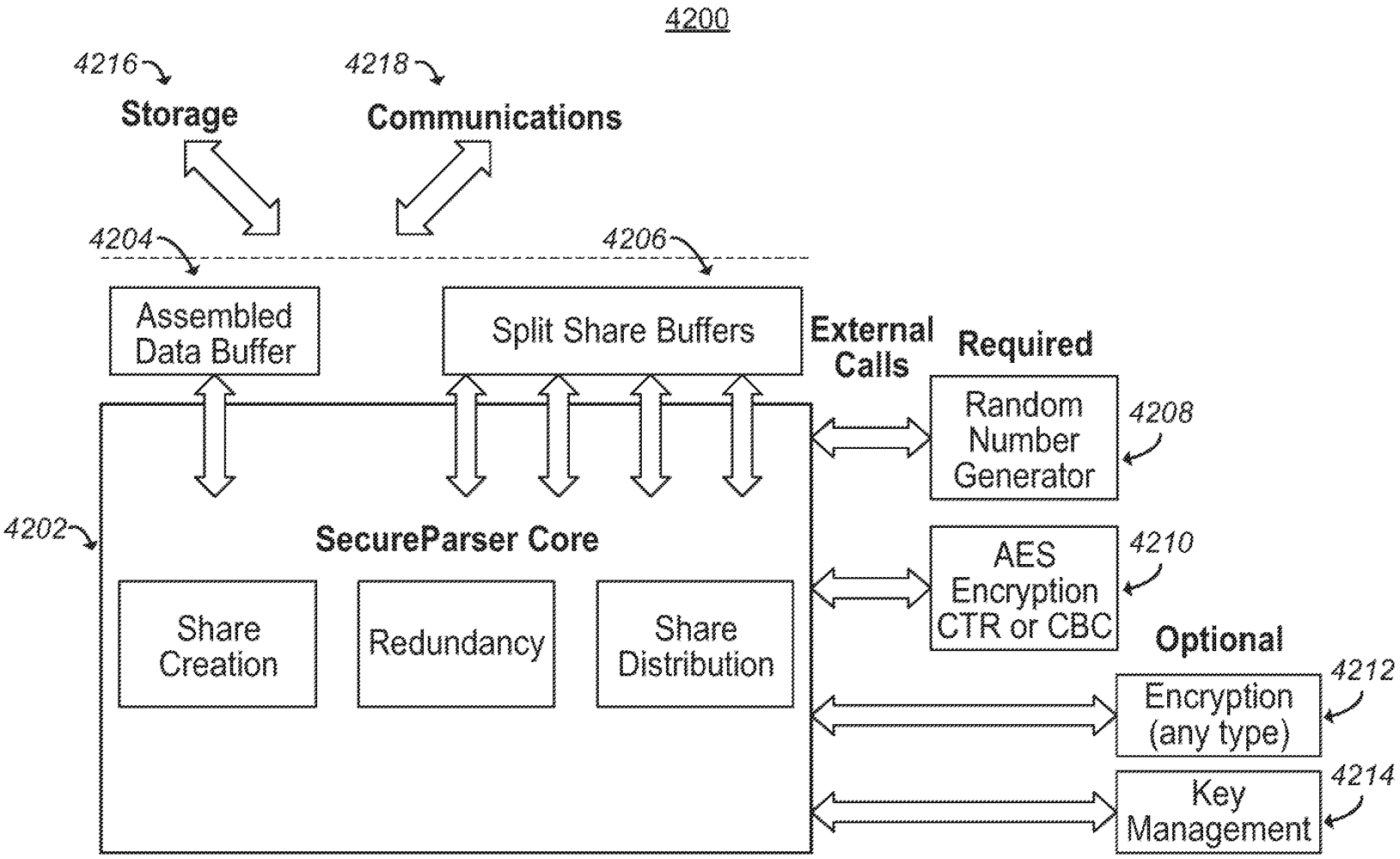

4200
4216
Storage
4218
Communications
4204
4206
Assembled Data Buffer
Split Share Buffers
External Calls
Required
Random Number Generator
4208
4202
SecureParser Core
AES Encryption CTR or CBC
4210
Share Creation
Redundancy
Share Distribution
Optional
Encryption (any type)
4212
Key Management
4214

FIG. 42

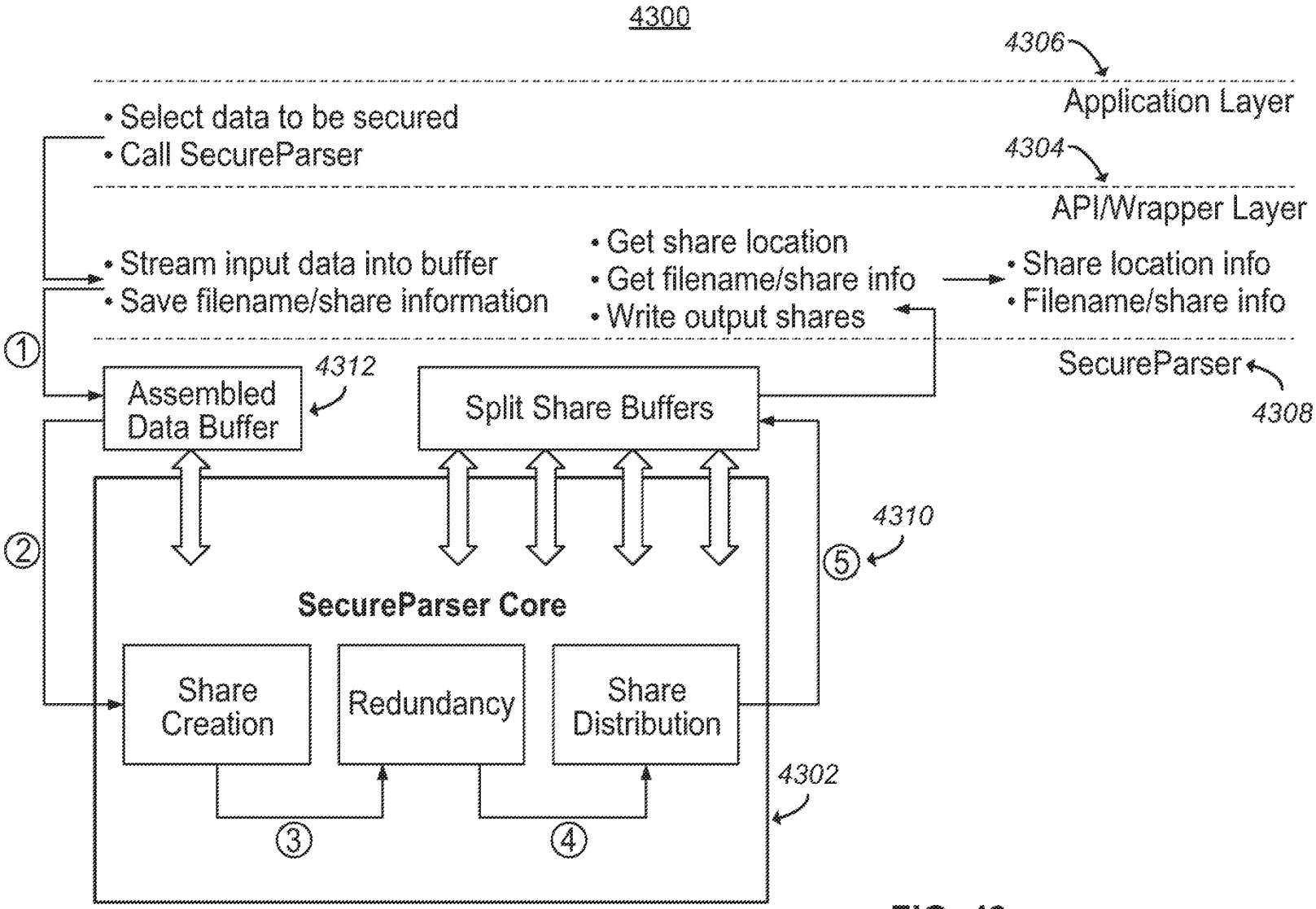


FIG. 43

EX1002 - Page 498

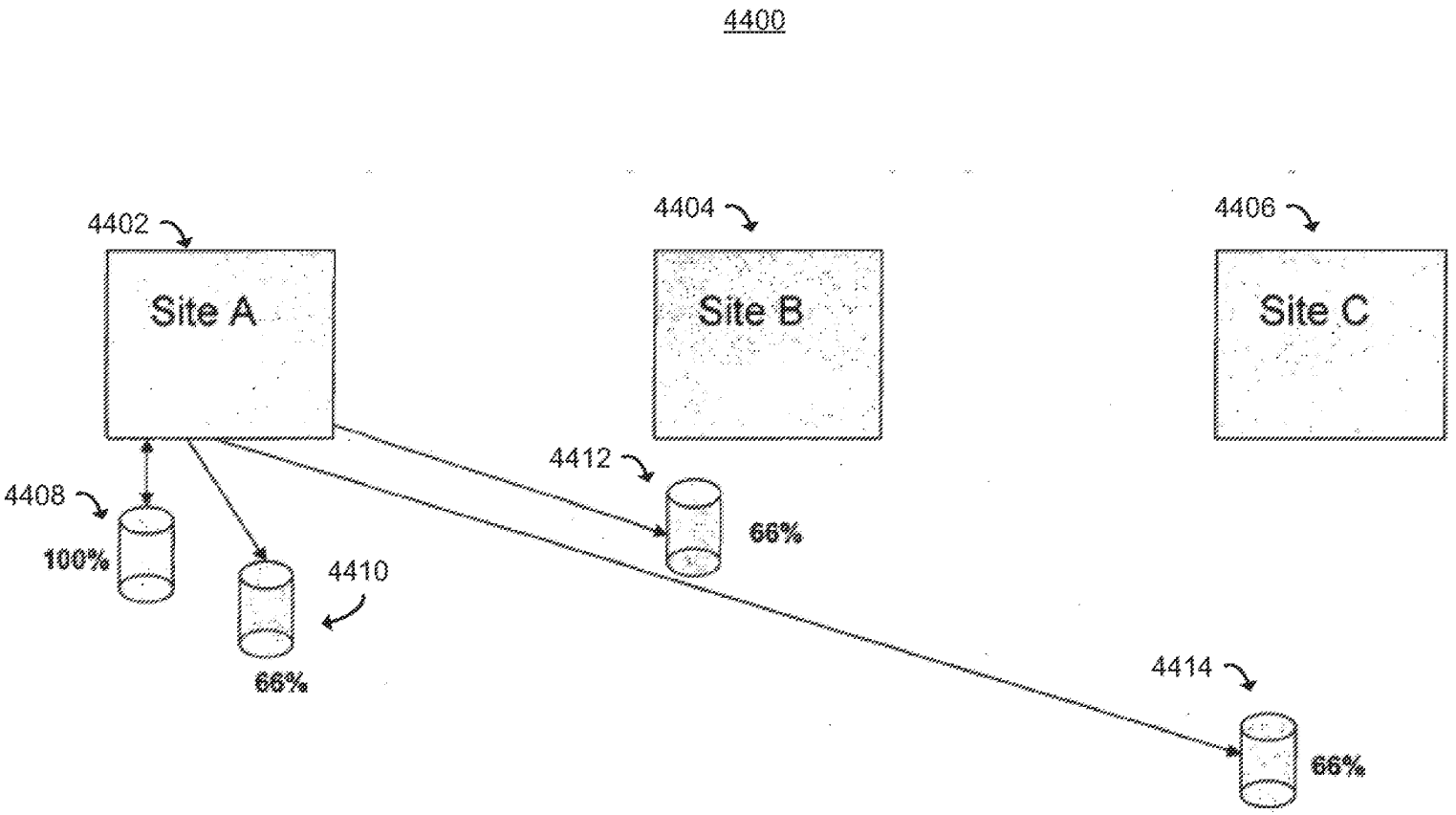

4400
4402
Site A
4404
Site B
4406
Site C
4408
100%
4410
66%
4412
66%
4414
66%

FIG. 44

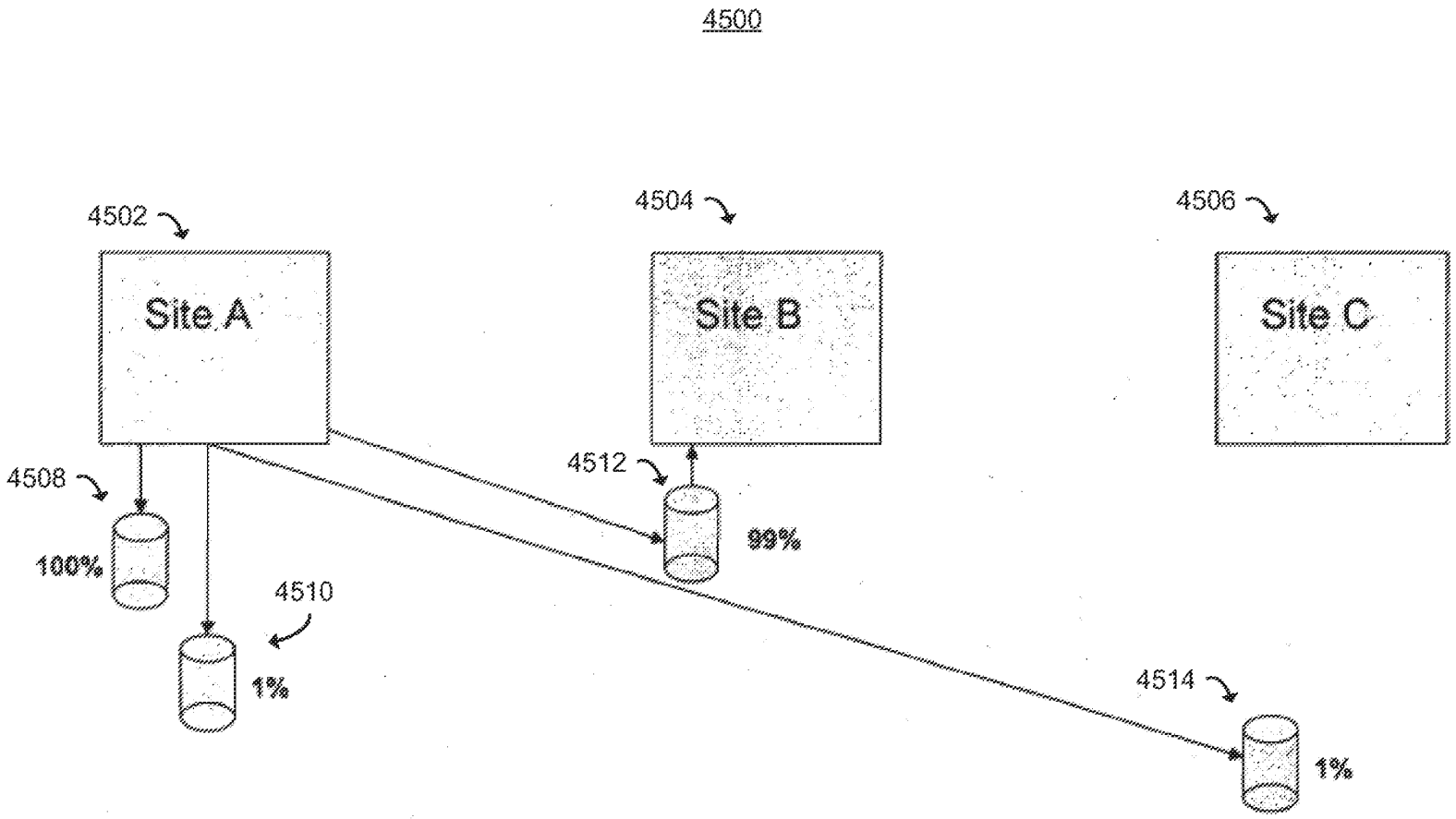

4500
4502
Site A
4504
Site B
4506
Site C
4508
100%
4510
1%
4512
99%
4514
1%

FIG. 45

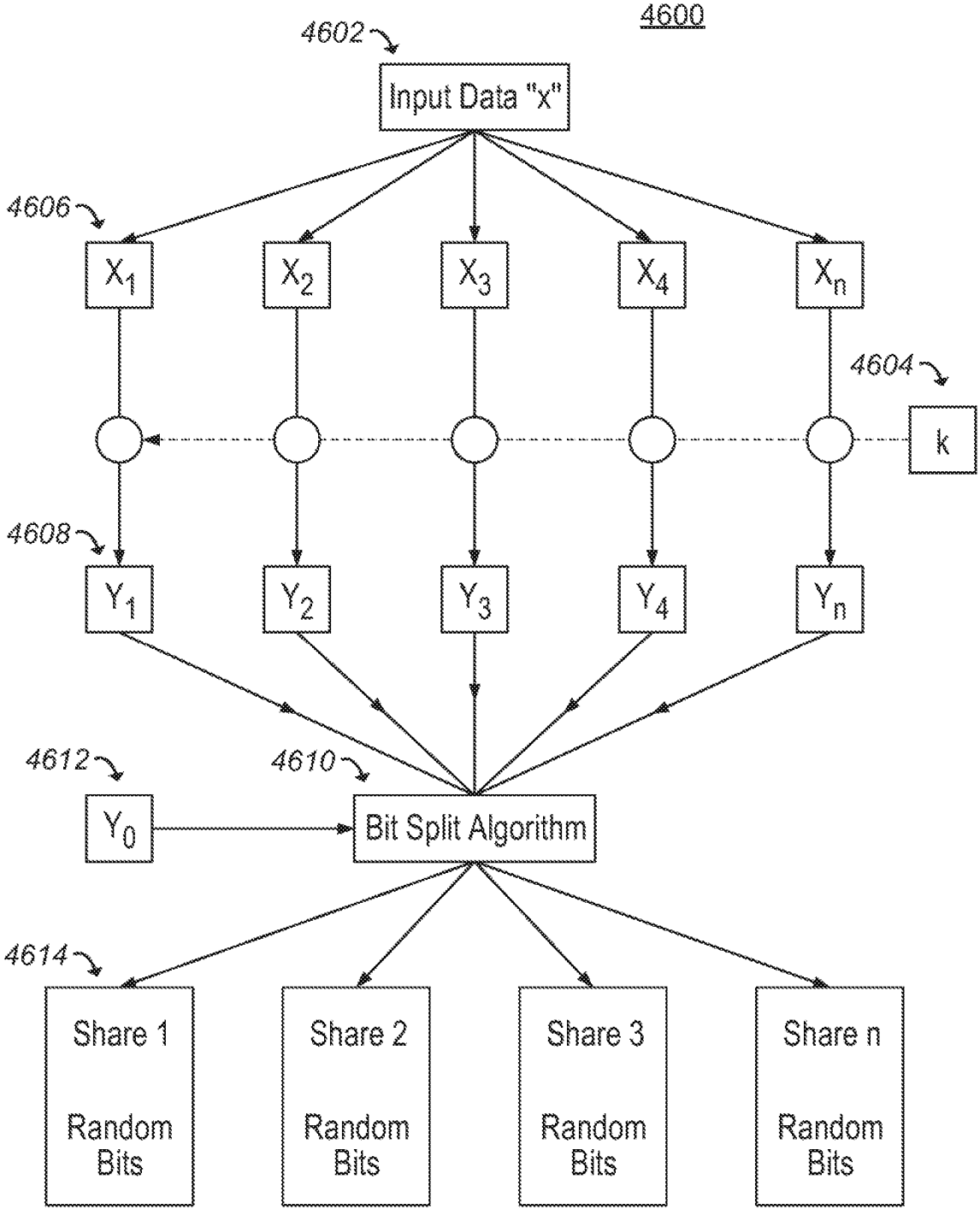

4600
4602
Input Data "x"
4606
X1
X2
X3
X4
Xn
4604
k
4608
Y1
Y2
Y3
Y4
Yn
4612
4610
Y0
Bit Split Algorithm
4614
Share 1
Random Bits
Share 2
Random Bits
Share 3
Random Bits
Share n
Random Bits

FIG. 46

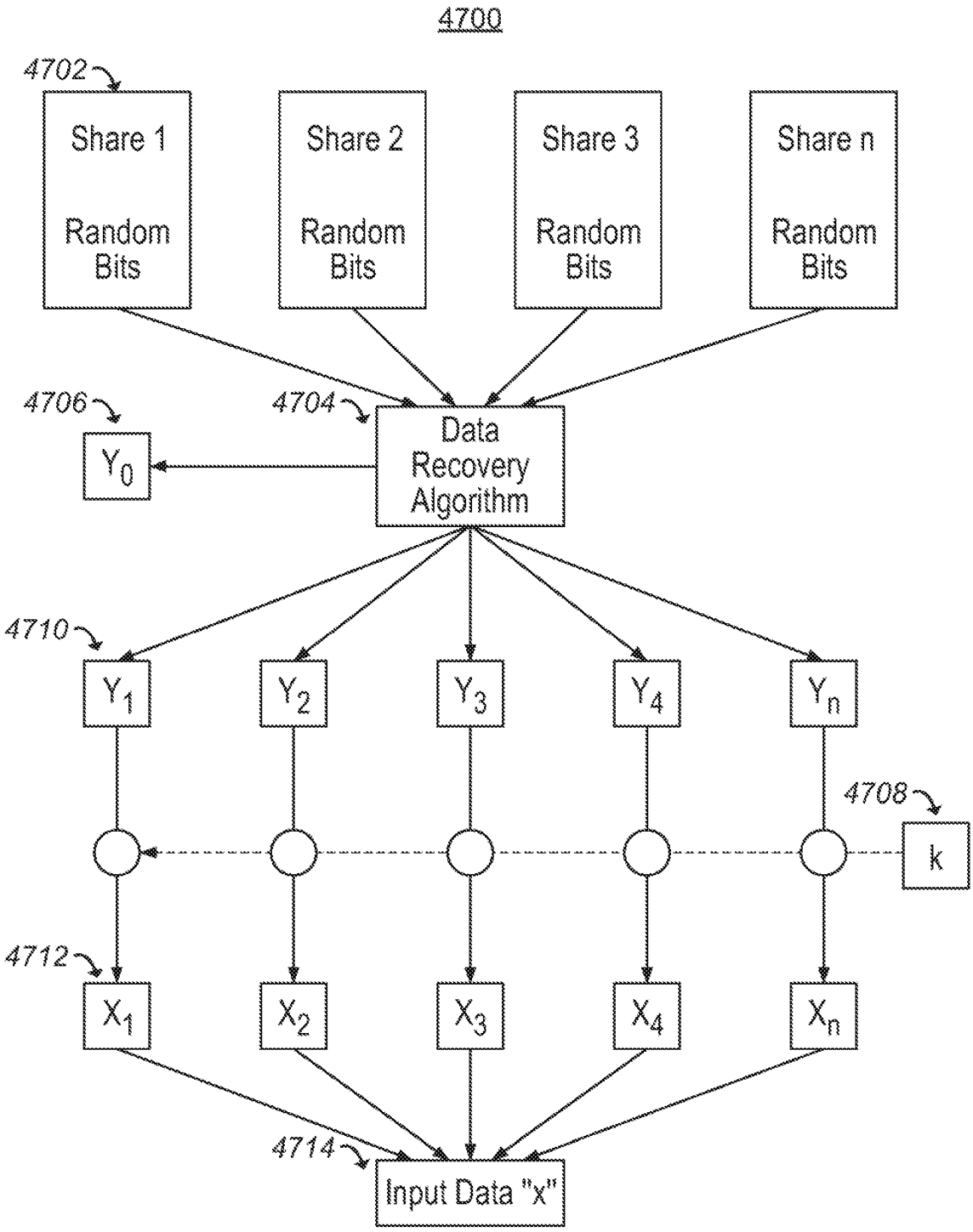

4700
4702
Share 1
Random Bits
Share 2
Random Bits
Share 3
Random Bits
Share n
Random Bits
4706
4704
Y_0
Data Recovery Algorithm
4710
Y_1
Y_2
Y_3
Y_4
Y_n
4708
k
4712
X_1
X_2
X_3
X_4
X_n
4714
Input Data "x"

FIG. 47

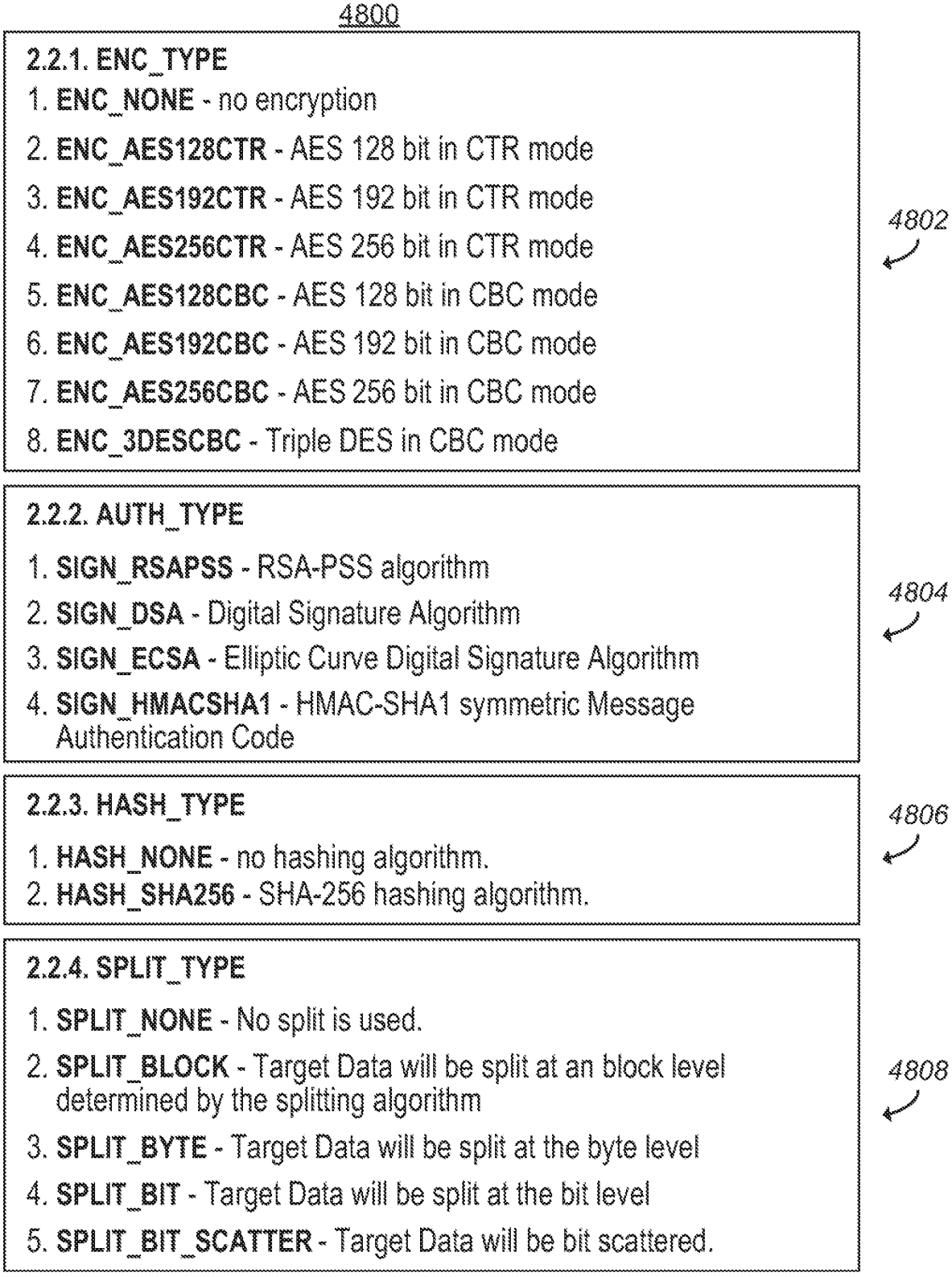


FIG. 48, Panel A

2.2.5. KEY_TYPE

1. **KEY_SYM** (keys for all symmetric algorithms)
2. **KEY_RSAPUB**
3. **KEY_RSAPRI**
4. **KEY_DSAPUB**
5. **KEY_DSAPRI**
6. **KEY_ECDSAPUB**
7. **KEY_ECDSAPRI**

4810

2.2.6. ERROR_TYPE

1. **ERROR_NONE** - No error
2. **ERROR_NO_MASTER_KEY** - No master key, can not continue.
3. **ERROR_INVALID_CALLBACK** - An invalid callback was registered
4. **ERROR_INVALID_METHOD** - An invalid parse split method occurred.
5. **ERROR_NO_TARGET** - No target was set to parse.
6. **ERROR_NO_TARGET_LENGTH** - Target buffer has no length
7. **ERROR_NOT_ENOUGH_SHARES** - Unable to restore, not enough shares are present.
8. **ERROR_INVALID_SHARE** - An invalid share was set
9. **ERROR_INVALID_KEY** - An invalid key was set
10. **ERROR_INTEGRITY_CHECK** - An integrity check failure occurred
11. **ERROR_NO_MEMORY** - Out of memory

4812

FIG. 48, Panel B

4900

4902

Name	Type	Description
originalShare	Share	stores the original unsplit data.
shares	Share []	an array of Share data structures of size MAX_SHARE_COUNT.
shareCount	int	actual number of shares used.
splitEncContext	EncContext *	buffer holding pre-encryption context between calls to doSplit and doRestore.
finalFlag	int	indicates that the final call to doSplit or doRestore will be made next (default = 0).

4904

Name	Type	Description
L	int	total number of mandatory shares (default = 0).
N	int	total number of non-mandatory shares (default = 0).
M	int	total number of non-mandatory shares needed for recovery (default = 0).
splitType	SPLIT_TYPE	the split algorithm to use (default = NONE).
splitEncMode	ENC_TYPE	the encryption mode to use during the split (default = NONE).
preEncMode	ENC_TYPE	the pre-encryption mode to use (default = NONE).
postEncMode	ENC_TYPE	the post-encryption mode to use (default = NONE).
splitHashMode	HASH_TYPE	the hash mode to use (default = HASH_SHA256).
preAuthMode	AUTH_TYPE	the pre-signing mode to use (default = NONE).
postAuthMode	AUTH_TYPE	the post-signing mode to use (default = NONE).
preEncKey	char *	handle for the pre-encryption key (default = NONE).
postEncKey	char *	handle for the post-encryption key (default = NONE).
preAuthKey	char *	handle for the pre-signature key (default = NONE).
postAuthKey	char *	handle for the post-signature key (default = NONE).
maxOrigBufSize	int	max size for the original buffer (default = MAX_ ORIG_BUF_SIZE).
maxShareBufSize	int	max size for each share buffer (default = MAX_ SHARE_BUF_SIZE).

FIG. 49, Panel A

4906

Name	Type	Description
id	char *	unique identifier for this key.
idLen	int	length of buffer holding id.

4908

Name	Type	Description
data	uint8 *	key share data for this share.
dataLen	int	length of data (in bits) of data buffer.

4910

Name	Type	Description
keyId	KeyId	unique identifier for this key.
type	KEY_TYPE	type of key that this.
data	uint8 *	pointer to the buffer holding the key data.
dataLen	int	length of the buffer holding the key data.

4912

Name	Type	Description
data	uint8 *	data buffer for this share.
dataLen	int	length indicating the amount of data found in this share.
encContext	EncContext	data buffer storing the encryption context between calls to doSplit and doRestore.
authContext	SigContext	data buffer storing the authentication context between calls to doSplit and doRestore.
hashContext	HashContext	data buffer storing the hash context between calls to doSplit and doRestore.

FIG. 49, Panel B

5002 ↘ 5000

Name	Type	Description
encMode	ENC_TYPE	the type of encryption being used.
...	Union	various types of encryption contexts can be placed here.

5004 ↘

Name	Type	Description
encKeyId	KeyId	unique identifier of the encryption key to use for this context.
currentIV	uint8 *	the current IV being stored for this context.
currentIdLen	int	the length of the current IV in bytes.

5006 ↘

Name	Type	Description
encKeyId	KeyId	unique identifier of the encryption key to use for this context.
currentIV	uint8 *	the current IV being stored for this context.
currentIVLen	int	the length of the current IV in bytes.

5008 ↘

Name	Type	Description
authMode	AUTH_TYPE	the type of authentication being used.
...	Union	various types of authentication contexts can be placed here.

5020 ↘

Name	Type	Description
hashContext	openSSL?	Pointer to the OpenSSL hash context data type.

FIG. 50, Panel A

5010

Name	Type	Description
pubKeyId	KeyId	unique identifier of the public key to use for this context.
privKeyId	KeyId	unique identifier of the private key to use for this context.
hashContext	openSSL?	Pointer to the OpenSSL hash context data type.

5012

Name	Type	Description
pubKeyId	KeyId	unique identifier of the public key to use for this context.
privKeyId	KeyId	unique identifier of the private key to use for this context.
hashContext	openSSL?	Pointer to the OpenSSL hash context data type.

5014

Name	Type	Description
pubKeyId	KeyId	unique identifier of the public key to use for this context.
privKeyId	KeyId	unique identifier of the private key to use for this context.
hashContext	openSSL?	Pointer to the OpenSSL hash context data type.

5016

Name	Type	Description
macContext	openSSL?	Pointer to the OpenSSL mac context data type.

5018

Name	Type	Description
hashMode	HASH_TYPE	the type of hashing being used.
...	Union	various types of hashing contexts can be placed here.

FIG. 50, Panel B

5100

Share Data
\n----- BEGIN POST-ENC KEY ID -----\n
post-encryption key id
\n----- END POST-ENC KEY ID -----\n
\n----- BEGIN POST-SIG KEY ID -----\n
post-signature key id
\n----- END POST-SIG KEY ID -----\n
\n----- BEGIN POST-ENC HEADER -----\n
post-encrypted header
\n----- END POST-ENC HEADER -----\n
\n----- BEGIN POST-ENC DATA -----\n
post-encrypted data
\n----- END POST-ENC DATA-----\n
\n----- BEGIN POST-ENC FOOTER -----\n
post-encrypted footer
\n----- END POST-ENC FOOTER -----\n
\n----- BEGIN POST-SIG DATA -----\n
post-signature data
\n----- END POST-SIG DATA-----\n

5102

Encrypted footer
\n----- BEGIN SPLIT-HASH DATA -----\n
split-hash data
\n----- END SPLIT-HASH DATA -----\n
\n----- BEGIN PRE-SIG DATA -----\n
pre-signature data
\n----- END PRE-SIG DATA -----\n

5108

FIG. 51, Panel A

Post-encrypted footer
\n----- BEGIN ENCRYPTED FOOTER -----\n
encrypted footer
\n----- END ENCRYPTED FOOTER -----\n

5104

Post-encrypted header
\n----- BEGIN HEADER -----\n
Key share (len):key share information\n
Share id (2):share ID\n
L (2):L\n
M (2):M\n
N (2):N\n
Split mode (1):split mode\n
Split-encryption key (len):split-encryption key id\n
Split-encryption IV (len):split-encryption IV data\n
Split-hash mode (1):split-hash mode\n
Original buffer (4):original buffer size\n
Share buffers (4):share buffer size\n
Pre-encryption key (len):pre-encryption key id\n
Pre-signature key (len):pre-signature key id\n
\n----- END HEADER -----\n

5106

FIG. 51, Panel B

5200

parser_createParser
Parameters none
Returns Parser *p
Description Allocates the SecureParser context, and sets default values.

5202

parser_destroyParser
Parameters Parser *p
Returns void
Description Destroys the SecureParser context, including parser parameter objects and share buffers.

5204

parser_createKey
Parameters char *id
uint8 *data
size_t length
KEYTYPE type
Returns Key *k
Description Constructs the structure **k** for use with the parser from the unique id, key data buffer, length indicater and key type given.

5206

parser_destroyKey
Parameters Key *k
Returns *none*
Description Destroys the key pointed to by k. Note: Do not destroy a key currently in use with the Parser.

5208

parser_createShare
Parameters int length
Key *encKey
Key *authKey
HASH_MODE h
Returns Share *s
Description Constructs a Share data structure based on the given length, the encryption key type, authentication key type and hash mode.

5210

FIG. 52A, Panel A

parser_destroyShare
Parameters Share *s
Returns none
Description Destroys the share pointed to by s, including all encryption and authentication keys.

5212

parser_initParameters
Parameters ParserParams *params
Returns int error
Description Initializes a ParserParams data structure to the default parameter set. The return error should be 0 for success, and non-zero error message for failure.

5214

parser_setParameters
Parameters Parser *p, ParserParams *params
Returns int error
Description Deletes any old ParserParams that may have already been added to the Parser struct. Creates a copy of the new ParserParams pointed to by params for internal use and stores in the Parser pointed to by p. If params is altered or destroyed by the user, Parser p will still have retained a copy for itself that is not affected. Any data structures that must be created by the parameters struct, such as Shares or Keys will be created. The Parser will destroy the params object itself upon being closed.

5216

parser_setFinalize
Parameters Parser *p
Returns none
Description Sets the internal state of the Parser to finalize the output stream during the next SecureParser split session. After setFinalize is called, only one more call to doSessionSplit may be made.

5218

parser_getOriginalShare
Parameters Parser *p
Returns Share *s
Description Returns a Share structure representing the original buffer used by the Parser.

5220

FIG. 52A, Panel B

5200

parser_getShare
Parameters Parser *p,
int ShareID
Returns Share *s
Description Returns a Share containing the Share structure for the Share matching the given ShareID.

5222

parser_doSplit
Parameters Parser *p
Returns int error
Description Performs the SecureParser split. This action treats data that is in the target buffer as input and places split data that is output into buffers for each Share. A return value of 0 indicates success, otherwise a failure has occurred and the error is returned. If setFinalize has been called, this must be the last

5224

parser_doRestore
Parameters Parser *p
Returns int error
Description Performs the SecureParser restore. This action treats all data in share buffers as input and places output data (the reconstructed original data) into the target buffer. A return value of 0 indicates success, otherwise a failure has occured and the error is returned.

5226

parser_generateHeaders
Parameters Parser *p
Returns int error
Description Generates the necessary header information based on the parser's current parameter set and state, and puts this header information appropriately within each Share buffer.

5228

parser_generateFooters
Parameters Parser *p
Returns int error
Description Generates the necessary footer information based on the parser's current parameter set and state, and puts this footer information appropriately within each Share buffer.

5230

FIG. 52B, Panel A

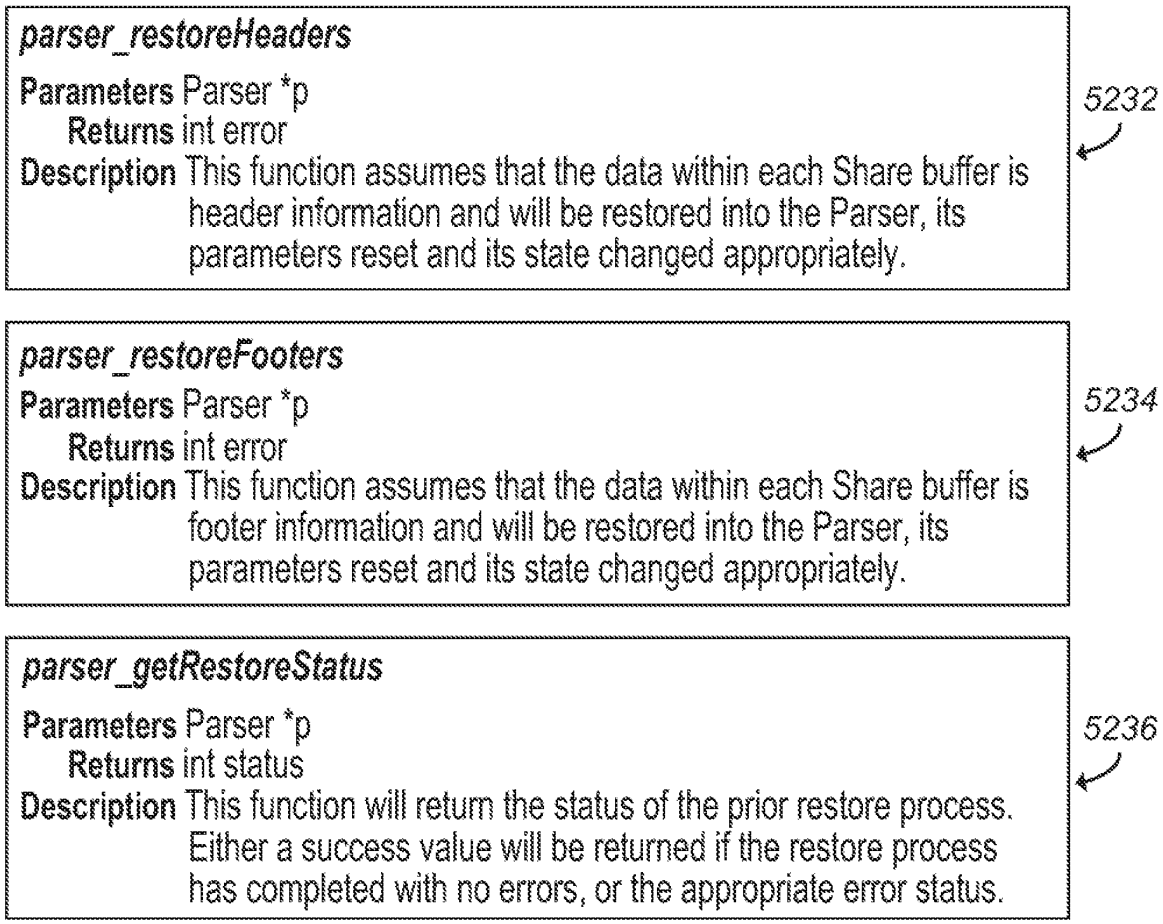


FIG. 52B, Panel B

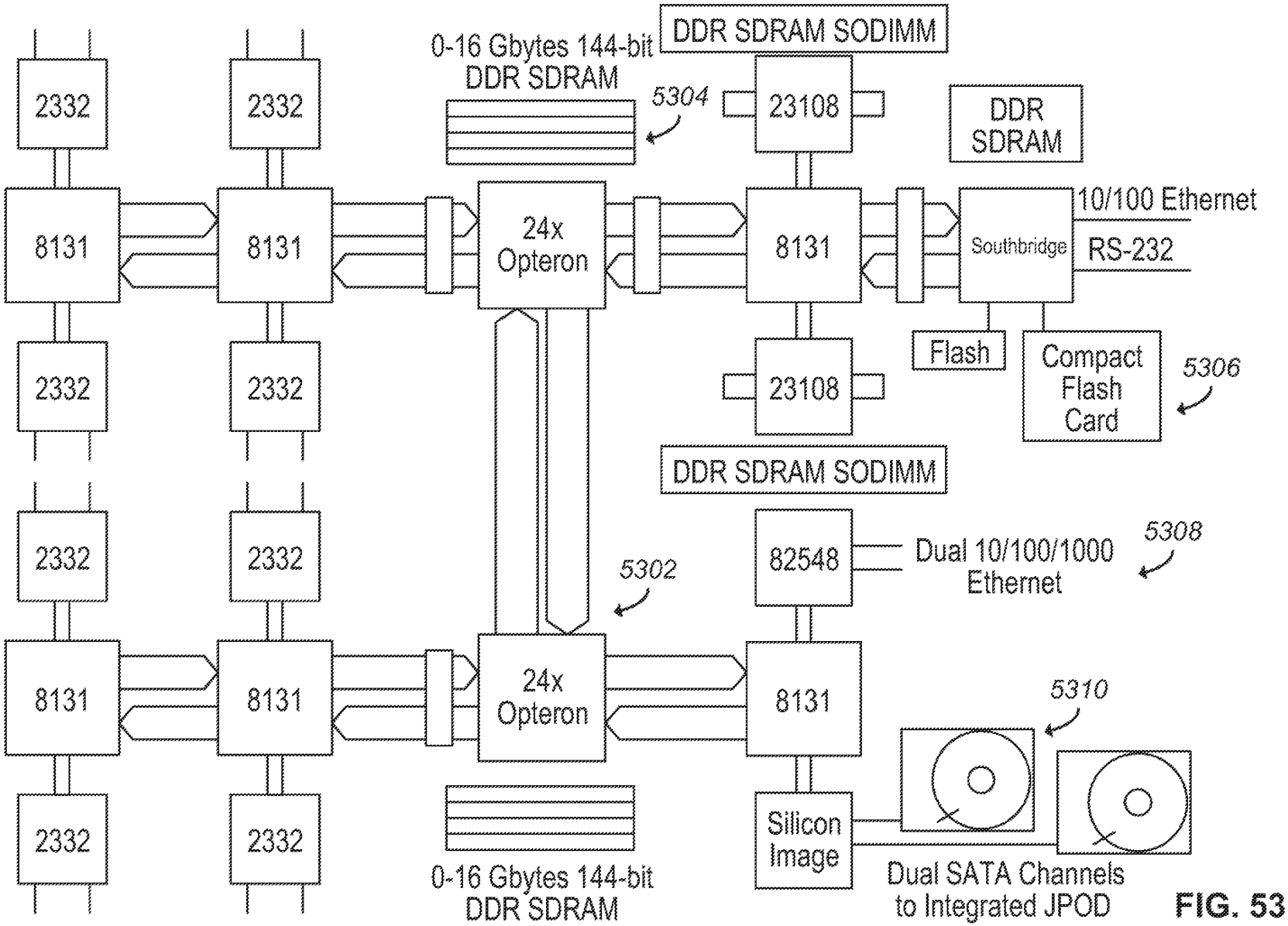

0-16 Gbytes 144-bit DDR SDRAM
DDR SDRAM SODIMM
5304
23108
DDR SDRAM
2332
8131
24x Opteron
Southbridge
10/100 Ethernet
RS-232
Flash
Compact Flash Card
5306
DDR SDRAM SODIMM
82548
Dual 10/100/1000 Ethernet
5308
5302
5310
Silicon Image
Dual SATA Channels to Integrated JPOD
0-16 Gbytes 144-bit DDR SDRAM

FIG. 53

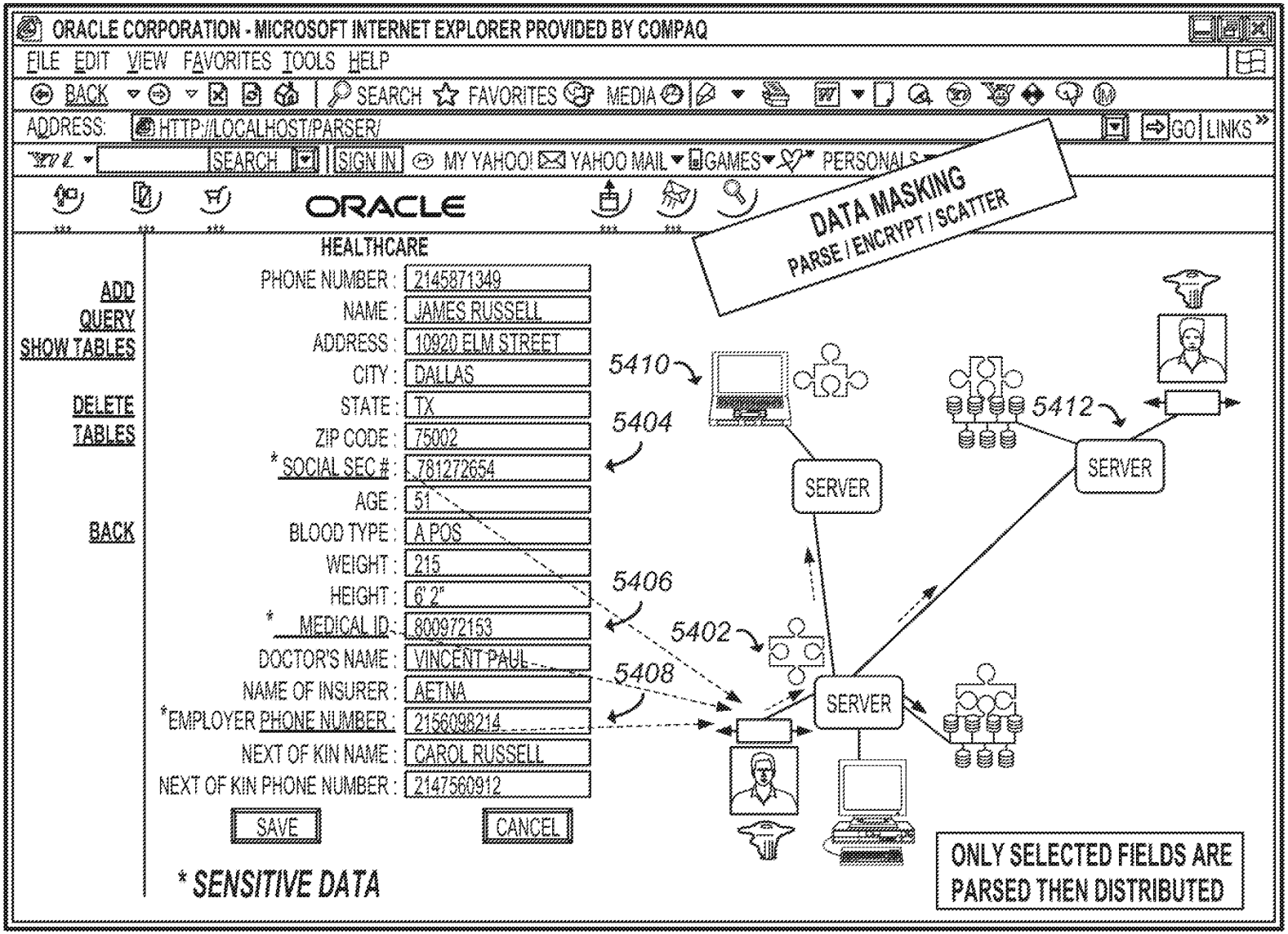

ORACLE CORPORATION - MICROSOFT INTERNET EXPLORER PROVIDED BY COMPAQ
FILE EDIT VIEW FAVORITES TOOLS HELP
BACK SEARCH FAVORITES MEDIA
ADDRESS: HTTP://LOCALHOST/PARSER/
GO LINKS
SEARCH SIGN IN MY YAHOO! YAHOO MAIL GAMES PERSONALS
ORACLE
DATA MASKING
PARSE / ENCRYPT / SCATTER
HEALTHCARE
ADD
QUERY
SHOW TABLES
DELETE
TABLES
BACK
PHONE NUMBER : 2145871349
NAME : JAMES RUSSELL
ADDRESS : 10920 ELM STREET
CITY : DALLAS
STATE : TX
ZIP CODE : 75002
* SOCIAL SEC # : 781272654
AGE : 51
BLOOD TYPE : A POS
WEIGHT : 215
HEIGHT : 6' 2"
* MEDICAL ID : 800972153
DOCTOR'S NAME : VINCENT PAUL
NAME OF INSURER : AETNA
*EMPLOYER PHONE NUMBER : 2156098214
NEXT OF KIN NAME : CAROL RUSSELL
NEXT OF KIN PHONE NUMBER : 2147560912
SAVE
CANCEL
* SENSITIVE DATA
5410
5404
5406
5408
5402
5412
SERVER
SERVER
SERVER
ONLY SELECTED FIELDS ARE PARSED THEN DISTRIBUTED

FIG. 54

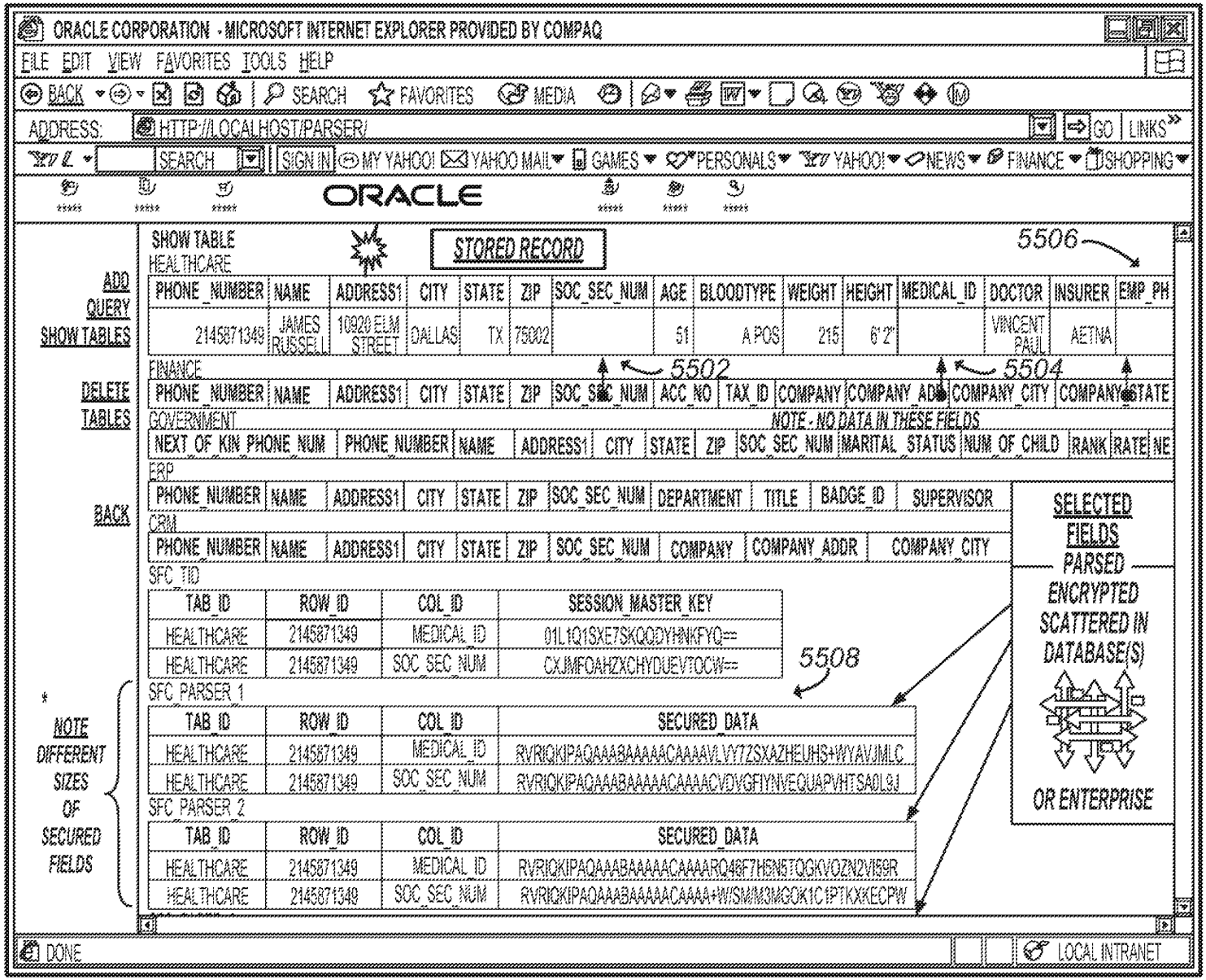

ORACLE CORPORATION - MICROSOFT INTERNET EXPLORER PROVIDED BY COMPAQ
FILE EDIT VIEW FAVORITES TOOLS HELP
BACK SEARCH FAVORITES MEDIA
ADDRESS: HTTP://LOCALHOST/PARSER/
GO LINKS
SEARCH SIGN IN MY YAHOO! YAHOO MAIL GAMES PERSONALS YAHOO! NEWS FINANCE SHOPPING
ORACLE
SHOW TABLE
HEALTHCARE
STORED RECORD
5506
ADD
QUERY
SHOW TABLES
DELETE
TABLES
BACK
PHONE_NUMBER | NAME | ADDRESS1 | CITY | STATE | ZIP | SOC_SEC_NUM | AGE | BLOODTYPE | WEIGHT | HEIGHT | MEDICAL_ID | DOCTOR | INSURER | EMP_PH
2145871349 | JAMES RUSSELL | 10920 ELM STREET | DALLAS | TX | 75002 | | 51 | A POS | 215 | 6'2" | | VINCENT PAUL | AETNA |
FINANCE
5502
5504
PHONE_NUMBER | NAME | ADDRESS1 | CITY | STATE | ZIP | SOC_SEC_NUM | ACC_NO | TAX_ID | COMPANY | COMPANY_ADDR | COMPANY_CITY | COMPANY_STATE
GOVERNMENT
NOTE - NO DATA IN THESE FIELDS
NEXT_OF_KIN_PHONE_NUM | PHONE_NUMBER | NAME | ADDRESS1 | CITY | STATE | ZIP | SOC_SEC_NUM | MARITAL_STATUS | NUM_OF_CHILD | RANK | RATE | NE
ERP
PHONE_NUMBER | NAME | ADDRESS1 | CITY | STATE | ZIP | SOC_SEC_NUM | DEPARTMENT | TITLE | BADGE_ID | SUPERVISOR
CRM
PHONE_NUMBER | NAME | ADDRESS1 | CITY | STATE | ZIP | SOC_SEC_NUM | COMPANY | COMPANY_ADDR | COMPANY_CITY
SFC_TID
TAB_ID | ROW_ID | COL_ID | SESSION_MASTER_KEY
HEALTHCARE | 2145871349 | MEDICAL_ID | 01L1Q1SXE7SKQODYHNKFYQ==
HEALTHCARE | 2145871349 | SOC_SEC_NUM | CXJMFOAHZXCHYDUEVTOOW==
5508
SFC_PARSER_1
TAB_ID | ROW_ID | COL_ID | SECURED_DATA
HEALTHCARE | 2145871349 | MEDICAL_ID | RVRIQKIPAQAAABAAAAACAAAAVLVYTZSXAZHEUHS+WYAVJMLC
HEALTHCARE | 2145871349 | SOC_SEC_NUM | RVRIQKIPAQAAABAAAAACAAAACVDVGFIYNVEQUAPVHTSA0L8J
SFC_PARSER_2
TAB_ID | ROW_ID | COL_ID | SECURED_DATA
HEALTHCARE | 2145871349 | MEDICAL_ID | RVRIQKIPAQAAABAAAAACAAAARQ4RFTH8NETOGKVOZN2VI59R
HEALTHCARE | 2145871349 | SOC_SEC_NUM | RVRIQKIPAQAAABAAAAACAAAA+W/SM/M3MGOK1C1PTKXXECPW
* NOTE DIFFERENT SIZES OF SECURED FIELDS
SELECTED FIELDS PARSED
ENCRYPTED SCATTERED IN DATABASE(S)
OR ENTERPRISE
DONE
LOCAL INTRANET

FIG. 55

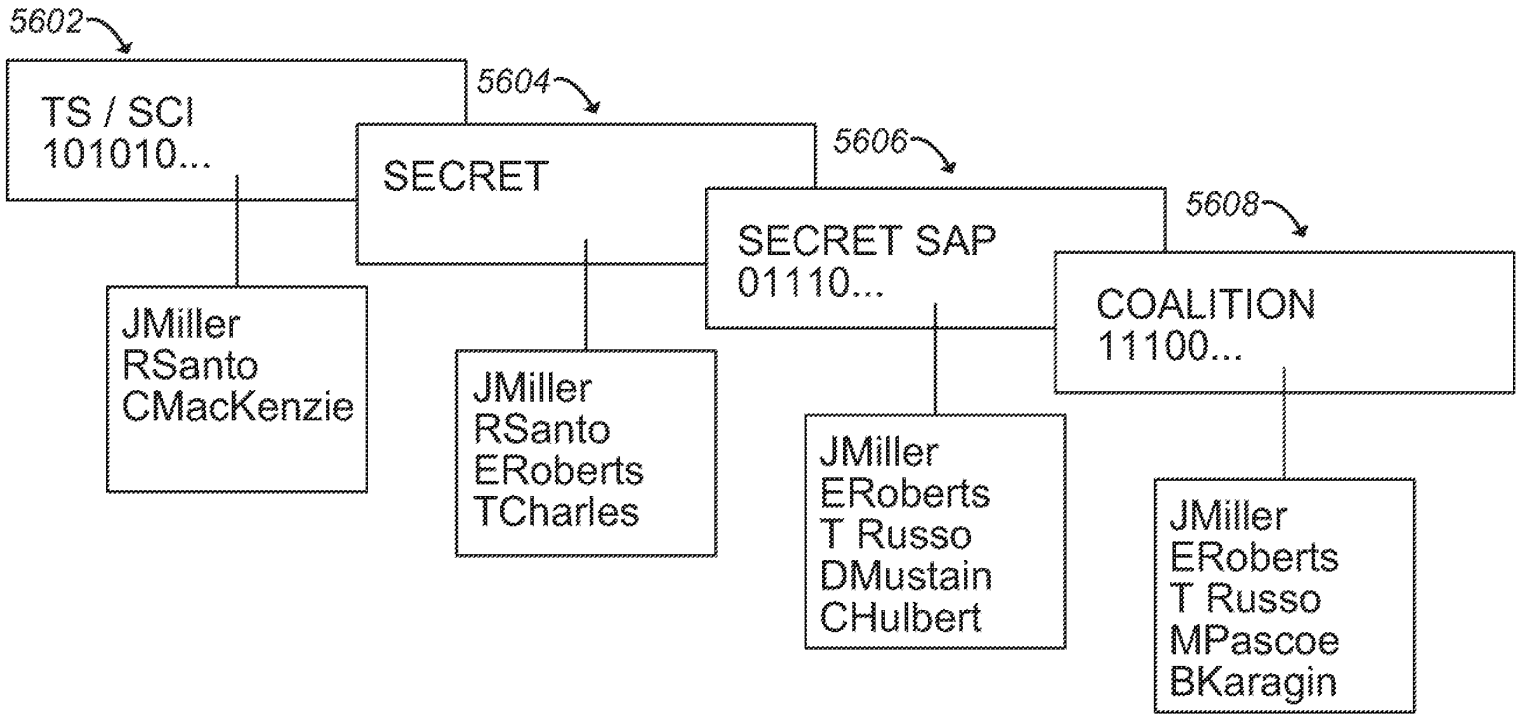


FIG. 56

EX1002 - Page 518

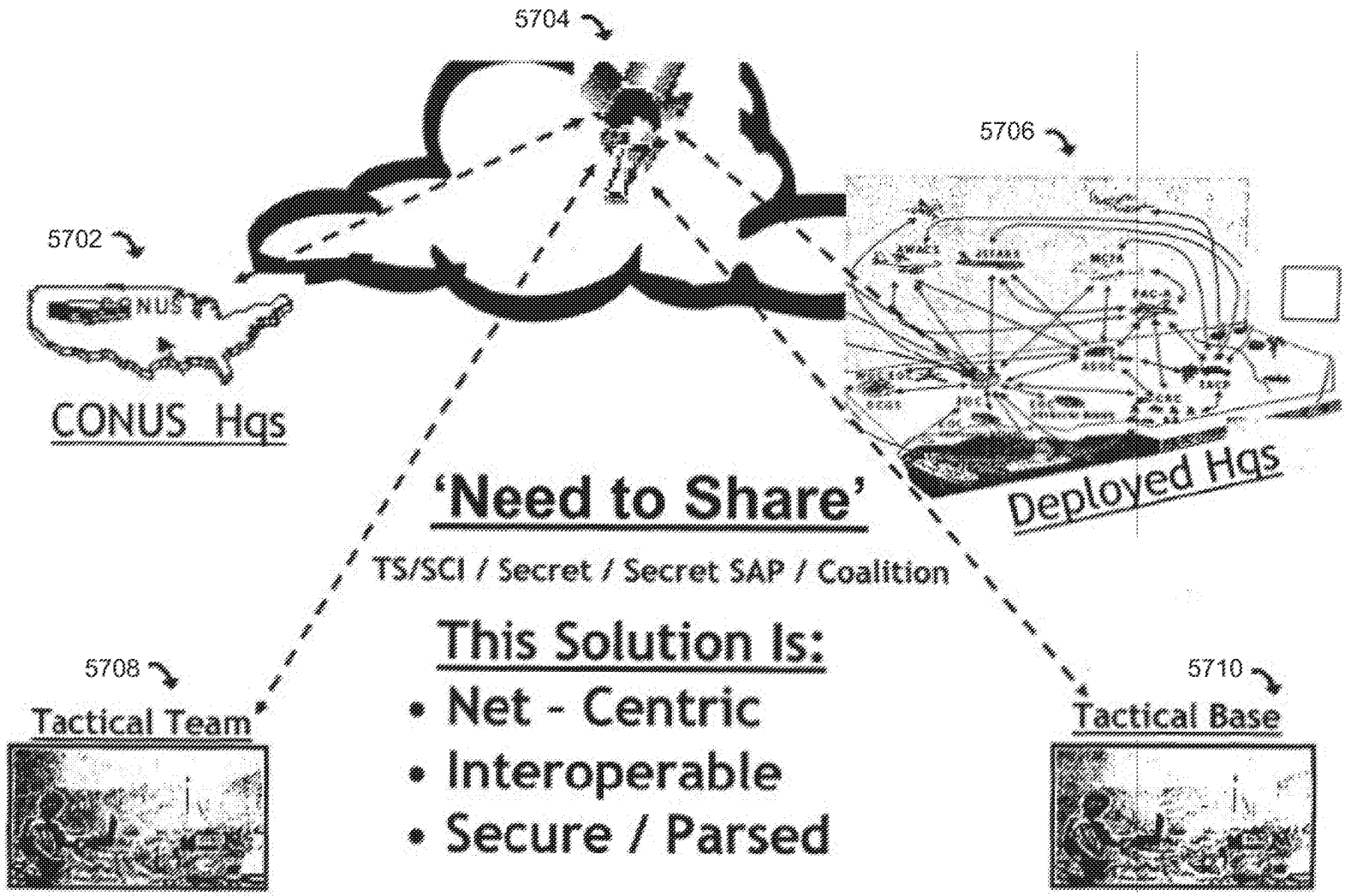


FIG. 57

EX1002 - Page 519

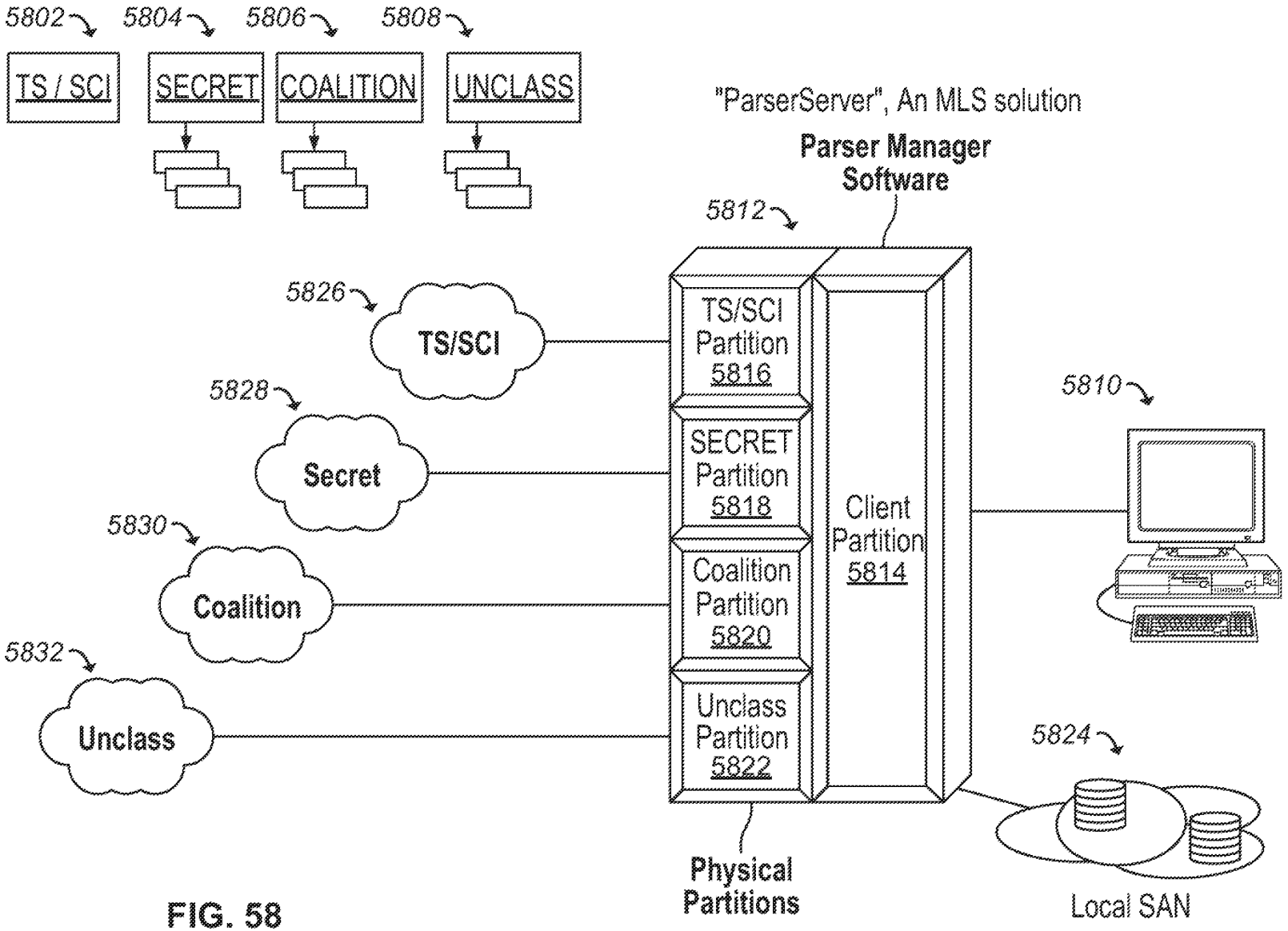


FIG. 58

EX1002 - Page 520

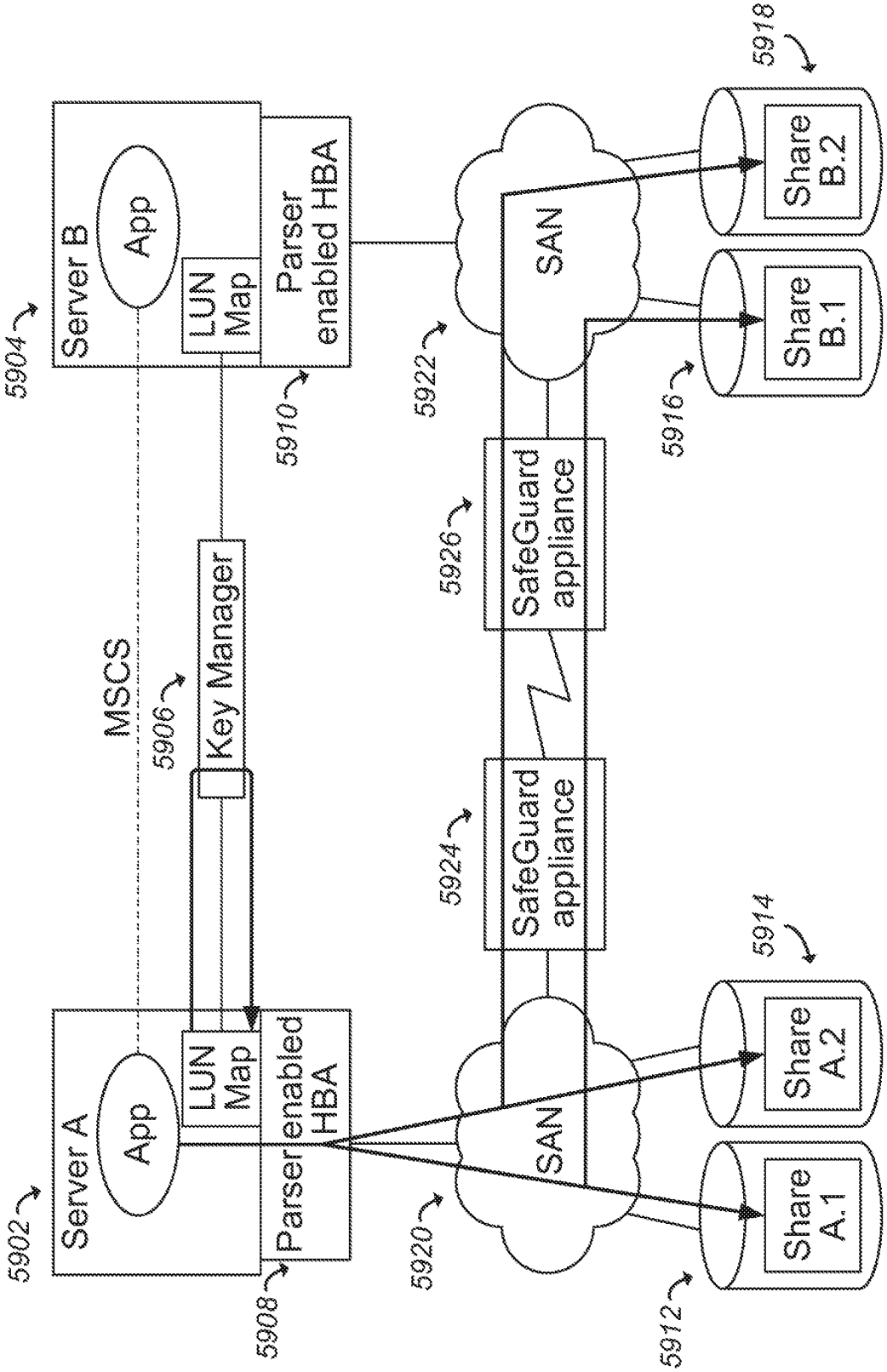

Server A
App
LUN Map
Parser enabled HBA
Server B
App
LUN Map
Parser enabled HBA
MSCS
Key Manager
SAN
SAN
SafeGuard appliance
SafeGuard appliance
Share A.1
Share A.2
Share B.1
Share B.2
5902
5904
5906
5908
5910
5912
5914
5916
5918
5920
5922
5924
5926

FIG. 59

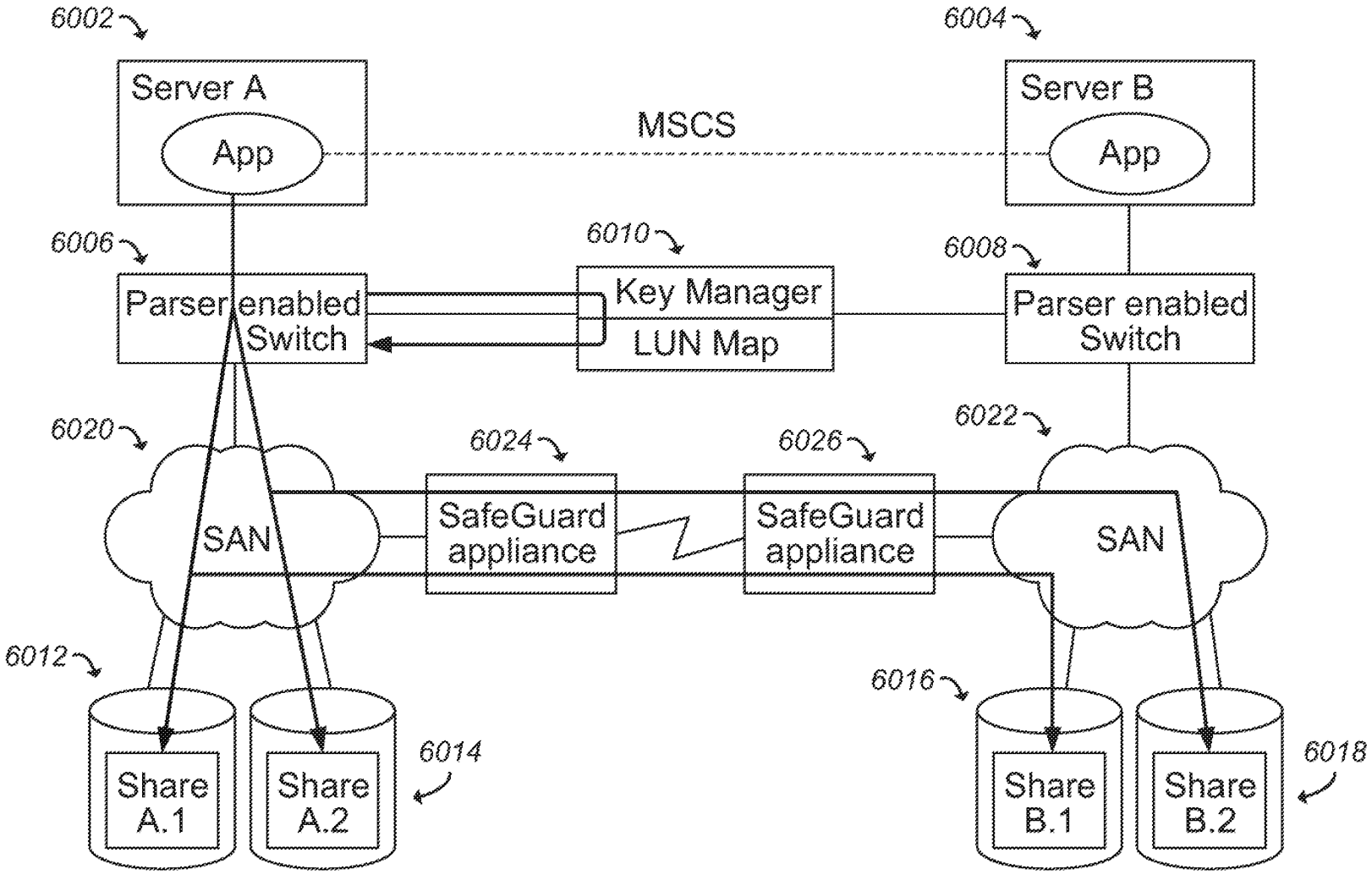


FIG. 60

EX1002 - Page 522

Electronic Acknowledgement Receipt

EFS ID:	32602619
Application Number:	15977748
International Application Number:	
Confirmation Number:	7200
Title of Invention:	SECURE DATA PARSER METHOD AND SYSTEM
First Named Inventor/Applicant Name:	Mark S. O'Hare
Customer Number:	15314
Filer:	Maxim Rapoport/Juanita Alvarez
Filer Authorized By:	Maxim Rapoport
Attorney Docket Number:	104093-0002-118
Receipt Date:	11-MAY-2018
Filing Date:	
Time Stamp:	17:01:59
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	104093_0002_118_ADS.pdf	1352958 7781604c62298326b249d201acd450bdca6e92f2	no	10

Warnings:

Information:					
2	Oath or Declaration filed	104093_0002_118_Declarations.pdf	751853 a7c35a8c04c6cf0f4537677f94138077fdafd1d6	no	4
Warnings:					
Information:					
3	Information Disclosure Statement (IDS) Form (SB08)	104093_0002_118_IDS.pdf	332094 1961f1688a18e60fbb9faf934419abae5dd44338	no	23
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
4	Power of Attorney	104093_0002_118_POA.pdf	1721488 cea66536db480c35844d349bc13b90cf95422748	no	2
Warnings:					
Information:					
5	Transmittal Letter	104093_0002_118_IDS_Letter.pdf	137640 76a8cd43c32e8320eed4f6fcec215a140568ab3c	no	2
Warnings:					
Information:					
6		104093_0002_118_Specification.pdf	994073 ecbf858a007490815160e346c8d4688aa101fdaa	yes	160

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Specification	1	158
	Claims	159	159
	Abstract	160	160

Warnings:
Information:

7	Drawings-only black and white line drawings	104093_0002_118_Drawings.pdf	24870535 b1946b43cc7c1656ecea0f81539fb6e2809007a2	no	68
Warnings:					
Information:					
			Total Files Size (in bytes):	30160641	

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	104093-0002-118
	Application Number	
Title of Invention	SECURE DATA PARSER METHOD AND SYSTEM	

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
	Mark	S.	O'Hare	

Residence Information (Select One) ● US Residency Non US Residency Active US Military Service

City	Coto De Caza	State/Province	CA	Country of Residence	US

Mailing Address of Inventor:

Address 1	8 Kennedy Court		
Address 2			
City	Coto De Caza	State/Province	CA
Postal Code	92679	Country	US

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Rick	L.	Orsini	

Residence Information (Select One) ◉ US Residency Non US Residency Active US Military Service

City	Flower Mound	State/Province	TX	Country of Residence	US

Mailing Address of Inventor:

Address 1	2100 Kings Forest Lane		
Address 2			
City	Flower Mound	State/Province	TX
Postal Code	75028	Country	US

Inventor 3 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Roger	S.	Davenport	

Residence Information (Select One) ◉ US Residency Non US Residency Active US Military Service

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	104093-0002-118
	Application Number	
Title of Invention	SECURE DATA PARSER METHOD AND SYSTEM	

City	Campbell	State/Province	TX	Country of Residence	US

Mailing Address of Inventor:

Address 1	3204 CR 4119		
Address 2			
City	Campbell	State/Province	TX
Postal Code	75422	Country	US

Inventor 4 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Steven		Winick	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Roslyn Heights	State/Province	NY	Country of Residence	US

Mailing Address of Inventor:

Address 1	3 Expressway Plaza		
Address 2			
City	Roslyn Heights	State/Province	NY
Postal Code	11577	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	15314		
Email Address	hgpatentdocket@hglaw.com	Add Email	Remove Email

Application Information:

Title of the Invention	SECURE DATA PARSER METHOD AND SYSTEM		
Attorney Docket Number	104093-0002-118	Small Entity Status Claimed	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	68	Suggested Figure for Publication (if any)	

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	104093-0002-118
	Application Number	
Title of Invention	SECURE DATA PARSER METHOD AND SYSTEM	

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	15314		

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	13915081	2013-06-11

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	104093-0002-118
	Application Number	
Title of Invention	SECURE DATA PARSER METHOD AND SYSTEM	

Prior Application Status	Patented			Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13915081	Division of	13468383	2012-05-10	9338140	2016-05-10
Prior Application Status	Patented			Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13468383	Continuation of	11258839	2005-10-25	8266438	2012-09-11
Prior Application Status	Expired			Remove	
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)		
11258839	Claims benefit of provisional	60718185	2005-09-16		
Prior Application Status	Expired			Remove	
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)		
11258839	Claims benefit of provisional	60622146	2004-10-25		
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.				Add	

Foreign Priority Information:

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

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

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

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	104093-0002-118
	Application Number	
Title of Invention	SECURE DATA PARSER METHOD AND SYSTEM	

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	104093-0002-118
	Application Number	
Title of Invention	SECURE DATA PARSER METHOD AND SYSTEM	

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	104093-0002-118
	Application Number	
Title of Invention	SECURE DATA PARSER METHOD AND SYSTEM	

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	Security First Corp.		
Mailing Address Information For Applicant:			
Address 1	29811 Santa Margarita Parkway, Suite 600		
Address 2			
City	Rancho Santa Margarita	**State/Province**	CA
Country	US	Postal Code	92688
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Assignee Information including Non-Applicant Assignee Information:

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

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	104093-0002-118
	Application Number	
Title of Invention	SECURE DATA PARSER METHOD AND SYSTEM	

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:

Remove

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	/Maxim Rapoport/			Date (YYYY-MM-DD)	2018-05-11
First Name	Maxim	Last Name	Rapoport	Registration Number	67675

Additional Signature may be generated within this form by selecting the Add button. Add

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	104093-0002-118
	Application Number	
Title of Invention	SECURE DATA PARSER METHOD AND SYSTEM	

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it 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	SECURE DATA PARSER METHOD AND SYSTEM

As the below named inventor, I hereby declare that:

This declaration is directed to:

[x] The attached application, or

[ ] United States application or PCT international application number _____ filed on _____ .

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

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

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

WARNING:

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

LEGAL NAME OF INVENTOR

Inventor: Mark S. O'Hare Date (Optional): June 5, 2013

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.

35903011_1

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it 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	SECURE DATA PARSER METHOD AND SYSTEM

As the below named inventor, I hereby declare that:

This declaration is directed to: [x] The attached application, or

[ ] United States application or PCT international application number _____ filed on _____.

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

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

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

WARNING:

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

LEGAL NAME OF INVENTOR

Inventor: Rick L. Orsini Date (Optional): 6/6/13

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.

35903011_1

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it 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	SECURE DATA PARSER METHOD AND SYSTEM

As the below named inventor, I hereby declare that:

This declaration is directed to:

[x] The attached application, or

[ ] United States application or PCT international application number _____ filed on _____ .

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

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

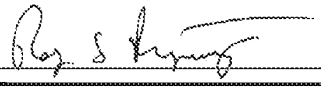
I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

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

LEGAL NAME OF INVENTOR

Inventor: Roger S. Davenport Date (Optional): 6/5/2013

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.

35903011_1

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it 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	SECURE DATA PARSER METHOD AND SYSTEM

As the below named inventor, I hereby declare that:

This declaration is directed to:
- [x] The attached application, or
- [ ] United States application or PCT international application number _____ filed on _____.

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

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

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

WARNING:

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

LEGAL NAME OF INVENTOR

Inventor: Steven Winick Date (Optional): _____

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.

35903011_1