Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	SECURE DATA PARSER METHOD AND SYSTEM
First Named Inventor/Applicant Name:	Rick L. Orsini
Filer:	Edward A. Gordon/Lily Jiang
Attorney Docket Number:	104093-0002-105

Filed as Large Entity

Track I Prioritized Examination - Nonprovisional Application under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility application filing	1011	1	380	380
Utility Search Fee	1111	1	620	620
Utility Examination Fee	1311	1	250	250
Request for Prioritized Examination	1817	1	4800	4800
Pages:				
Utility Appl Size fee per 50 sheets >100	1081	2	310	620
Claims:				
Claims in excess of 20	1202	7	60	420

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous-Filing:				
Publ. Fee- early, voluntary, or normal	1504	1	300	300
Processing Fee, except for Provis. apps	1808	1	130	130
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**7520**

Application Data Sheet

Application Information

Application Type::	Regular
Subject Matter::	Utility
Suggested Group Art Unit::	2432
CD-ROM or CD-R?::	None
Sequence submission?::	None
Computer Readable Form (CRF)?::	No
Title::	SECURE DATA PARSER METHOD AND SYSTEM
Attorney Docket Number::	104093-0002-105
Request for Early Publication?::	No
Request for Non-Publication?::	No
Total Drawing Sheets::	36
Small Entity?::	No
Petition included?::	No
Secrecy Order in Parent Appl.?::	No

Applicant Information

Applicant Authority Type::	Inventor
Primary Citizenship Country::	US
Status::	Full Capacity
Given Name::	Rick

Middle Name::	L.
Family Name::	Orsini
City of Residence::	Flower Mound
State or Province of Residence::	TX
Country of Residence::	US
Street of mailing address::	2100 Kings Forest Lane
City of mailing address::	Flower Mound
State or Province of mailing address::	TX
Postal or Zip Code of mailing address::	75028

Applicant Authority Type::	Inventor
Primary Citizenship Country::	US
Status::	Full Capacity
Given Name::	Mark
Middle Name::	S.
Family Name::	O'Hare
City of Residence::	Coto De Caza
State or Province of Residence::	CA
Country of Residence::	US
Street of mailing address::	8 Kennedy Court
City of mailing address::	Coto De Caza
State or Province of mailing address::	CA

Postal or Zip Code of mailing address::	92679

Applicant Authority Type::	Inventor
Primary Citizenship Country::	US
Status::	Full Capacity
Given Name::	Roger
Middle Name::	S.
Family Name::	Davenport
City of Residence::	Campbell
State or Province of Residence::	TX
Country of Residence::	US
Street of mailing address::	3204 CR 4119
City of mailing address::	Campbell
State or Province of mailing address::	TX
Postal or Zip Code of mailing address::	75422

Applicant Authority Type::	Inventor
Primary Citizenship Country::	US
Status::	Full Capacity
Given Name::	Steven
Family Name::	Winick
City of Residence::	Roslyn Heights

State or Province of Residence:: NY

Country of Residence:: US

Street of mailing address:: 3 Expressway Plaza

City of mailing address:: Roslyn Heights

State or Province of mailing address:: NY

Postal or Zip Code of mailing address:: 11577

Correspondence Information

Correspondence Customer Number:: 01473

Representative Information

Representative Customer Number:: 01473

Domestic Priority Information

Application::	Continuity Type::	Parent Application::	Parent Filing Date::
This Application	Continuation of	11/258,839	10/25/05
11/258,839	An application claiming the benefit under 35 USC 119(e)	60/718,185	09/16/05
11/258,839	An application claiming the benefit under 35 USC 119(e)	60/622,146	10/25/04

Foreign Priority Information

Assignee Information

Assignee name::	Security First Corp.
Street of mailing address::	29811 Santa Margarita Parkway, Suite 600
City of mailing address::	Rancho Santa Margarita
State or Province of mailing address::	CA
Postal or Zip Code of mailing address::	92688

29475135_1

OIPE IAP37
APR 17 2006
PATENT & TRADEMARK OFFICE

DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am an original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

SECURE DATA PARSER METHOD AND SYSTEM

the specification of which

[ ] is attached hereto

[X] was filed on October 25, 2005 as Application Serial No. 11/258,839 .

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims.

I do not know and do not believe that the invention was ever patented or described in any printed publication in any country before my or our invention thereof or more than one year prior to this application.

I do not know and do not believe that the invention was in public use or on sale in the United States of America more than one year prior to this application.

I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known by me to be material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, § 119(a)-(d) of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)

(Number)	(Country)	(Filing Date)	Priority Claimed [ ] Yes	[ ] No

I hereby claim the benefit under Title 35, United States Code § 119(e) of any United States provisional application(s) listed below.

60/622,146	October 25, 2004
(Application Serial No.)	(Filing Date)
60/718,185	September 16, 2005
(Application Serial No.)	(Filing Date)

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known by me to be material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)

As a named inventor, I hereby appoint the following attorneys or agents to prosecute this application and transact all business in the United States Patent and Trademark Office connected therewith:

Robert R. Jackson, Esq. - Reg. No. 26,183
Jeffrey H. Ingerman, Esq. - Reg. No. 31,069
Alexander Shvarts, Esq. - Reg. No. 47,943

Send correspondence to: Alexander Shvarts
FISH & NEAVE IP GROUP
ROPES & GRAY LLP
1251 Avenue of the Americas
New York, New York 10020-1104

Direct telephone calls to: Alexander Shvarts

(212) 596-9000

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of first inventor Rick L. Orsini

First inventor's signature _____ 2/7/06
Date

Residence 2100 Kings Forest Lane, Flower Mound, Texas 75028
Citizenship United States
Post Office Address 2100 Kings Forest Lane, Flower Mound, Texas 75028

Full name of second inventor Mark S. O'Hare

Second inventor's signature _____ _____
Date

Residence 8 Kennedy Court, Coto De Caza, CA 92679
Citizenship United States
Post Office Address 8 Kennedy Court, Coto De Caza, CA 92679

Full name of third Inventor Roger Davenport

Third Inventor's signature _____ _____
Date

Residence 3204 CR 4119, Campbell, Texas 75422
Citizenship United States
Post Office Address 3204 CR 4119, Campbell, Texas 75422

Full name of fourth Inventor Steven Winick

Fourth Inventor's signature _____ _____
Date

Residence 3 Expressway Plaza, Roslyn Heights, NY 11577
Citizenship United States
Post Office Address 3 Expressway Plaza, Roslyn Heights, NY 11577

OIPE IAP37
APR 17 2006
PATENT & TRADEMARK OFFICE

SEC-2

DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am an original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

SECURE DATA PARSER METHOD AND SYSTEM

the specification of which

[ ] is attached hereto

[X] was filed on October 25, 2005 as Application Serial No. 11/258,839 .

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims.

I do not know and do not believe that the invention was ever patented or described in any printed publication in any country before my or our invention thereof or more than one year prior to this application.

I do not know and do not believe that the invention was in public use or on sale in the United States of America more than one year prior to this application.

I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known by me to be material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, § 119(a)-(d) of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)

(Number)	(Country)	(Filing Date)	Priority Claimed [ ] Yes [ ] No

I hereby claim the benefit under Title 35, United States Code § 119(e) of any United States provisional application(s) listed below.

60/622,146 (Application Serial No.) October 25, 2004 (Filing Date)

60/718,185 (Application Serial No.) September 16, 2005 (Filing Date)

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known by me to be material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)

As a named inventor, I hereby appoint the following attorneys or agents to prosecute this application and transact all business in the United States Patent and Trademark Office connected therewith:

Robert R. Jackson, Esq. - Reg. No. 26,183
Jeffrey H. Ingerman, Esq. - Reg. No. 31,069
Alexander Shvarts, Esq. - Reg. No. 47,943

Send correspondence to: Alexander Shvarts
FISH & NEAVE IP GROUP
ROPES & GRAY LLP
1251 Avenue of the Americas
New York, New York 10020-1104

Direct telephone calls to: Alexander Shvarts

(212) 596-9000

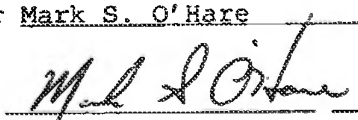
I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of first inventor Rick L. Orsini

First inventor's signature _____ _____
Date

Residence 2100 Kings Forest Lane, Flower Mound, Texas 75028
Citizenship United States
Post Office Address 2100 Kings Forest Lane, Flower Mound, Texas 75028

Full name of second inventor Mark S. O'Hare

Second inventor's signature  _____
Date

Residence 8 Kennedy Court, Coto De Caza, CA 92679
Citizenship United States
Post Office Address 8 Kennedy Court, Coto De Caza, CA 92679

Full name of third Inventor Roger Davenport

Third Inventor's signature _____ _____
Date

Residence 3204 CR 4119, Campbell, Texas 75422
Citizenship United States
Post Office Address 3204 CR 4119, Campbell, Texas 75422

Full name of fourth Inventor Steven Winick

Fourth Inventor's signature _____ _____
Date

Residence 3 Expressway Plaza, Roslyn Heights, NY 11577
Citizenship United States
Post Office Address 3 Expressway Plaza, Roslyn Heights, NY 11577

APR 17 2006
PATENT & TRADEMARK OFFICE
1AP37

SEC-2

DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am an original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

SECURE DATA PARSER METHOD AND SYSTEM

the specification of which

[ ] is attached hereto

[X] was filed on October 25, 2005 as Application Serial No. 11/258,839.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims.

I do not know and do not believe that the invention was ever patented or described in any printed publication in any country before my or our invention thereof or more than one year prior to this application.

I do not know and do not believe that the invention was in public use or on sale in the United States of America more than one year prior to this application.

I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known by me to be material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, § 119(a)-(d) of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)

(Number)	(Country)	(Filing Date)	Priority Claimed [ ] Yes [ ] No

I hereby claim the benefit under Title 35, United States Code § 119(e) of any United States provisional application(s) listed below.

60/622,146 (Application Serial No.) October 25, 2004 (Filing Date)

60/718,185 (Application Serial No.) September 16, 2005 (Filing Date)

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known by me to be material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)

As a named inventor, I hereby appoint the following attorneys or agents to prosecute this application and transact all business in the United States Patent and Trademark Office connected therewith:

Robert R. Jackson, Esq. - Reg. No. 26,183
Jeffrey H. Ingerman, Esq. - Reg. No. 31,069
Alexander Shvarts, Esq. - Reg. No. 47,943

Send correspondence to: Alexander Shvarts
FISH & NEAVE IP GROUP
ROPES & GRAY LLP
1251 Avenue of the Americas
New York, New York 10020-1104

Direct telephone calls to: Alexander Shvarts

(212) 596-9000

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of first inventor Rick L. Orsini

First inventor's signature _____ _____
Date

Residence 2100 Kings Forest Lane, Flower Mound, Texas 75028
Citizenship United States
Post Office Address 2100 Kings Forest Lane, Flower Mound, Texas 75028

Full name of second inventor Mark S. O'Hare

Second inventor's signature _____ _____
Date

Residence 8 Kennedy Court, Coto De Caza, CA 92679
Citizenship United States
Post Office Address 8 Kennedy Court, Coto De Caza, CA 92679

Full name of third Inventor Roger Davenport

Third Inventor's signature [signature] 2/15/06
Date

Residence 3204 CR 4119, Campbell, Texas 75422
Citizenship United States
Post Office Address 3204 CR 4119, Campbell, Texas 75422

Full name of fourth Inventor Steven Winick

Fourth Inventor's signature _____ _____
Date

Residence 3 Expressway Plaza, Roslyn Heights, NY 11577

Citizenship United States

Post Office Address 3 Expressway Plaza, Roslyn Heights, NY 11577

OIPE
APR 17 2006
PATENT & TRADEMARK OFFICE
1AP37

DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am an original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

SECURE DATA PARSER METHOD AND SYSTEM

the specification of which

[ ] is attached hereto

[X] was filed on October 25, 2005 as Application Serial No. 11/258,839 .

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims.

I do not know and do not believe that the invention was ever patented or described in any printed publication in any country before my or our invention thereof or more than one year prior to this application.

I do not know and do not believe that the invention was in public use or on sale in the United States of America more than one year prior to this application.

I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known by me to be material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, § 119(a)-(d) of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)

(Number)	(Country)	(Filing Date)	Priority Claimed [ ] Yes [ ] No

I hereby claim the benefit under Title 35, United States Code § 119(e) of any United States provisional application(s) listed below.

60/622,146 (Application Serial No.) October 25, 2004 (Filing Date)

60/718,185 (Application Serial No.) September 16, 2005 (Filing Date)

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known by me to be material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)

As a named inventor, I hereby appoint the following attorneys or agents to prosecute this application and transact all business in the United States Patent and Trademark Office connected therewith:

Robert R. Jackson, Esq. - Reg. No. 26,183
Jeffrey H. Ingerman, Esq. - Reg. No. 31,069
Alexander Shvarts, Esq. - Reg. No. 47,943

Send correspondence to: Alexander Shvarts
FISH & NEAVE IP GROUP
ROPES & GRAY LLP
1251 Avenue of the Americas
New York, New York 10020-1104

Direct telephone calls to: Alexander Shvarts

(212) 596-9000

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of first inventor Rick L. Orsini

First inventor's signature _____ Date _____

Residence 2100 Kings Forest Lane, Flower Mound, Texas 75028

Citizenship United States

Post Office Address 2100 Kings Forest Lane, Flower Mound, Texas 75028

Full name of second inventor Mark S. O'Hare

Second inventor's signature _____ Date _____

Residence 8 Kennedy Court, Coto De Caza, CA 92679

Citizenship United States

Post Office Address 8 Kennedy Court, Coto De Caza, CA 92679

Full name of third Inventor Roger Davenport

Third Inventor's signature _____ Date _____

Residence 3204 CR 4119, Campbell, Texas 75422

Citizenship United States

Post Office Address 3204 CR 4119, Campbell, Texas 75422

Full name of fourth Inventor Steven Winick

Fourth Inventor's signature _____ 4/10/06
Date

Residence 3 Expressway Plaza, Roslyn Heights, NY 11577
Citizenship United States
Post Office Address 3 Expressway Plaza, Roslyn Heights, NY 11577

PTO/SB/81 (01-09)
Approved for use through 11/30/2011. 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 OR REVOCATION OF POWER OF ATTORNEY WITH A NEW POWER OF ATTORNEY AND CHANGE OF CORRESPONDENCE ADDRESS

Application Number	11/258,839
Filing Date	October 25, 2005
First Named Inventor	Rick L. Orsini
Title	SECURE DATA PARSER METHOD AND SYSTEM
Art Unit	2432
Examiner Name	Samson B. Lemma
Attorney Docket No.	SFC-2

I hereby revoke all previous powers of attorney given in the above-identified application.

☐ A Power of Attorney is submitted herewith.

OR

☒ I hereby appoint Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

1473

OR

☐ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

Practitioner(s) Name	Registration Number	Practitioner(s) Name	Registration Number

Please recognize or change the correspondence address for the above-identified application 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/Inventor

OR

☒ Assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) (Form PTO/SB/96) submitted herewith or filed on _____

SIGNATURE of Applicant or Assignee of Record

Signature		Date	6-29-11
Name	Mark S. O'Hare	Telephone	(949) 533-9901
Title and Company	President & CEO, Security First Corp.		

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below.*

☒ *Total of 1 forms are submitted.

Doc Code: TRACK1.REQ
Document Description: TrackOne Request

PTO/SB/424 (09-11)

CERTIFICATION AND REQUEST FOR PRIORITIZED EXAMINATION (TRACK I) (Page 1 of 1)

First Named Inventor:	Rick L. Orsini	Nonprovisional Application Number (if known):	Not Yet Assigned
Title of Invention:	SECURE DATA PARSER METHOD AND SYSTEM		

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS PRIORITIZED EXAMINATION (TRACK I) FOR THE ABOVE-IDENTIFIED APPLICATION.

1. (a) The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a). This certification and request is being filed with the utility application via EFS-Web.

   OR

   (b) The application is an original nonprovisional plant application filed under 35 U.S.C. 111(a). This certification and request is being filed with the plant application in paper. (Note: Plant applications cannot be filed via EFS-Web.)

   Note: The following are excluded from the Track I program: design applications, provisional applications, national stage applications, PCT international applications, reissue applications, and reexamination proceedings.

2. The following fees (in amounts consistent with the current fee schedule available at http://www.uspto.gov/about/offices/cfo/finance/fees.jsp) are filed with the application: (1) basic filing fee; (2) search fee; (3) examination fee; (4) any required excess claims fees; (5) any required application size fee; (6) publication fee; (7) processing fee (Track I) set forth in 37 CFR 1.17(i); and (8) prioritized examination fee (Track I) set forth in 37 CFR 1.17(c).

3. An executed oath or declaration under 37 CFR 1.63 is filed with the application.

4. The application contains or is amended to contain no more than four independent claims and no more than thirty total claims, and no multiple dependent claims.

Signature /Edward A. Gordon/	Date February 10, 2012
Name (Print/Typed) Edward A. Gordon	Practitioner Registration Number 54,130

Note: *Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required in accordance with 37 CFR 1.33 and 11.18. Please see 37 CFR 1.4(d) for the form of the signature. If necessary, submit multiple forms for more than one signature, see below*.*

☑ *Total of 1 forms are submitted.

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.

SCORE Placeholder Sheet for IFW Content

Application Number: 13371363 Document Date: 2/10/2012

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

- Drawings – Other than Black and White Line Drawings

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

To access the documents in the SCORE database, refer to instructions developed by SIRA.

At the time of document entry (noted above):

- Examiners may access SCORE content via the eDAN interface.
- Other USPTO employees can bookmark the current SCORE URL (http://es/ScoreAccessWeb/).
- External customers may access SCORE content via the Public and Private PAIR interfaces.

Form Revision Date: February 8, 2006

SECURE DATA PARSER METHOD AND SYSTEM

Abstract of the Invention

[0455] 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.

Electronic Acknowledgement Receipt

EFS ID:	12054868
Application Number:	13371363
International Application Number:	
Confirmation Number:	7984
Title of Invention:	SECURE DATA PARSER METHOD AND SYSTEM
First Named Inventor/Applicant Name:	Rick L. Orsini
Customer Number:	1473
Filer:	Edward A. Gordon/Lily Jiang
Filer Authorized By:	Edward A. Gordon
Attorney Docket Number:	104093-0002-105
Receipt Date:	10-FEB-2012
Filing Date:	
Time Stamp:	21:32:23
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$7520
RAM confirmation Number	6356
Deposit Account	061075
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 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	TrackOne Request	104093-0002-105_Certificate_Request_TrackI.pdf	39368 7eccc76fe482646f584ea9f9a00ff6e60cc695e6	no	2
Warnings:					
Information:					
2	Application Data Sheet	104093-0002-105_ADS.pdf	61944 34f5fd13bf83b959493e8e82d9f40a126677ab99	no	6
Warnings:					
Information:					
This is not an USPTO supplied ADS fillable form					
3	Oath or Declaration filed	104093-0002-105_Declaration_POA.pdf	503734 dc7a07bf1cbe213a41c5930d764d35566bb96433	no	16
Warnings:					
Information:					
4	Power of Attorney	104093-0002-105_Revocation_of_POA_and_Address.pdf	1956514 bf1453989cb68a1a7c18f1de369cd439135e52be	no	1
Warnings:					
Information:					
5		104093-0002-105_Specification.pdf	263996 d908f803b1d2600d25510453939704da81cc6073	yes	182

Multipart Description/PDF files in .zip description

Document Description	Start	End
Specification	1	174
Claims	175	181
Abstract	182	182

Warnings:					
Information:					
6	Drawings-only black and white line drawings	104093-0002-105_Drawings.pdf	1055821 36b2874b5d1538f46ceb6dd3b9b6349ead8edde0	no	36

Warnings:					
Information:					
7	Assignee showing of ownership per 37 CFR 3.73(b).	104093-0002-105_Statement.pdf	57586 44e4ab57681357f61e99189b0ec5be76098 5674d	no	1
Warnings:					
Information:					
8	Transmittal of New Application	104093-0002-105_Transmittal.pdf	103541 4d7510309a1012adabb7f2dbad1de8a8c6e 0d0f7	no	1
Warnings:					
Information:					
9	Fee Worksheet (SB06)	fee-info.pdf	43282 af915beadf8933163a44980405501ee08d7 74b31	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	4085786		

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/SB/96 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: Security First Corp

Application No./Patent No.: 11/258,839 Filed/Issue Date: October 26, 2005

Titled: SECURE DATA PARSER METHOD AND SYSTEM

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

states that it is:

1. [X] the assignee of the entire right, title, and interest in;

2. [ ] an assignee of less than the entire right, title, and interest in
(The extent (by percentage) of its ownership interest is _____ %); or

3. [ ] an assignee of an undivided interest in the entirety of (a complete assignment from one of the joint inventors was made) the patent application/patent identified above by virtue of either:

A. [X] 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 017501, Frame 0777, or for which a copy thereof is attached.

OR

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

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

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

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

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

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

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

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

Signature _____ Date: 6-29-11

Mark S. O'Hare — Printed or Typed Name

President & CEO — Title

What is claimed is:

1. A method for securing a data set, the method steps implemented by a programmed computer system, the method steps comprising:

encrypting the data set based on an encryption key to produce an encrypted data set;

creating hash information based on a hash operation using the data set;

generating data splitting information, wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;

separating the encrypted data set into the plurality of shares based on the data splitting information;

including in the plurality of shares data indicative of (a) the encryption key and (b) the hash information; and

causing the plurality of shares to be stored in respective separate storage locations;

wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares.

2. The method of claim 1, wherein the step of separating the encrypted data set comprises using a deterministic technique.

3. The method of claim 1, wherein the step of separating the encrypted data set comprises using a substantially random technique.

4. The method of claim 1, further comprising causing a plurality of data units in each of the shares to be rearranged relative to one another after the separating step.

5. The method of claim 1, wherein the step of separating the encrypted data into the plurality of shares comprises causing the plurality of shares to have a substantially randomly distribution of the encrypted data set.

6. The method of claim 1, wherein the data indicative of the encryption key comprises data created using a Shamir algorithm.

7. The method of claim 1, wherein the step of including data indicative of the encryption key comprises:

encrypting the encryption key with a second key; and

including in the plurality of shares data indicative of the encrypted encryption key.

8. The method of claim 7 further comprising the method step of storing the second key outside of the plurality of shares, wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares, and the second key.

9. The method of claim 1, wherein the step of storing the shares in respective separate storage

locations comprises storing the shares on at least two separate storage devices.

10. A non-transitory computer readable medium storing computer executable instructions that, when executed by at least one processor, cause a computer system to carry out a method for securing a data set, the method comprising the steps of:

encrypting the data set based on an encryption key to produce an encrypted data set;

creating hash information based on a hash operation using the data set;

generating data splitting information, wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;

separating the encrypted data set into the plurality of shares based on the data splitting information;

including in the plurality of shares data indicative of (a) the encryption key and (b) the hash information; and

causing the plurality of shares to be stored in respective separate storage locations;

wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares.

11. The non-transitory computer readable medium of claim 10, wherein the step of separating the encrypted data set comprises using a deterministic technique.

12. The non-transitory computer readable medium of claim 10, wherein the step of separating the encrypted data set comprises using a substantially random technique.

13. The non-transitory computer readable medium of claim 10, wherein the method further comprises causing a plurality of data units of the encrypted data set to be rearranged relative to one another after the separating step.

14. The non-transitory computer readable medium of claim 10, wherein the step of separating the encrypted data into the plurality of shares comprises causing the plurality of shares to have a substantially randomly distribution of the encrypted data set.

15. The non-transitory computer readable medium of claim 10, wherein the data indicative of the encryption key comprises data created using a Shamir algorithm.

16. The non-transitory computer readable medium of claim 11, wherein the step of including data indicative of the encryption key comprises:

encrypting the encryption key with a second key; and

including in the plurality of shares data indicative of the encrypted encryption key.

17. The non-transitory computer readable medium of claim 16 wherein the method further comprises storing the second key outside of the plurality of

shares, wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares, and the second key.

18. The non-transitory computer readable medium of claim 10, wherein the step of storing the shares in respective separate storage locations comprises storing the shares on at least two separate storage devices.

19. A computer system for securing a data set, the system comprising:

at least one processor;

a non-transitory computer readable medium storing computer executable instructions that, when executed by the at least one processor, cause the computer system to carry out the following steps:

encrypting the data set based on an encryption key to produce an encrypted data set;

creating hash information based on a hash operation using the data set;

generating data splitting information, wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;

separating the encrypted data set into the plurality of shares based on the data splitting information;

including in the plurality of shares data indicative of (a) the encryption key and (b) the hash information;, and

causing the plurality of shares to be stored in respective separate storage locations;

wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares.

20. The system of claim 19, wherein the step of separating the encrypted data set comprises using a deterministic technique.

21. The system of claim 19, wherein the step of separating the encrypted data set comprises using a substantially random technique.

22. The system of claim 19, wherein the method further comprises causing a plurality of data units of the encrypted data set to be rearranged relative to one another after the separating step.

23. The system of claim 19, wherein the step of separating the encrypted data into the plurality of shares comprises causing the plurality of shares to have a substantially randomly distribution of the encrypted data set.

24. The system of claim 19, wherein data indicative of the encryption key comprises data that was created using a Shamir algorithm.

25. The system of claim 19, wherein the step of including data indicative of the encryption key comprises:

encrypting the encryption key with a second key; and

including in the plurality of shares data indicative of the encrypted encryption key.

26. The system of claim 25 wherein the method further comprises storing the second key outside of the plurality of shares, wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares, and the second key.

27. The system of claim 19, wherein the separate storage locations are located on at least two separate storage devices.

Electronic Acknowledgement Receipt

EFS ID:	12054868
Application Number:	13371363
International Application Number:	
Confirmation Number:	7984
Title of Invention:	SECURE DATA PARSER METHOD AND SYSTEM
First Named Inventor/Applicant Name:	Rick L. Orsini
Customer Number:	1473
Filer:	Edward A. Gordon/Lily Jiang
Filer Authorized By:	Edward A. Gordon
Attorney Docket Number:	104093-0002-105
Receipt Date:	10-FEB-2012
Filing Date:	
Time Stamp:	21:32:23
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$7520
RAM confirmation Number	6356
Deposit Account	061075
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 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	TrackOne Request	104093-0002-105_Certificate_Request_TrackI.pdf	39368 7eccc76fe482646f584ea9f9a00ff6e60cc695e6	no	2
Warnings:					
Information:					
2	Application Data Sheet	104093-0002-105_ADS.pdf	61944 34f5fd13bf83b959493e8e82d9f40a126677ab99	no	6
Warnings:					
Information:					
This is not an USPTO supplied ADS fillable form					
3	Oath or Declaration filed	104093-0002-105_Declaration_POA.pdf	503734 dc7a07bf1cbe213a41c5930d764d35566bb96433	no	16
Warnings:					
Information:					
4	Power of Attorney	104093-0002-105_Revocation_of_POA_and_Address.pdf	1956514 bf1453989cb68a1a7c18f1de369cd439135e52be	no	1
Warnings:					
Information:					
5		104093-0002-105_Specification.pdf	263996 d908f803b1d2600d25510453939704da81cc6073	yes	182

Multipart Description/PDF files in .zip description

Document Description	Start	End
Specification	1	174
Claims	175	181
Abstract	182	182

Warnings:					
Information:					
6	Drawings-only black and white line drawings	104093-0002-105_Drawings.pdf	1055821 36b2874b5d1538f46ceb6dd3b9b6349ead8edde0	no	36

Warnings:					
Information:					
7	Assignee showing of ownership per 37 CFR 3.73(b).	104093-0002-105_Statement.pdf	57586 44e4ab57681357f61e99189b0ec5be76098 5674d	no	1
Warnings:					
Information:					
8	Transmittal of New Application	104093-0002-105_Transmittal.pdf	103541 4d7510309a1012adabb7f2dbad1de8a8c6e 0d0f7	no	1
Warnings:					
Information:					
9	Fee Worksheet (SB06)	fee-info.pdf	43282 af915beadf8933163a44980405501ee08d7 74b31	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	4085786		

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.

Figure 1

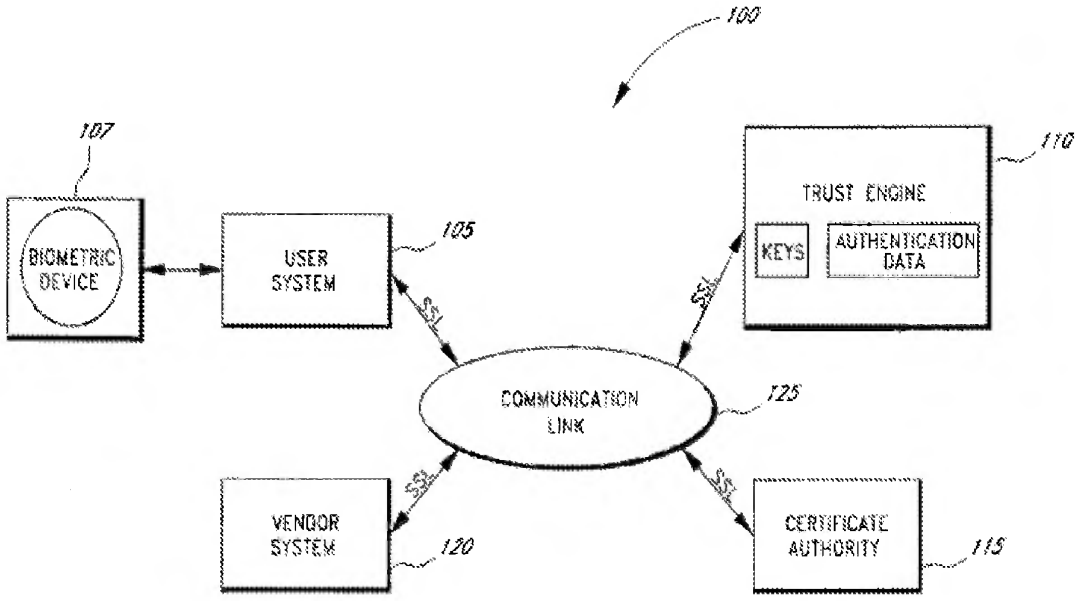

100
107
BIOMETRIC DEVICE
USER SYSTEM
105
SSL
TRUST ENGINE
110
KEYS
AUTHENTICATION DATA
SSL
COMMUNICATION LINK
125
SSL
SSL
VENDOR SYSTEM
120
CERTIFICATE AUTHORITY
115

Figure 2

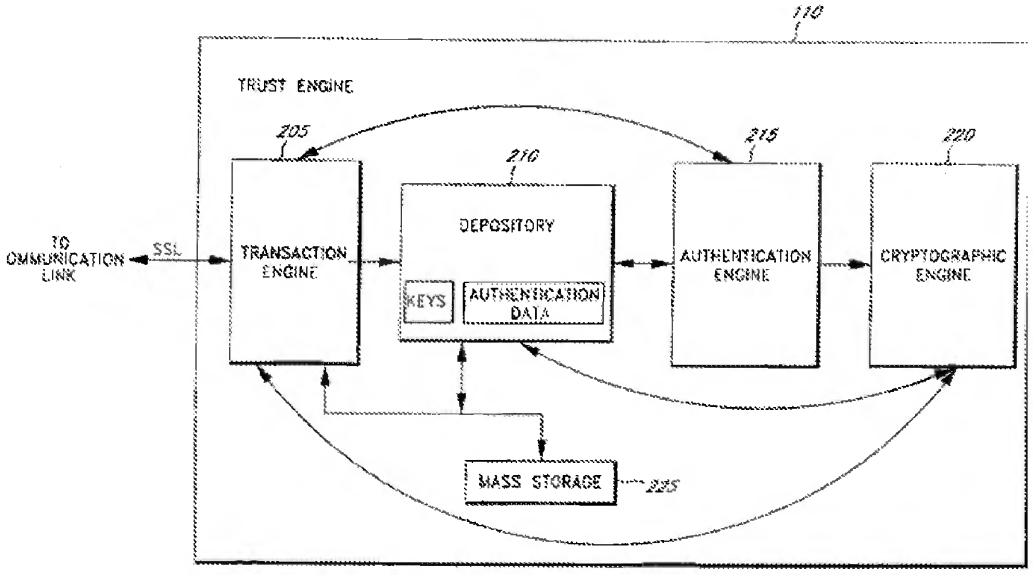

110
TRUST ENGINE
205
210
215
220
TO COMMUNICATION LINK
SSL
TRANSACTION ENGINE
DEPOSITORY
KEYS
AUTHENTICATION DATA
AUTHENTICATION ENGINE
CRYPTOGRAPHIC ENGINE
MASS STORAGE
225

Figure 3

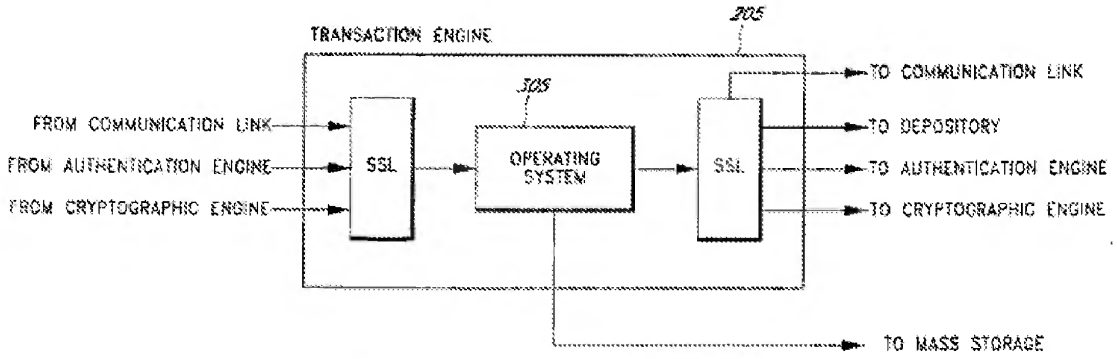

TRANSACTION ENGINE
305
FROM COMMUNICATION LINK
FROM AUTHENTICATION ENGINE
FROM CRYPTOGRAPHIC ENGINE
SSL
OPERATING SYSTEM
SSL
TO COMMUNICATION LINK
TO DEPOSITORY
TO AUTHENTICATION ENGINE
TO CRYPTOGRAPHIC ENGINE
TO MASS STORAGE

Figure 4

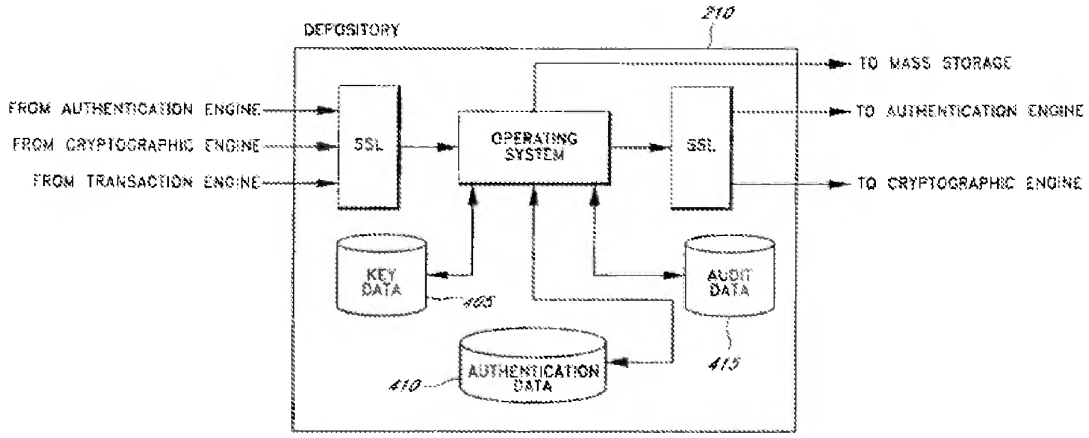

DEPOSITORY
210
FROM AUTHENTICATION ENGINE
FROM CRYPTOGRAPHIC ENGINE
FROM TRANSACTION ENGINE
SSL
OPERATING SYSTEM
SSL
TO MASS STORAGE
TO AUTHENTICATION ENGINE
TO CRYPTOGRAPHIC ENGINE
KEY DATA
405
AUDIT DATA
415
AUTHENTICATION DATA
410

Figure 5

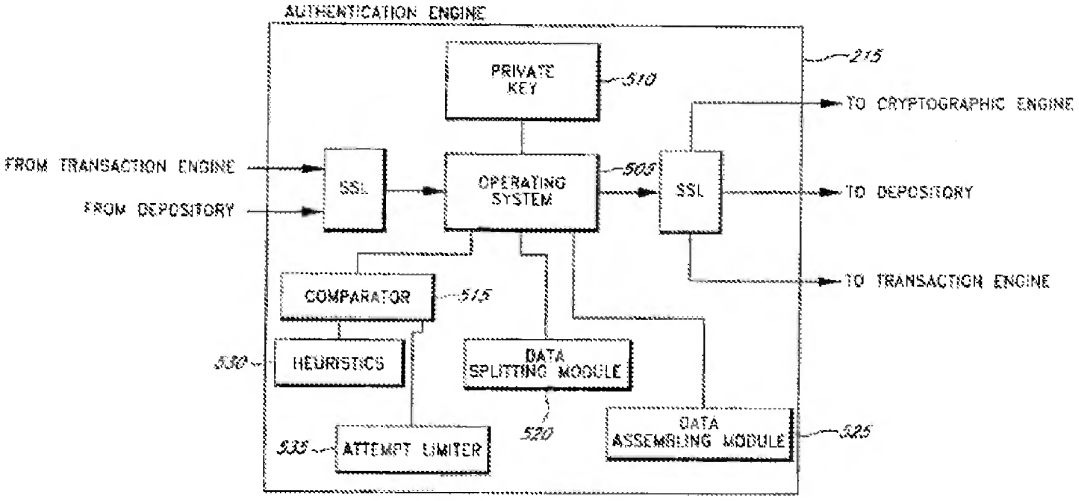

AUTHENTICATION ENGINE
215
PRIVATE KEY
510
TO CRYPTOGRAPHIC ENGINE
FROM TRANSACTION ENGINE
FROM DEPOSITORY
SSL
OPERATING SYSTEM
505
SSL
TO DEPOSITORY
TO TRANSACTION ENGINE
COMPARATOR
515
530
HEURISTICS
DATA SPLITTING MODULE
520
DATA ASSEMBLING MODULE
525
535
ATTEMPT LIMITER

Figure 6

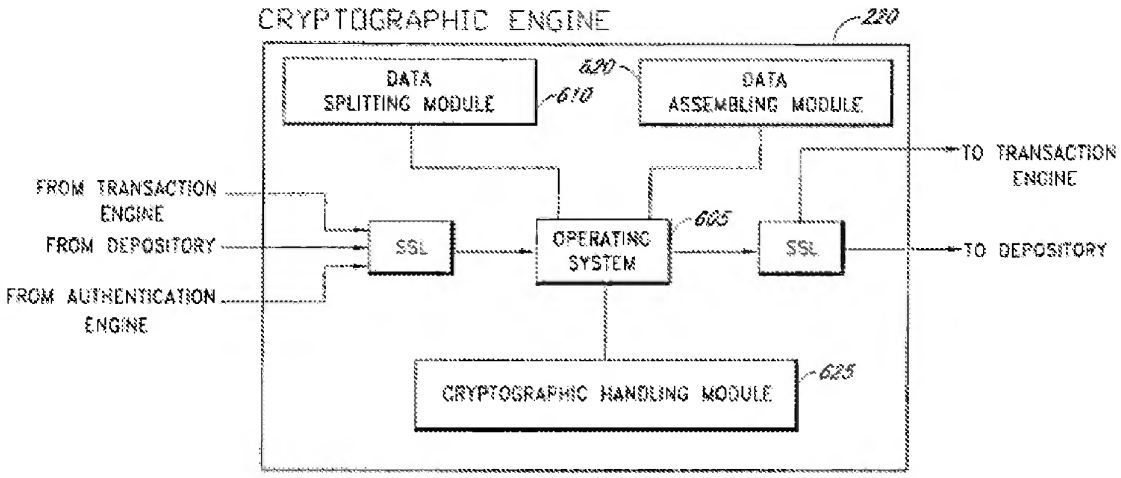

CRYPTOGRAPHIC ENGINE
220
DATA SPLITTING MODULE
610
630
DATA ASSEMBLING MODULE
FROM TRANSACTION ENGINE
FROM DEPOSITORY
FROM AUTHENTICATION ENGINE
SSL
OPERATING SYSTEM
605
SSL
TO TRANSACTION ENGINE
TO DEPOSITORY
CRYPTOGRAPHIC HANDLING MODULE
625

Figure 7

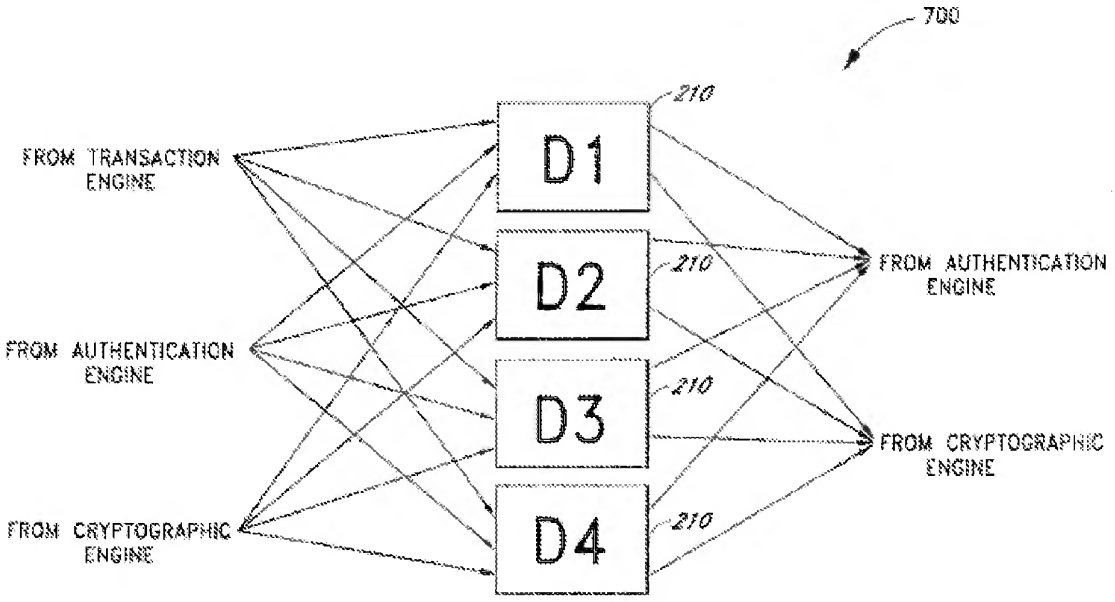

700
210
D1
D2
D3
D4
FROM TRANSACTION ENGINE
FROM AUTHENTICATION ENGINE
FROM CRYPTOGRAPHIC ENGINE
FROM AUTHENTICATION ENGINE
FROM CRYPTOGRAPHIC ENGINE

Figure 8

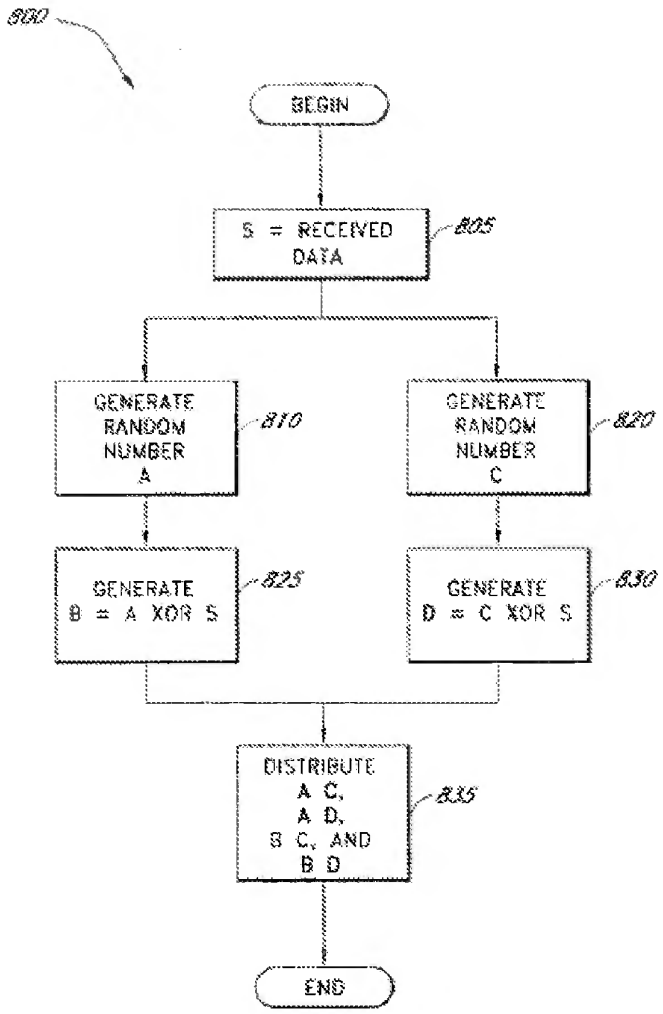

800
BEGIN
S = RECEIVED DATA
805
GENERATE RANDOM NUMBER A
810
GENERATE RANDOM NUMBER C
820
GENERATE B = A XOR S
825
GENERATE D = C XOR S
830
DISTRIBUTE A C, A D, S C, AND B D
835
END

Figure 9, Panel A

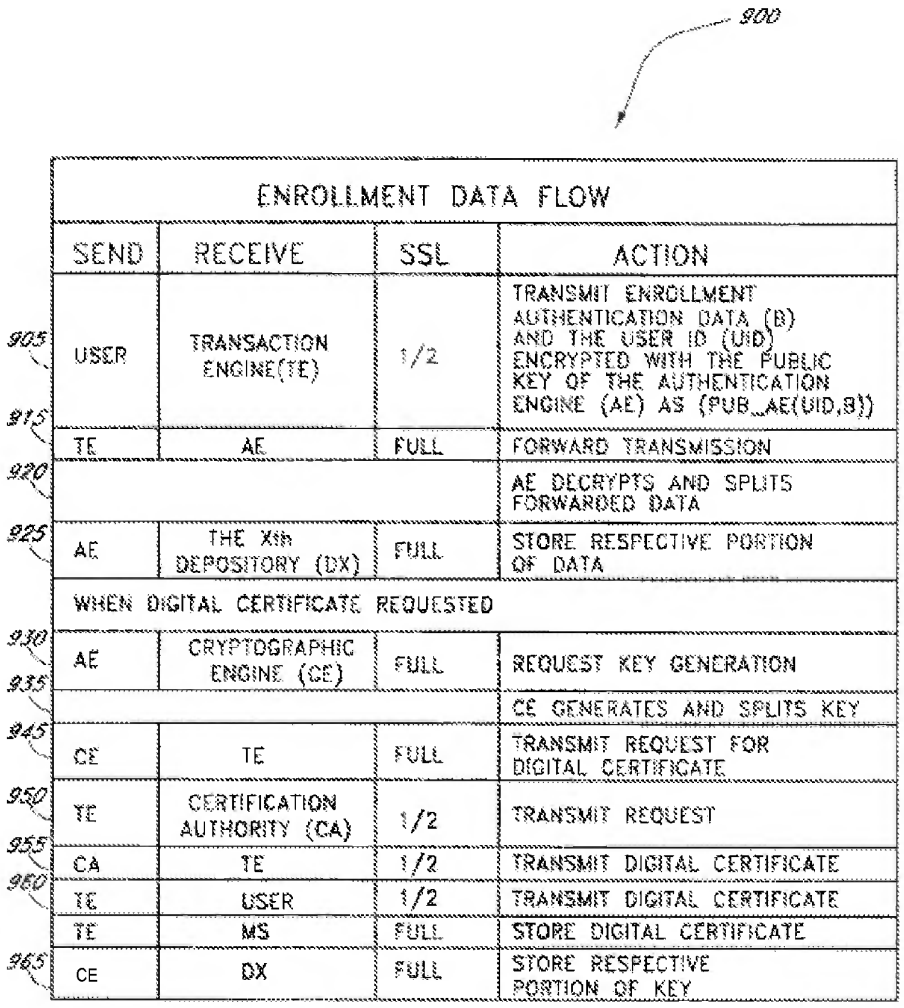


Figure 9, Panel B

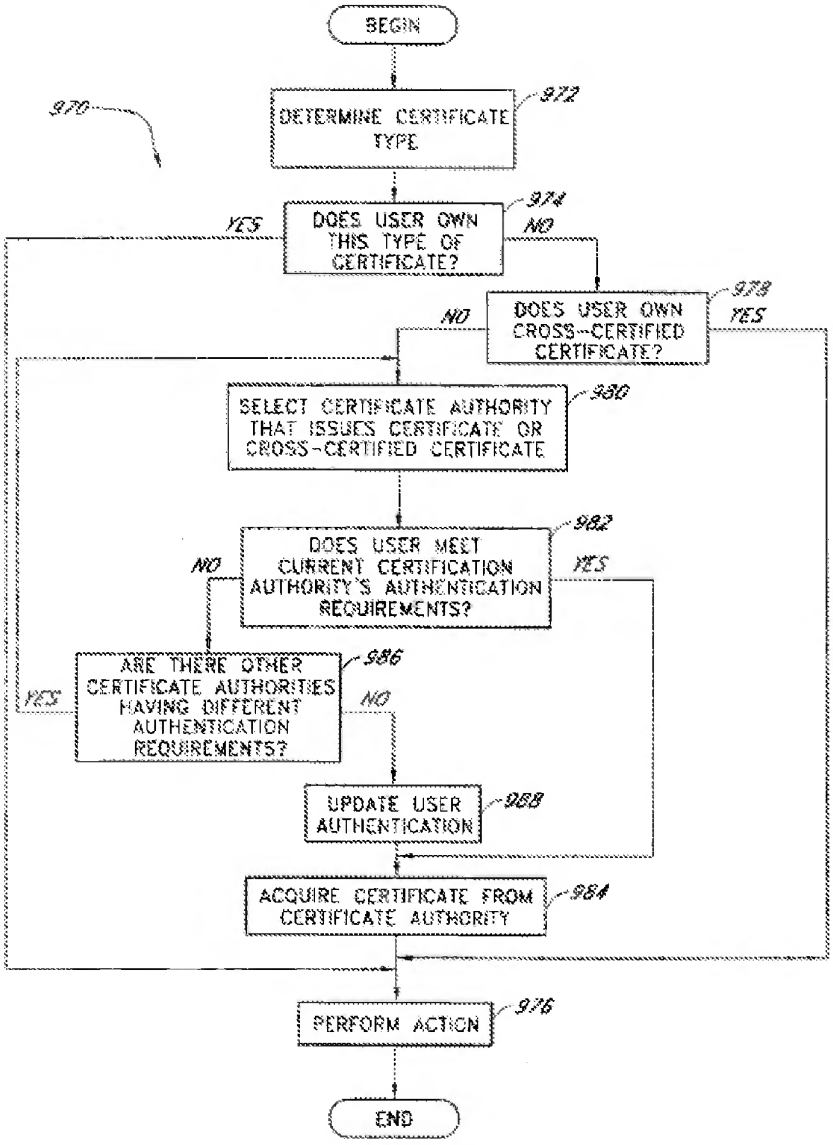
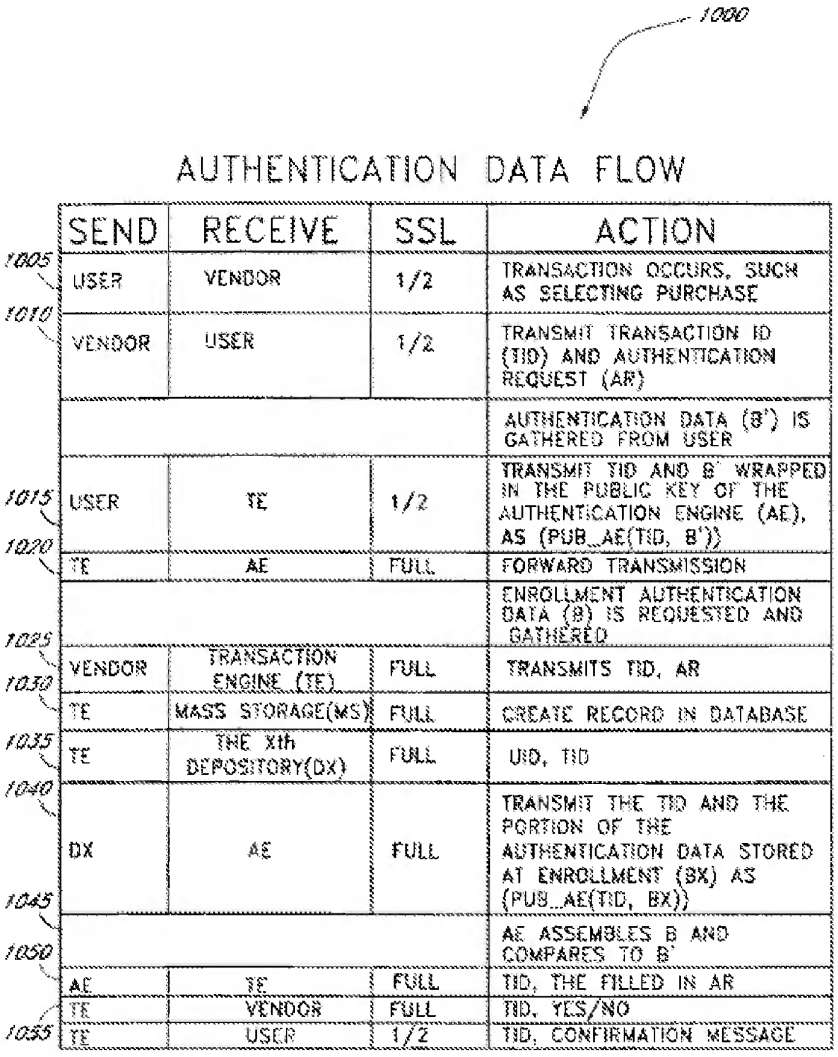


Figure 10



SEND	RECEIVE	SSL	ACTION
USER	VENDOR	1/2	TRANSACTION OCCURS, SUCH AS SELECTING PURCHASE
VENDOR	USER	1/2	TRANSMIT TRANSACTION ID (TID) AND AUTHENTICATION REQUEST (AR)
			AUTHENTICATION DATA (B') IS GATHERED FROM USER
USER	TE	1/2	TRANSMIT TID AND B' WRAPPED IN THE PUBLIC KEY OF THE AUTHENTICATION ENGINE (AE), AS (PUB_AE(TID, B'))
TE	AE	FULL	FORWARD TRANSMISSION
			ENROLLMENT AUTHENTICATION DATA (B) IS REQUESTED AND GATHERED
VENDOR	TRANSACTION ENGINE (TE)	FULL	TRANSMITS TID, AR
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))
			AE ASSEMBLES B AND COMPARES TO B'
AE	TE	FULL	TID, THE FILLED IN AR
TE	VENDOR	FULL	TID, YES/NO
TE	USER	1/2	TID, CONFIRMATION MESSAGE

Figure 11

1100

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 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 CRYPTOGRAPHIC 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

Figure 12

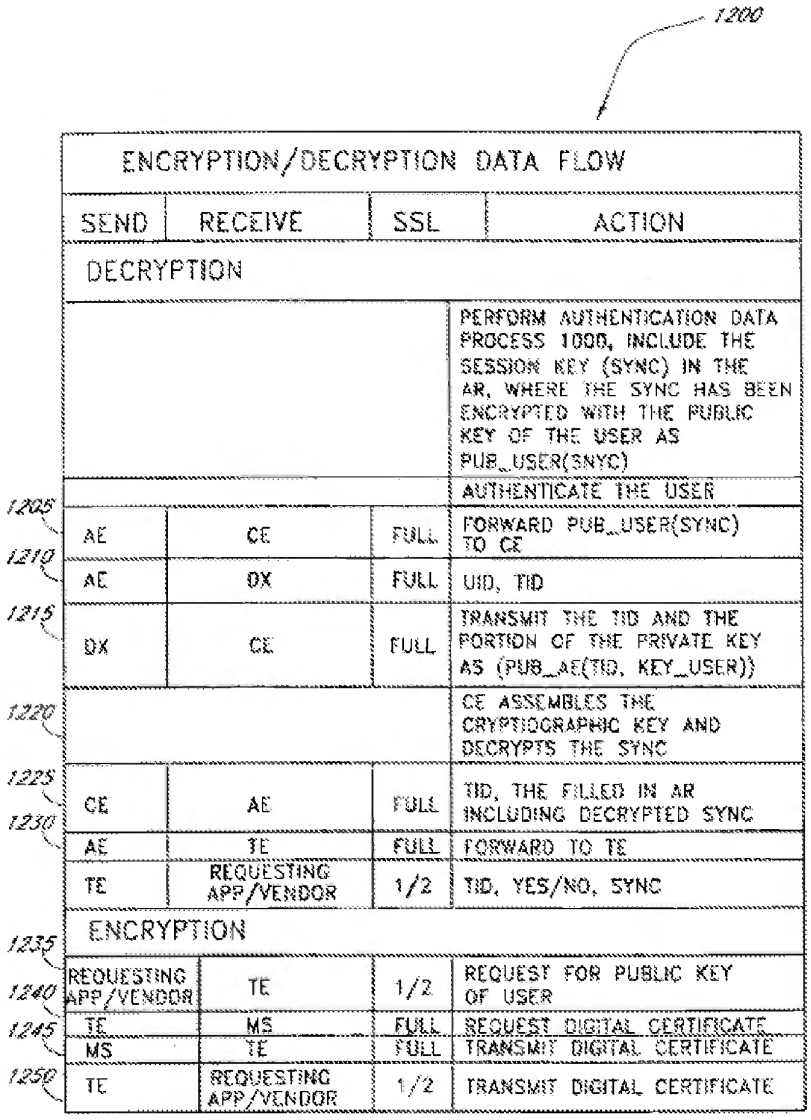

1200
ENCRYPTION/DECRYPTION DATA FLOW
SEND
RECEIVE
SSL
ACTION
DECRYPTION
PERFORM AUTHENTICATION DATA PROCESS 1000, INCLUDE THE SESSION KEY (SYNC) IN THE AR, WHERE THE SYNC HAS BEEN ENCRYPTED WITH THE PUBLIC KEY OF THE USER AS PUB_USER(SNYC)
AUTHENTICATE THE USER
1205
AE
CE
FULL
FORWARD PUB_USER(SYNC) 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 CRYPTIOGRAPHIC 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

Figure 13

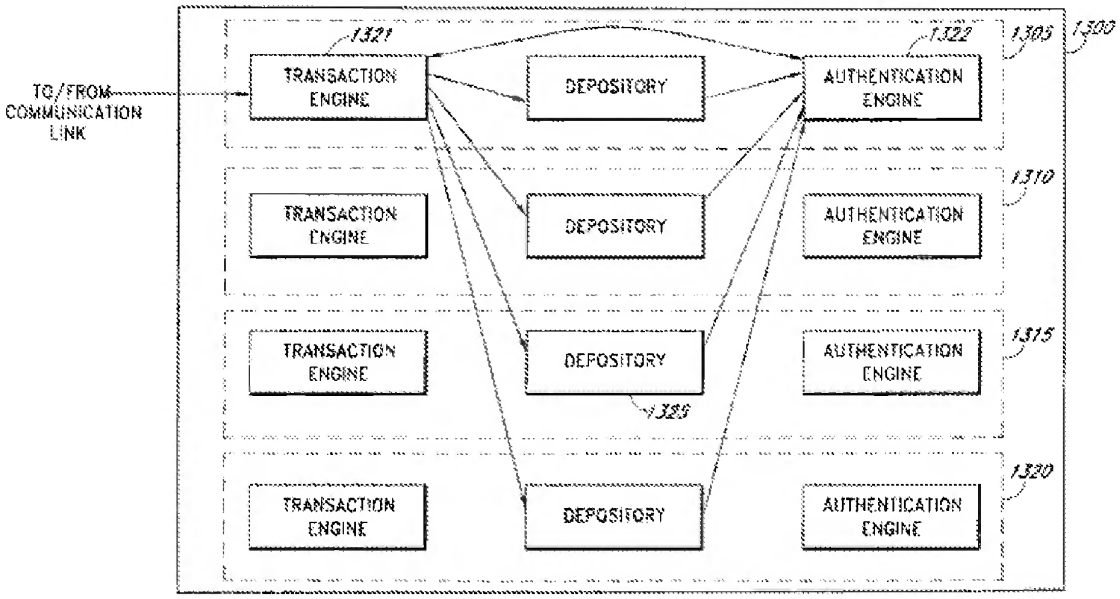

TO/FROM COMMUNICATION LINK
1321
TRANSACTION ENGINE
DEPOSITORY
1322
AUTHENTICATION ENGINE
1305
1300
TRANSACTION ENGINE
DEPOSITORY
AUTHENTICATION ENGINE
1310
TRANSACTION ENGINE
DEPOSITORY
1355
AUTHENTICATION ENGINE
1315
TRANSACTION ENGINE
DEPOSITORY
AUTHENTICATION ENGINE
1330

Figure 14

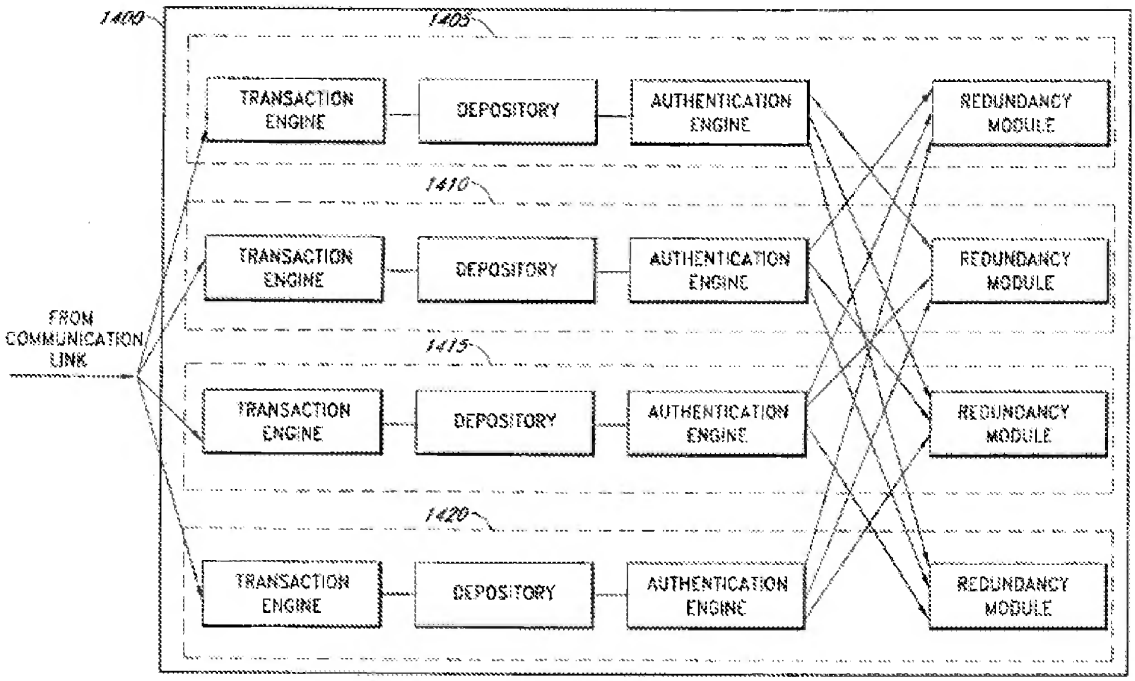

1400
1405
TRANSACTION ENGINE
DEPOSITORY
AUTHENTICATION ENGINE
REDUNDANCY MODULE
1410
TRANSACTION ENGINE
DEPOSITORY
AUTHENTICATION ENGINE
REDUNDANCY MODULE
FROM COMMUNICATION LINK
1415
TRANSACTION ENGINE
DEPOSITORY
AUTHENTICATION ENGINE
REDUNDANCY MODULE
1420
TRANSACTION ENGINE
DEPOSITORY
AUTHENTICATION ENGINE
REDUNDANCY MODULE

Figure 15

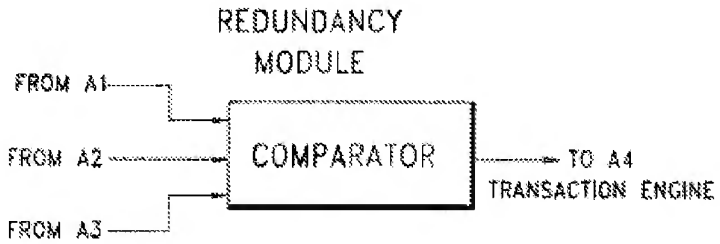

REDUNDANCY
MODULE
FROM A1
FROM A2
FROM A3
COMPARATOR
TO A4
TRANSACTION ENGINE

Figure 16

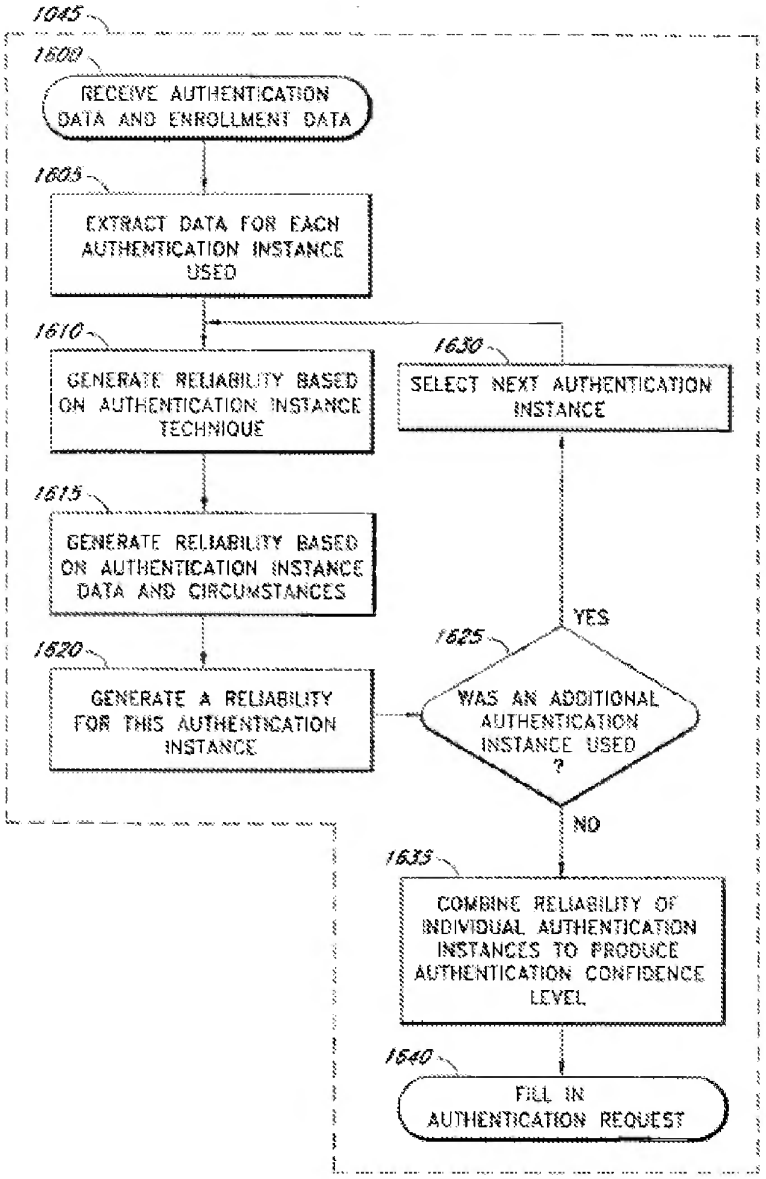

1045
1600
RECEIVE AUTHENTICATION DATA AND ENROLLMENT DATA
1605
EXTRACT DATA FOR EACH AUTHENTICATION INSTANCE USED
1610
GENERATE RELIABILITY BASED ON AUTHENTICATION INSTANCE TECHNIQUE
1615
GENERATE RELIABILITY BASED ON AUTHENTICATION INSTANCE DATA AND CIRCUMSTANCES
1620
GENERATE A RELIABILITY FOR THIS AUTHENTICATION INSTANCE
1625
WAS AN ADDITIONAL AUTHENTICATION INSTANCE USED ?
YES
NO
1630
SELECT NEXT AUTHENTICATION INSTANCE
1635
COMBINE RELIABILITY OF INDIVIDUAL AUTHENTICATION INSTANCES TO PRODUCE AUTHENTICATION CONFIDENCE LEVEL
1640
FILL IN AUTHENTICATION REQUEST

Figure 17

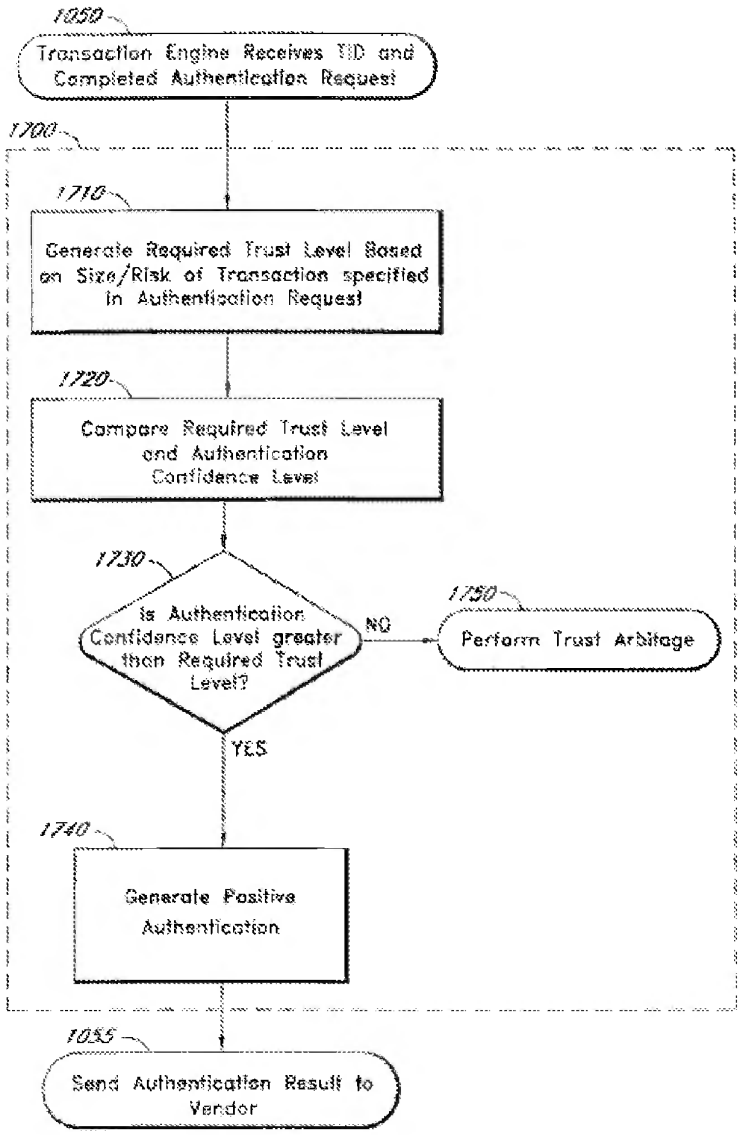

1050
Transaction Engine Receives TID and Completed Authentication Request
1700
1710
Generate Required Trust Level Based on Size/Risk of Transaction specified in Authentication Request
1720
Compare Required Trust Level and Authentication Confidence Level
1730
Is Authentication Confidence Level greater than Required Trust Level?
NO
1750
Perform Trust Arbitage
YES
1740
Generate Positive Authentication
1055
Send Authentication Result to Vendor

Figure 18

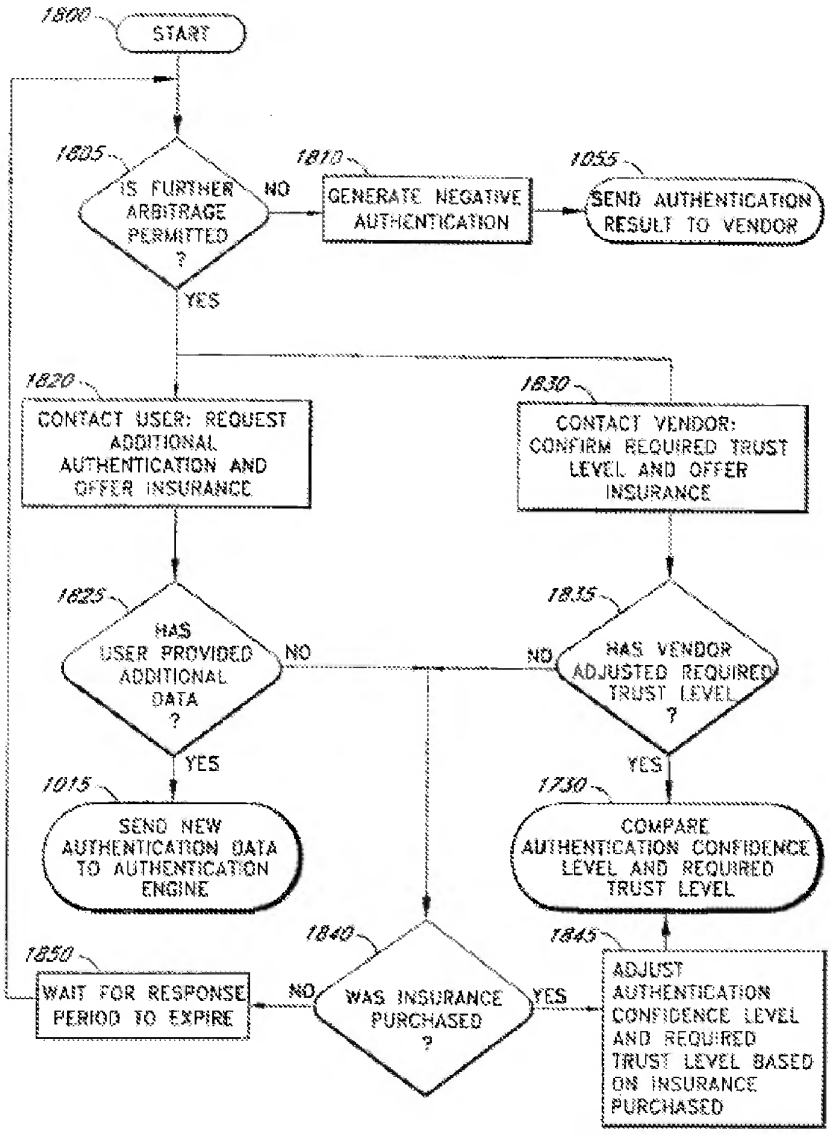

1800
START
1805
IS FURTHER ARBITRAGE PERMITTED ?
NO
1810
GENERATE NEGATIVE AUTHENTICATION
1055
SEND AUTHENTICATION RESULT TO VENDOR
YES
1820
CONTACT USER: REQUEST ADDITIONAL AUTHENTICATION AND OFFER INSURANCE
1830
CONTACT VENDOR: CONFIRM REQUIRED TRUST LEVEL AND OFFER INSURANCE
1825
HAS USER PROVIDED ADDITIONAL DATA ?
NO
1835
HAS VENDOR ADJUSTED REQUIRED TRUST LEVEL ?
NO
YES
YES
1015
SEND NEW AUTHENTICATION DATA TO AUTHENTICATION ENGINE
1730
COMPARE AUTHENTICATION CONFIDENCE LEVEL AND REQUIRED TRUST LEVEL
1840
WAS INSURANCE PURCHASED ?
NO
YES
1845
ADJUST AUTHENTICATION CONFIDENCE LEVEL AND REQUIRED TRUST LEVEL BASED ON INSURANCE PURCHASED
1850
WAIT FOR RESPONSE PERIOD TO EXPIRE

Figure 19

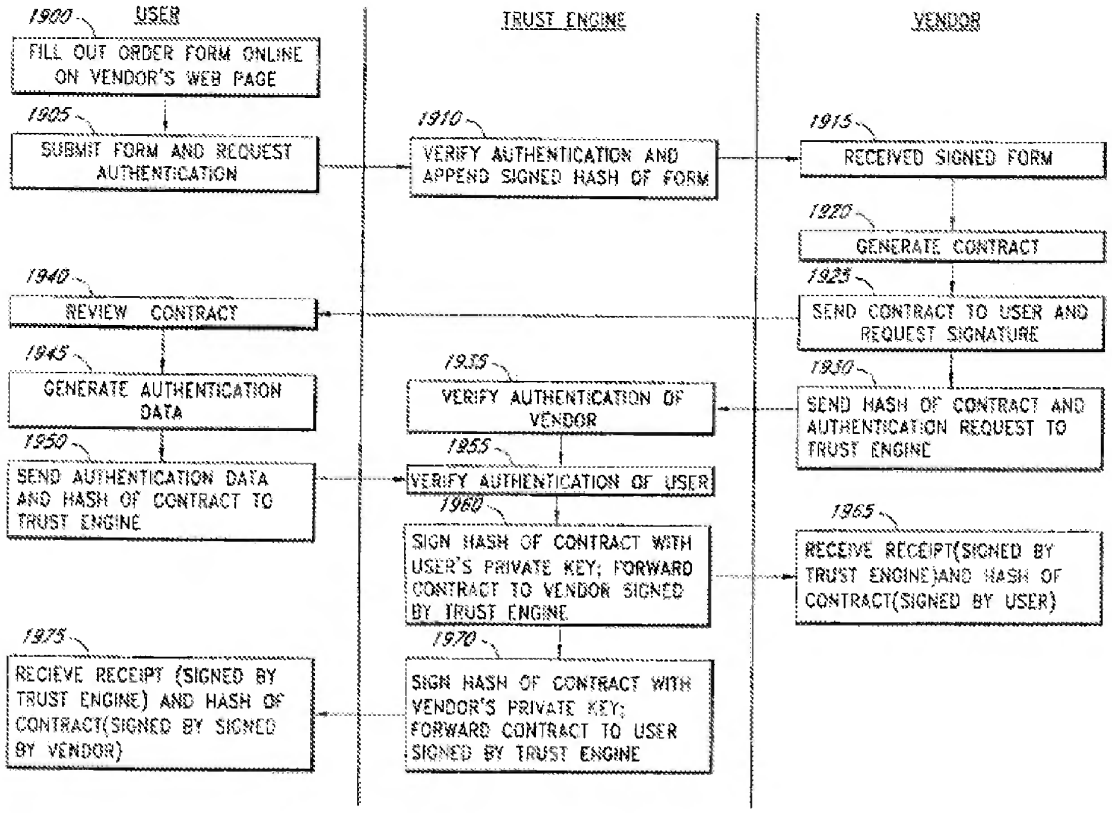

USER
TRUST ENGINE
VENDOR
1900
FILL OUT ORDER FORM ONLINE ON VENDOR'S WEB PAGE
1905
SUBMIT FORM AND REQUEST AUTHENTICATION
1910
VERIFY AUTHENTICATION AND APPEND SIGNED HASH OF FORM
1915
RECEIVED SIGNED FORM
1920
GENERATE CONTRACT
1925
SEND CONTRACT TO USER AND REQUEST SIGNATURE
1930
SEND HASH OF CONTRACT AND AUTHENTICATION REQUEST TO TRUST ENGINE
1935
VERIFY AUTHENTICATION OF VENDOR
1940
REVIEW CONTRACT
1945
GENERATE AUTHENTICATION DATA
1950
SEND AUTHENTICATION DATA AND HASH OF CONTRACT TO TRUST ENGINE
1955
VERIFY AUTHENTICATION OF USER
1960
SIGN HASH OF CONTRACT WITH USER'S PRIVATE KEY; FORWARD CONTRACT TO VENDOR SIGNED BY TRUST ENGINE
1965
RECEIVE RECEIPT(SIGNED BY TRUST ENGINE)AND HASH OF CONTRACT(SIGNED BY USER)
1970
SIGN HASH OF CONTRACT WITH VENDOR'S PRIVATE KEY; FORWARD CONTRACT TO USER SIGNED BY TRUST ENGINE
1975
RECIEVE RECEIPT (SIGNED BY TRUST ENGINE) AND HASH OF CONTRACT(SIGNED BY SIGNED BY VENDOR)

Figure 20

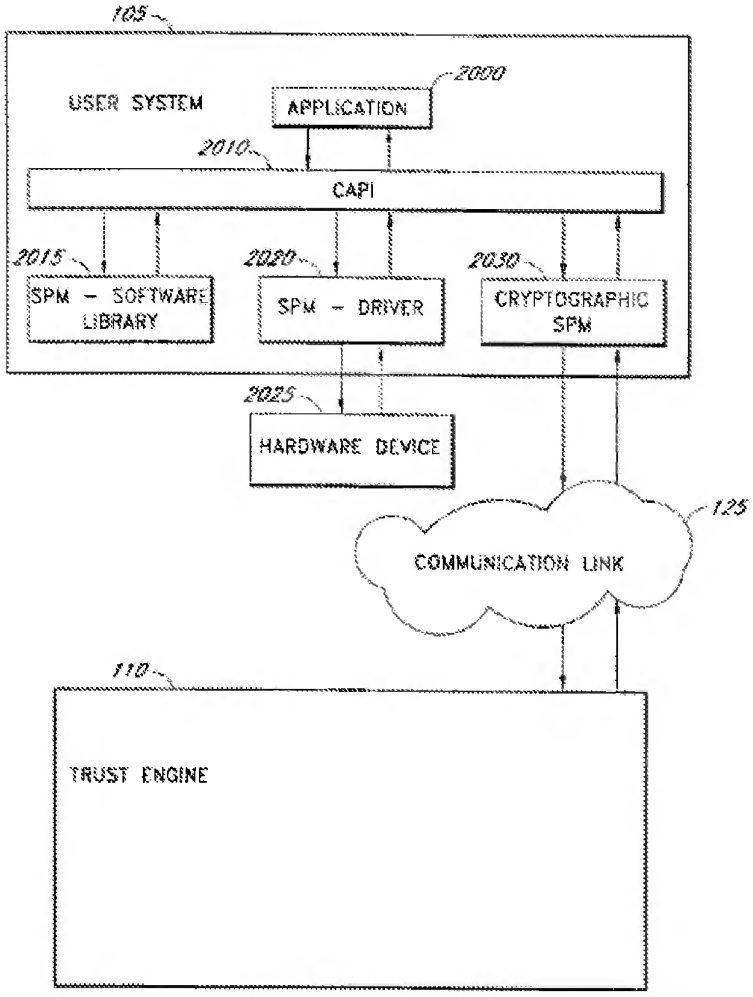

105
USER SYSTEM
APPLICATION
2000
2010
CAPI
2015
SPM – SOFTWARE LIBRARY
2020
SPM – DRIVER
2030
CRYPTOGRAPHIC SPM
2025
HARDWARE DEVICE
125
COMMUNICATION LINK
110
TRUST ENGINE

Figure 21

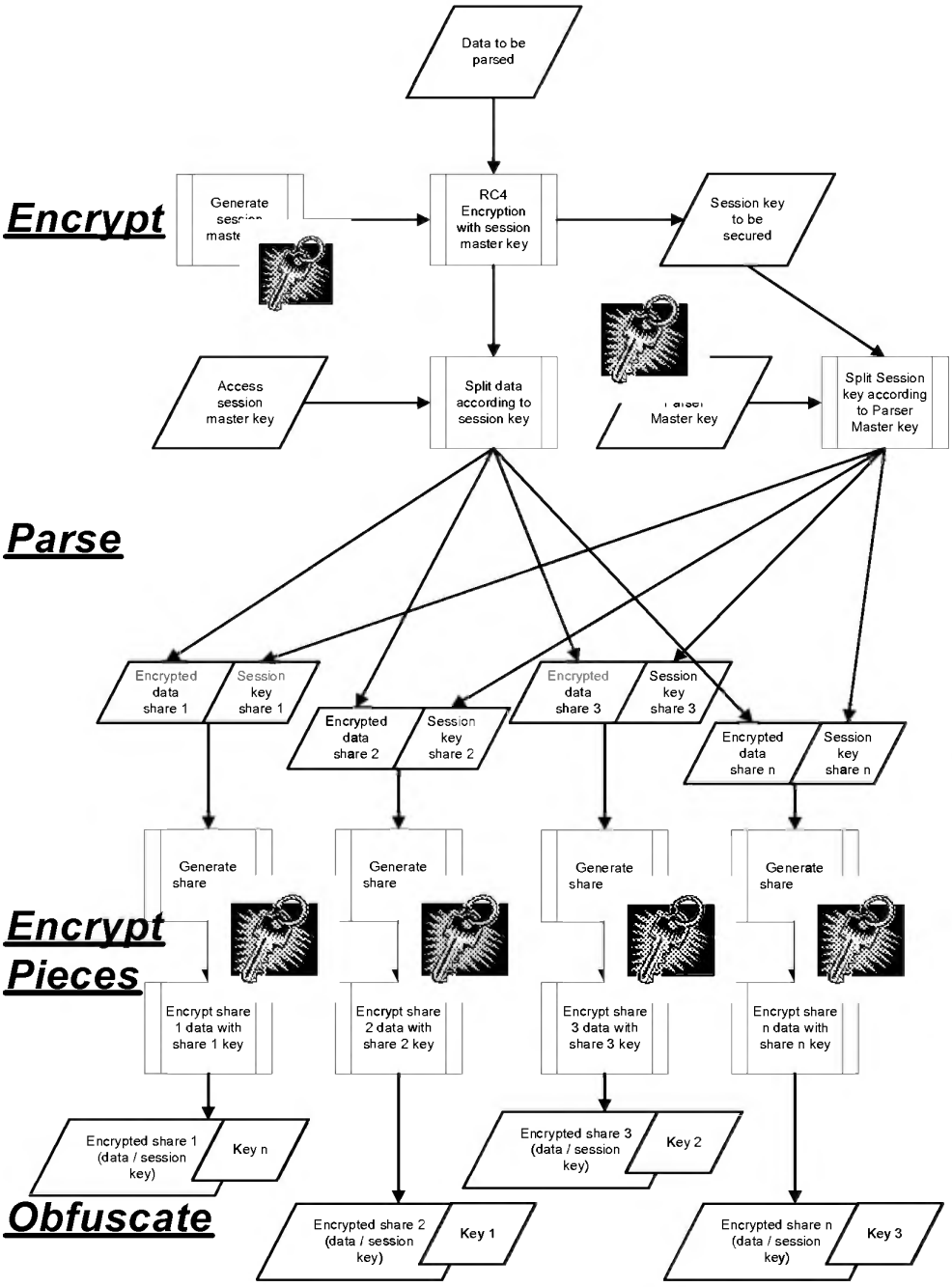

Data to be parsed
Encrypt
Generate
RC4 Encryption with session master key
Session key to be secured
Access session master key
Split data according to session key
Master key
Split Session key according to Parser Master key
Parse
Encrypted data share 1
Session key share 1
Encrypted data share 2
Session key share 2
Encrypted data share 3
Session key share 3
Encrypted data share n
Session key share n
Generate share
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

Figure 22

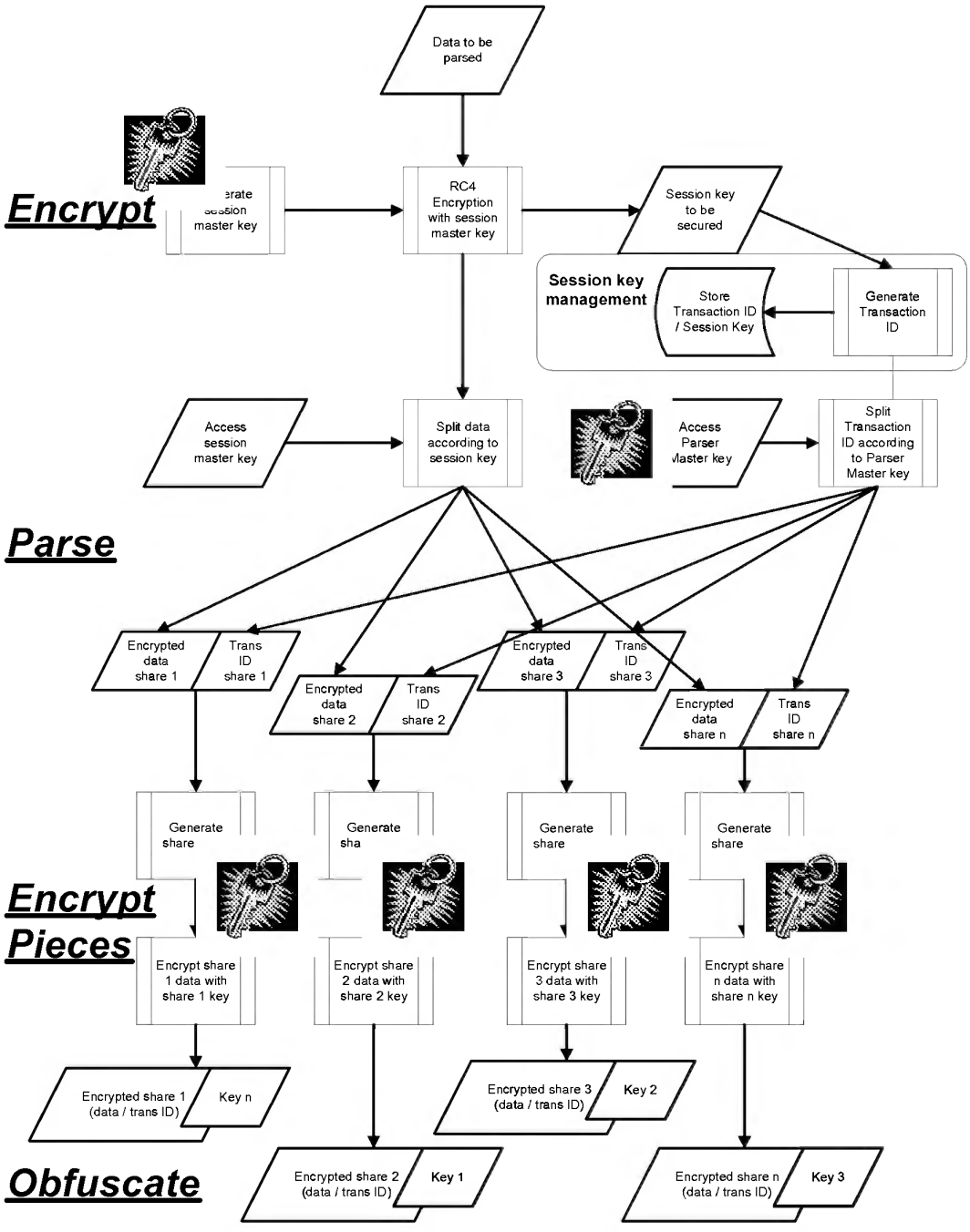

Data to be parsed
Encrypt
erate session master key
RC4 Encryption with session master key
Session key to be secured
Session key management
Store Transaction ID / Session Key
Generate Transaction ID
Access session master key
Split data according to session key
Access Parser Master key
Split Transaction 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
Generate sha
Generate share
Generate share
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

Figure 23

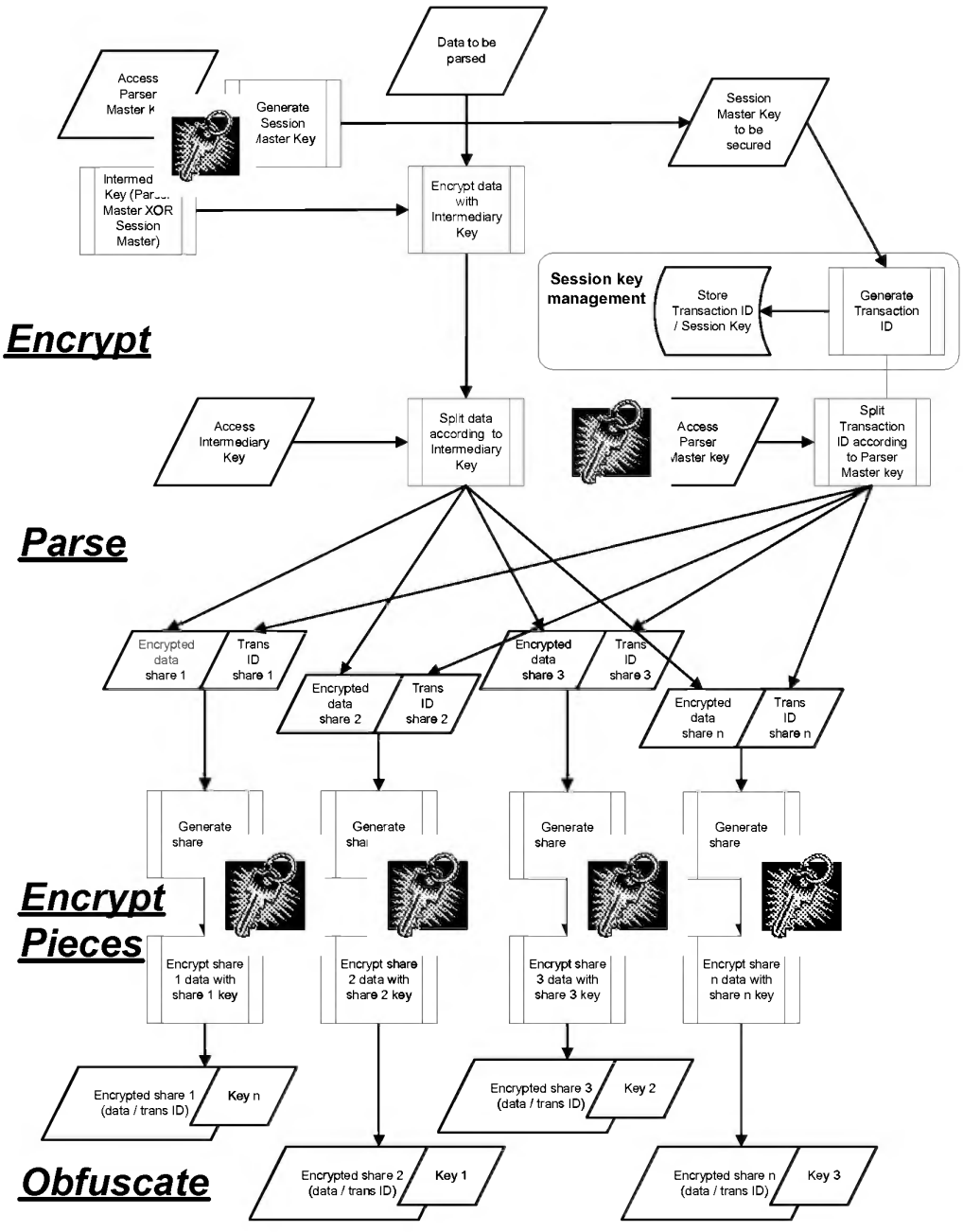

Data to be parsed
Access Parser Master K
Generate Session Master Key
Session Master Key to be secured
Intermed Key (Par... Master XOR Session Master)
Encrypt data with Intermediary Key
Session key management
Store Transaction ID / Session Key
Generate Transaction ID
Encrypt
Access Intermediary Key
Split 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
Generate shar
Generate share
Generate share
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

Figure 24

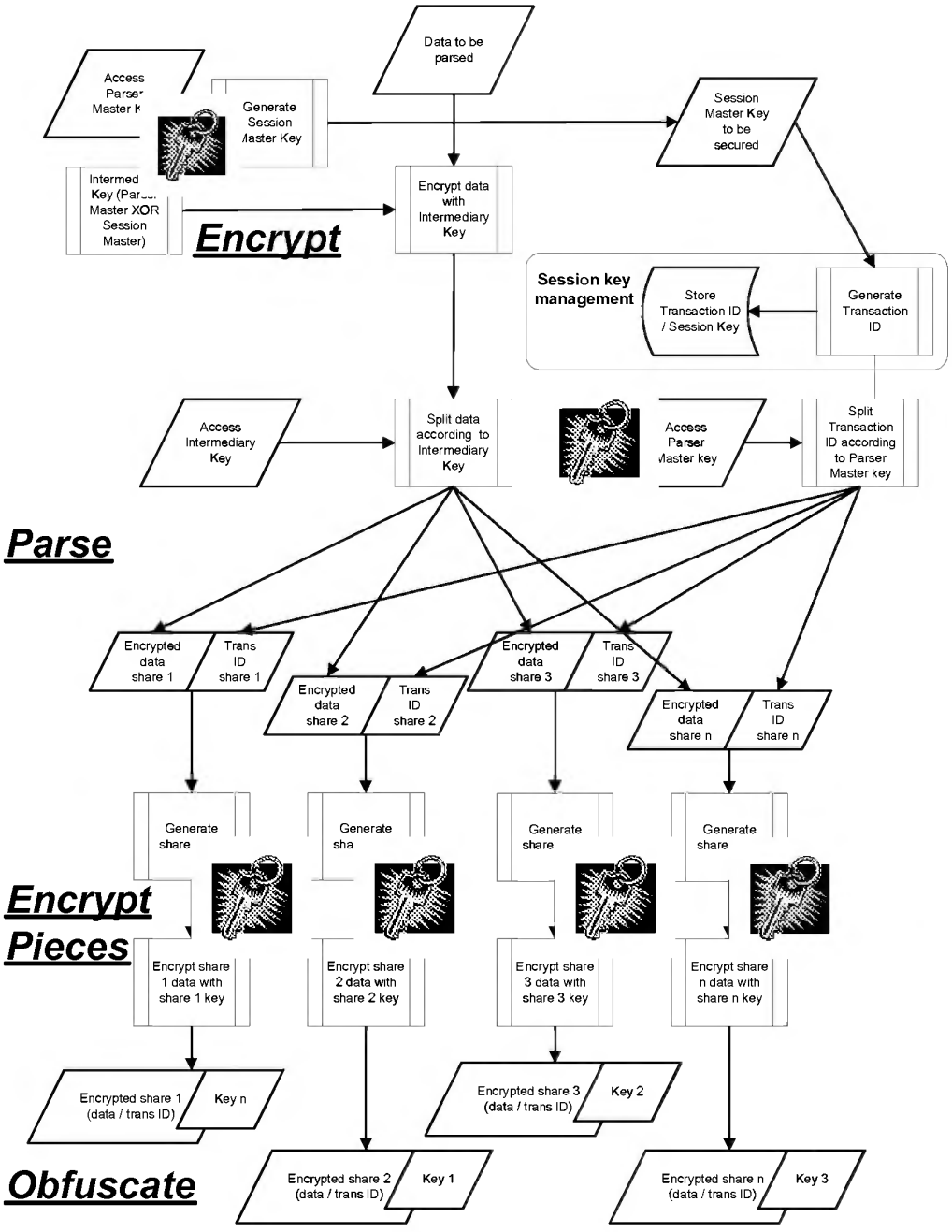
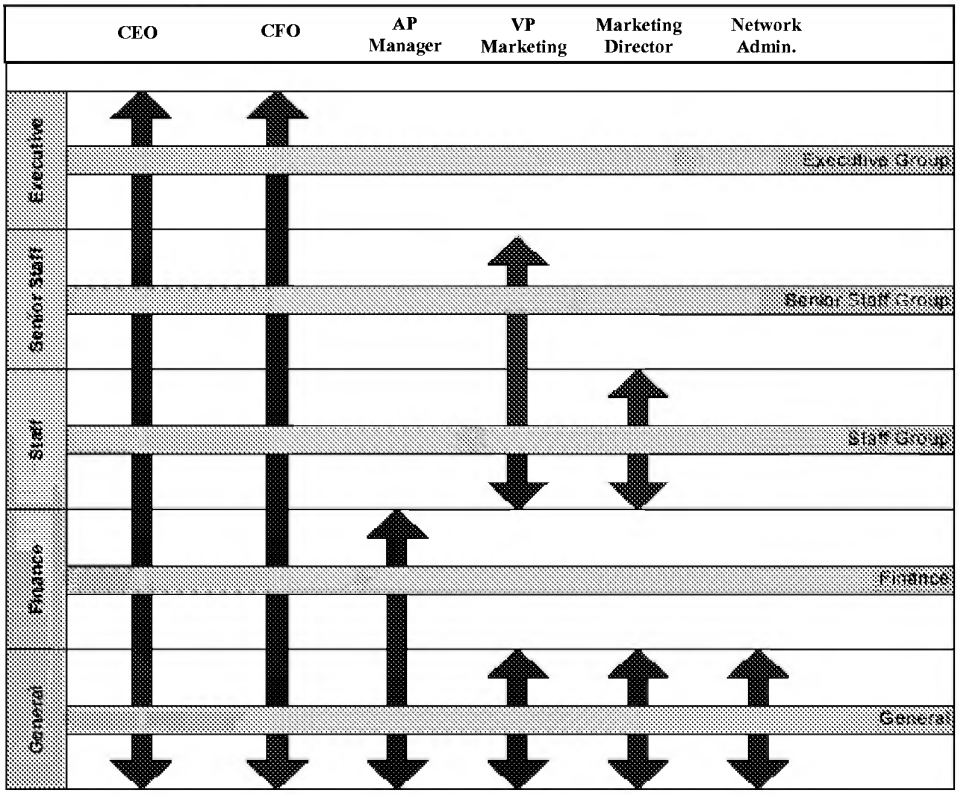

Data to be parsed
Access Parser Master k
Generate Session Master Key
Session Master Key to be secured
Intermed Key (Par... Master XOR Session Master)
Encrypt data with Intermediary Key
Encrypt
Session key management
Store Transaction ID / Session Key
Generate Transaction ID
Access Intermediary Key
Split 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
Generate sha
Generate share
Generate share
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

Figure 25


CEO
CFO
AP Manager
VP Marketing
Marketing Director
Network Admin.
Executive
Senior Staff
Staff
Finance
General
Executive Group
Senior Staff Group
Staff Group
Finance
General

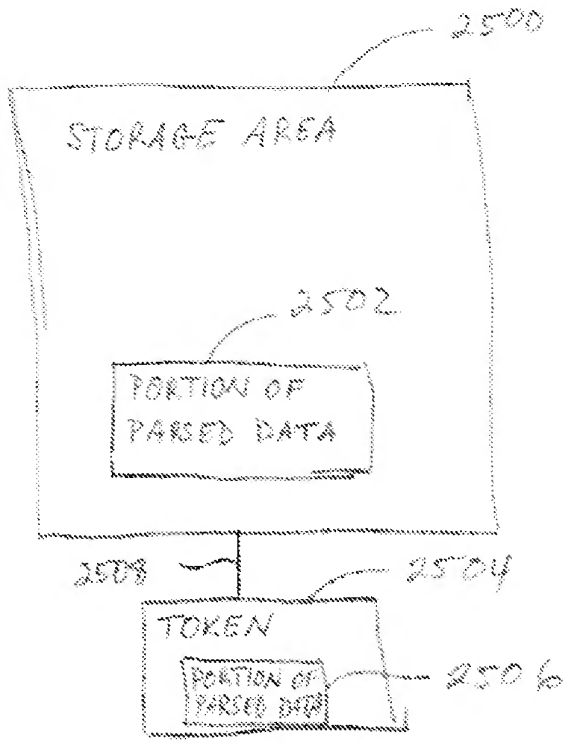

2500
STORAGE AREA
2502
PORTION OF PARSED DATA
2508
2504
TOKEN
PORTION OF PARSED DATA
2506

FIGURE 26

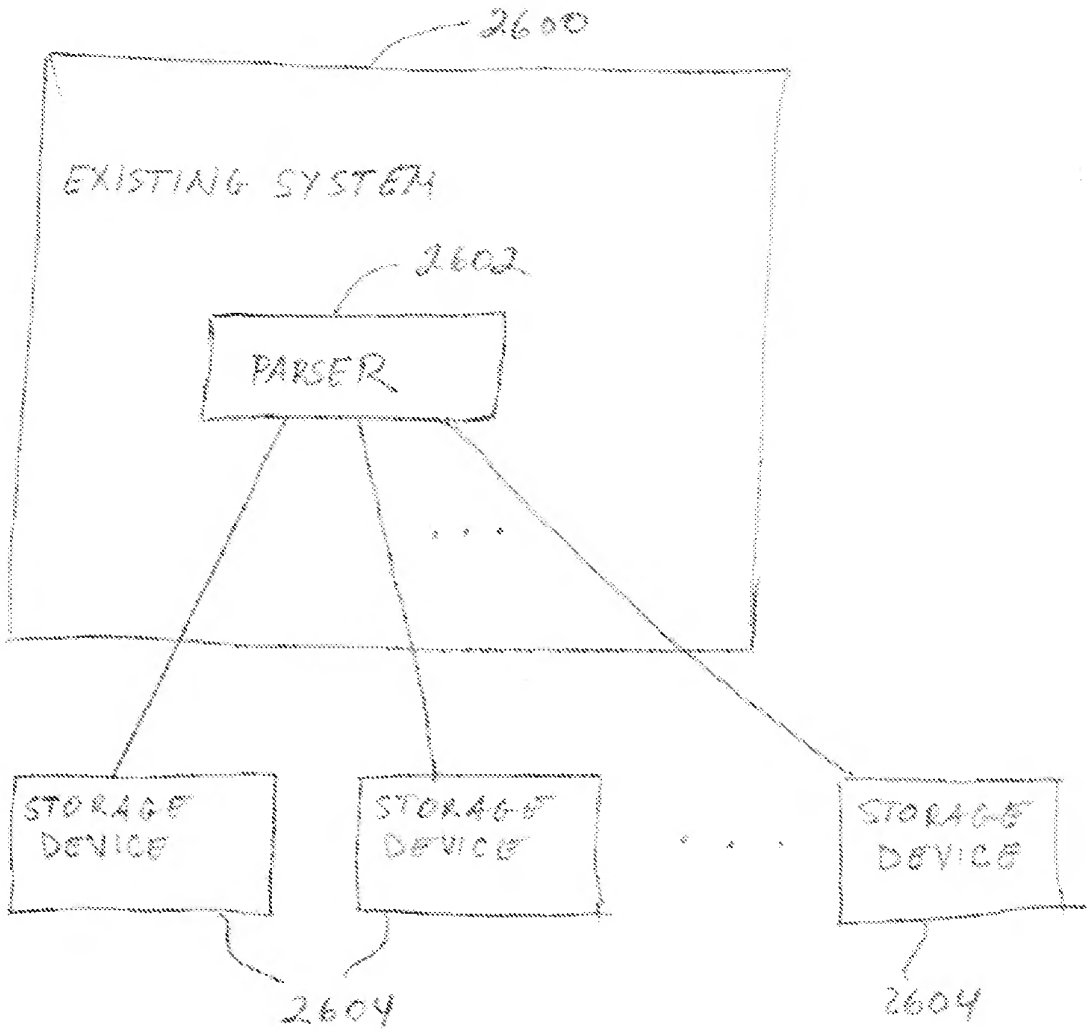

2600
EXISTING SYSTEM
2602
PARSER
STORAGE DEVICE
STORAGE DEVICE
STORAGE DEVICE
2604
2604

FIGURE 27

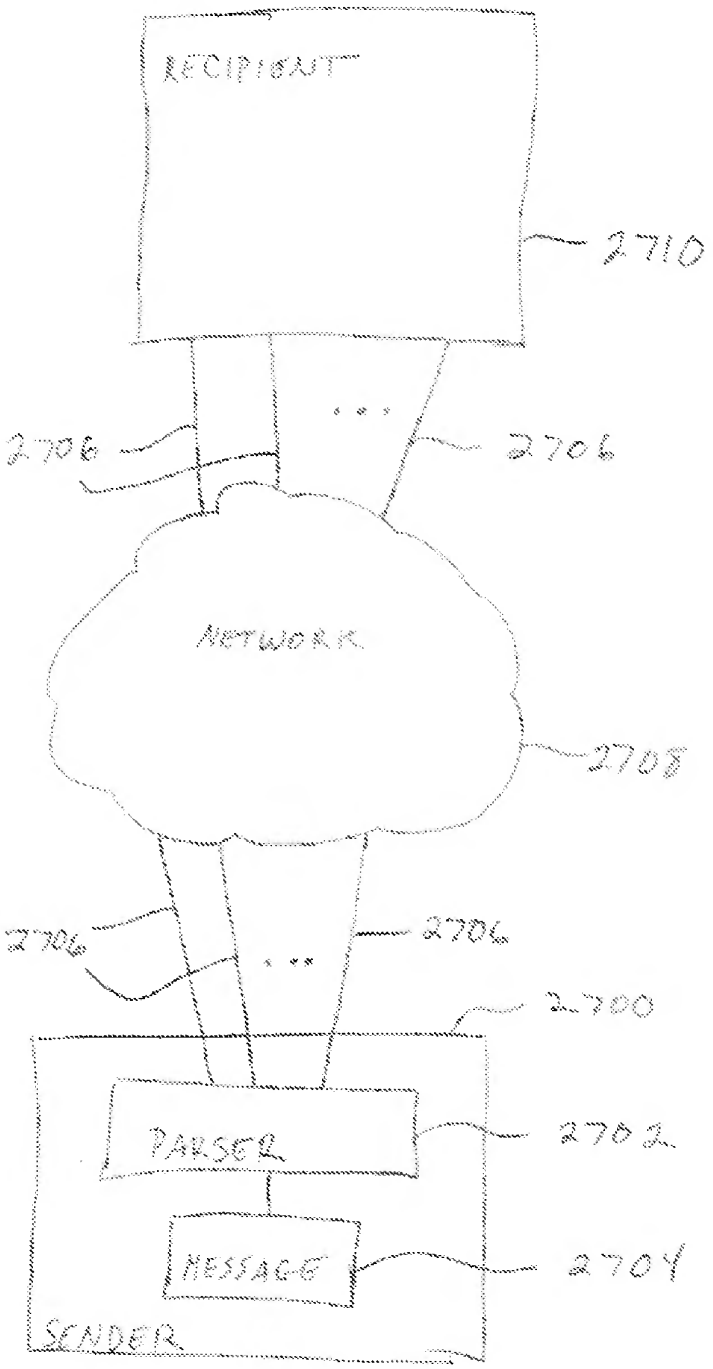

RECIPIENT
2710
2706
2706
NETWORK
2708
2706
2706
2700
PARSER
2702
MESSAGE
2704
SENDER

FIGURE 28

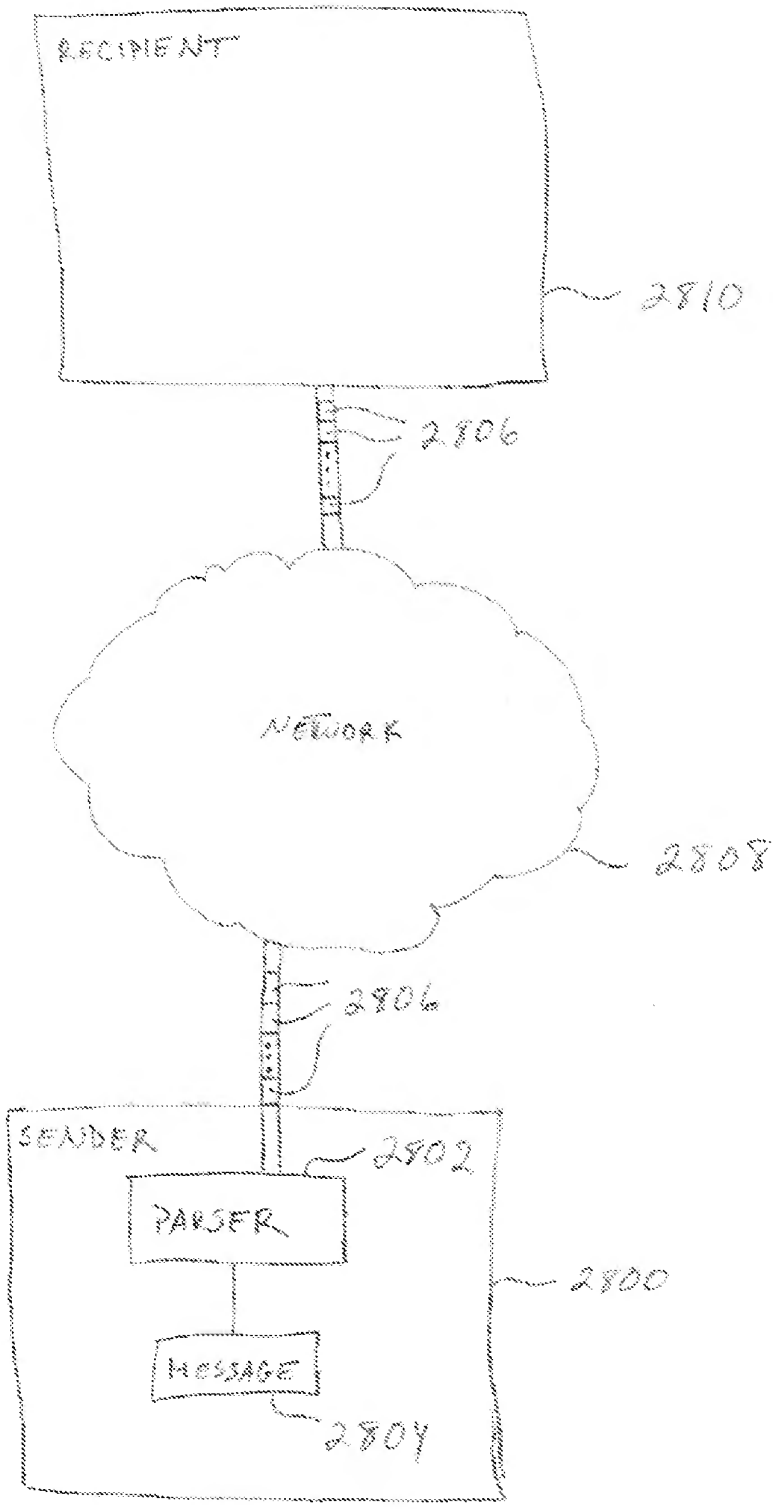
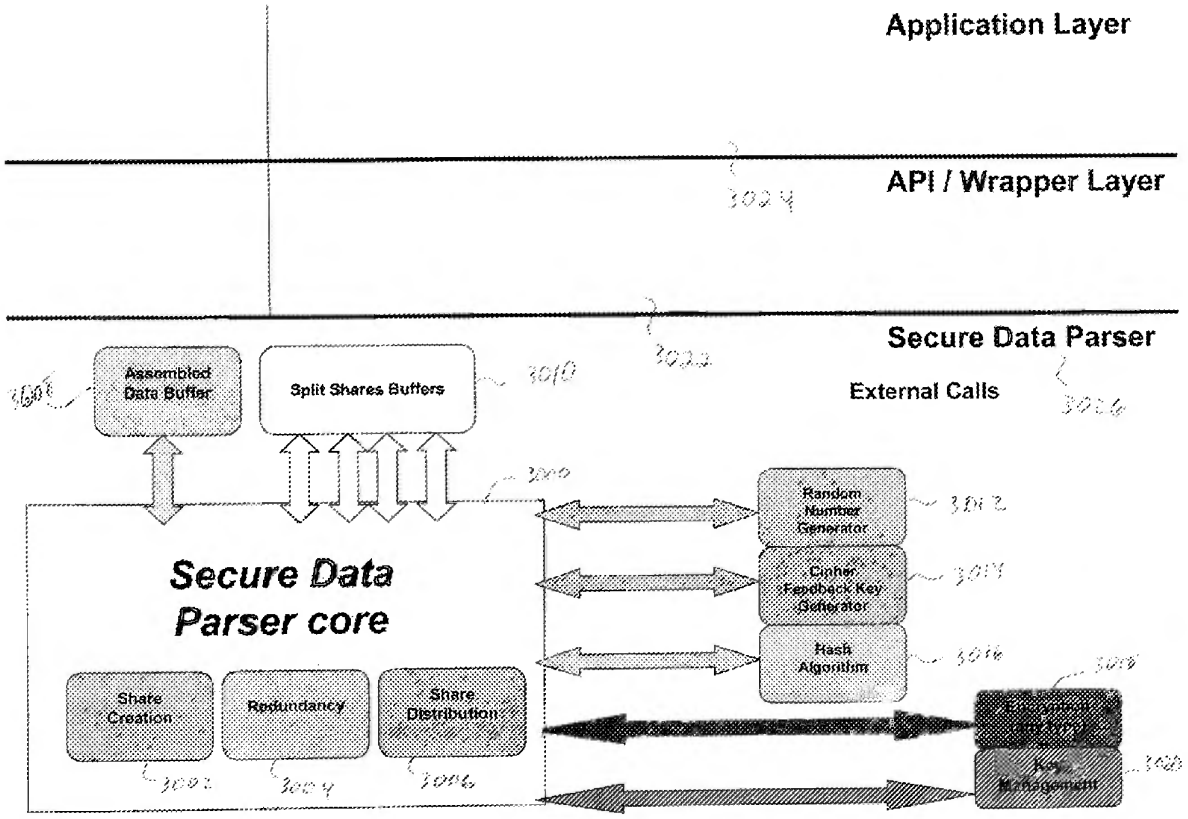

RECIPIENT
2810
2806
NETWORK
2808
2806
SENDER
2802
PARSER
2800
MESSAGE
2804

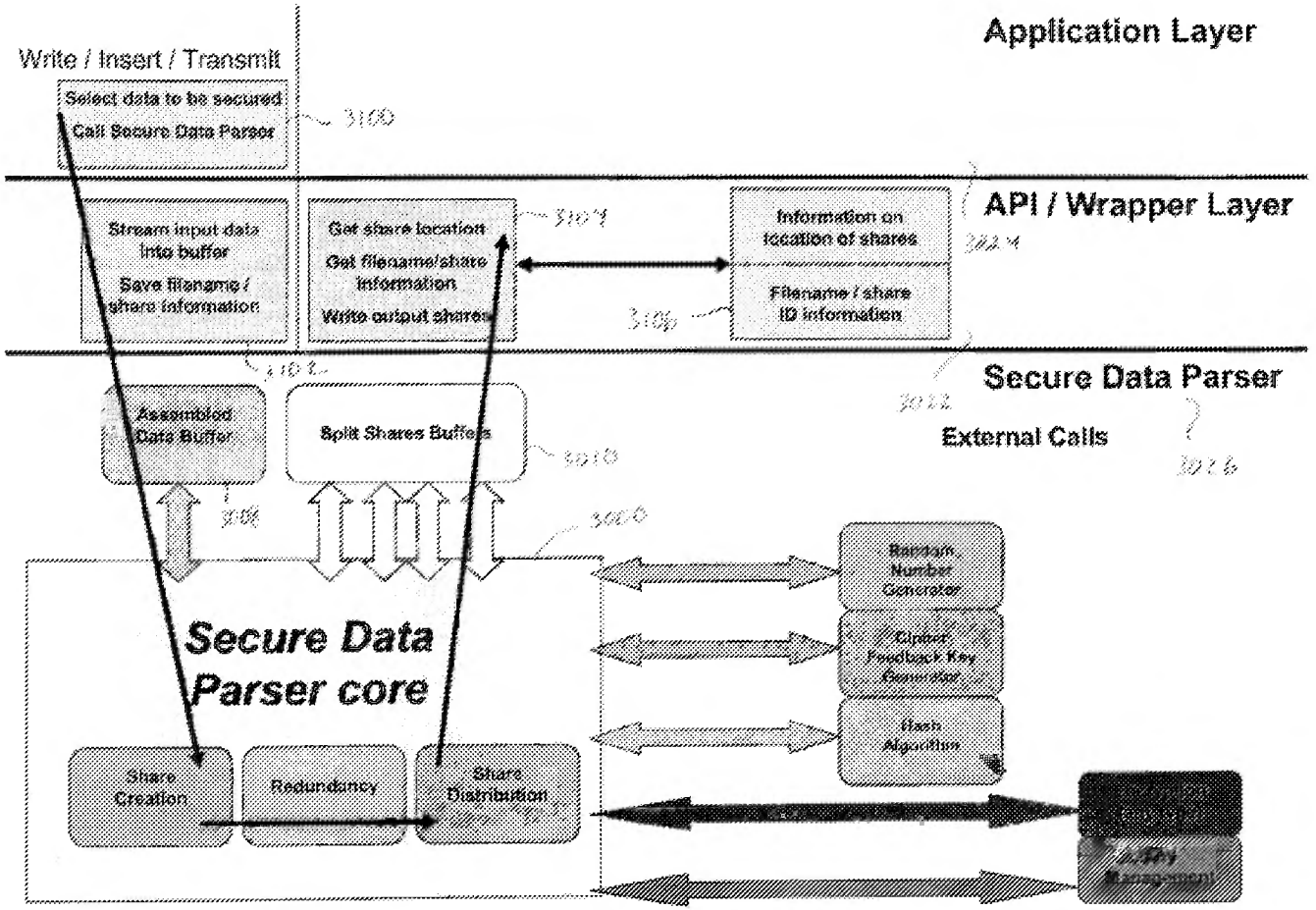
FIGURE 29



Interface to the SecureParser is facilitated by the creation of an API / Wrapper Layer between the Application and the Parser

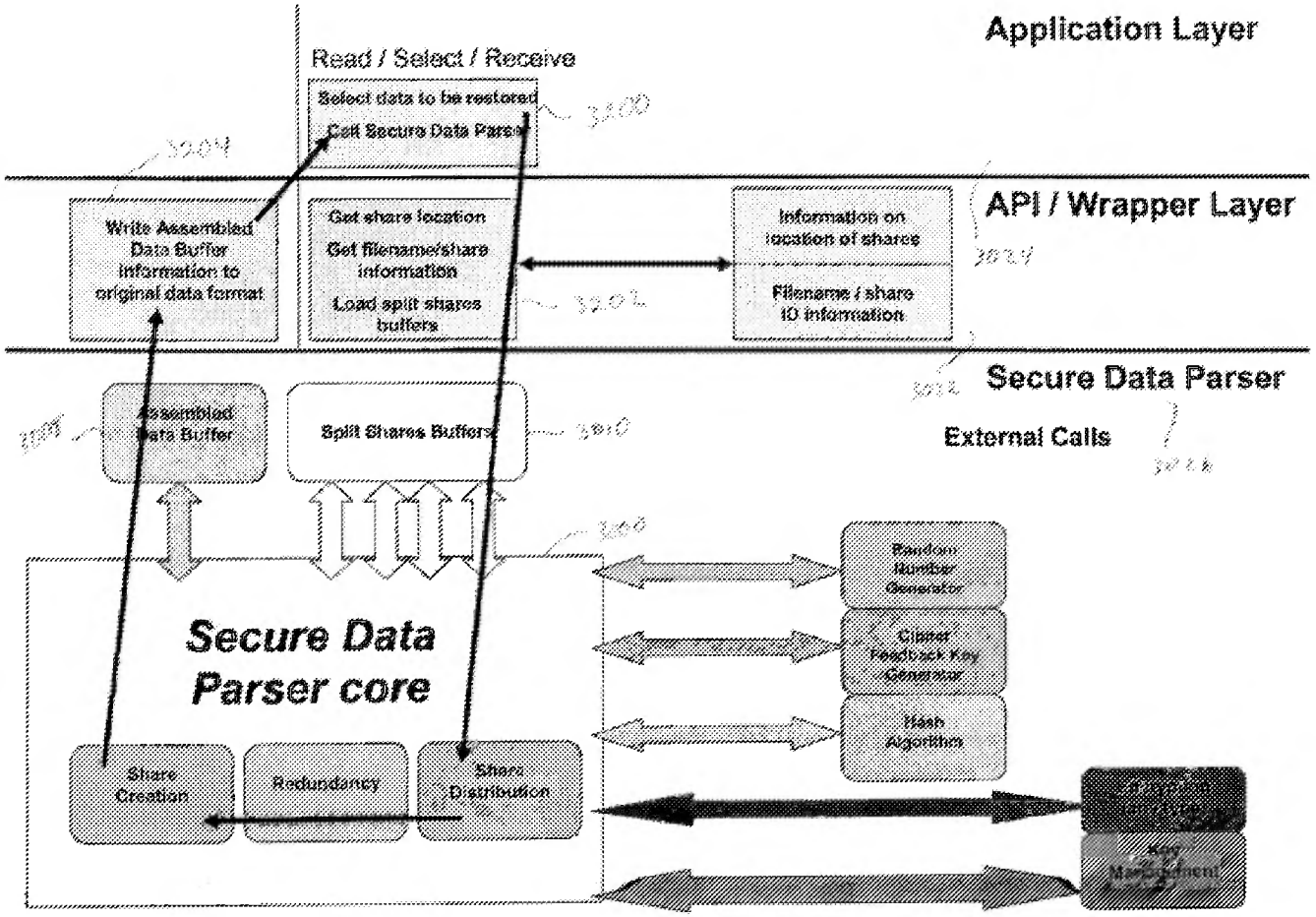
FIGURE 30

EX1009, Page 74



The API layer handles streaming of the data to the SecureParser and secure storage of the resulting shares

FIGURE 31



For retrieval of information, the host application identifies the data to be restored and invokes the Secure Data Parser API

FIGURE 32

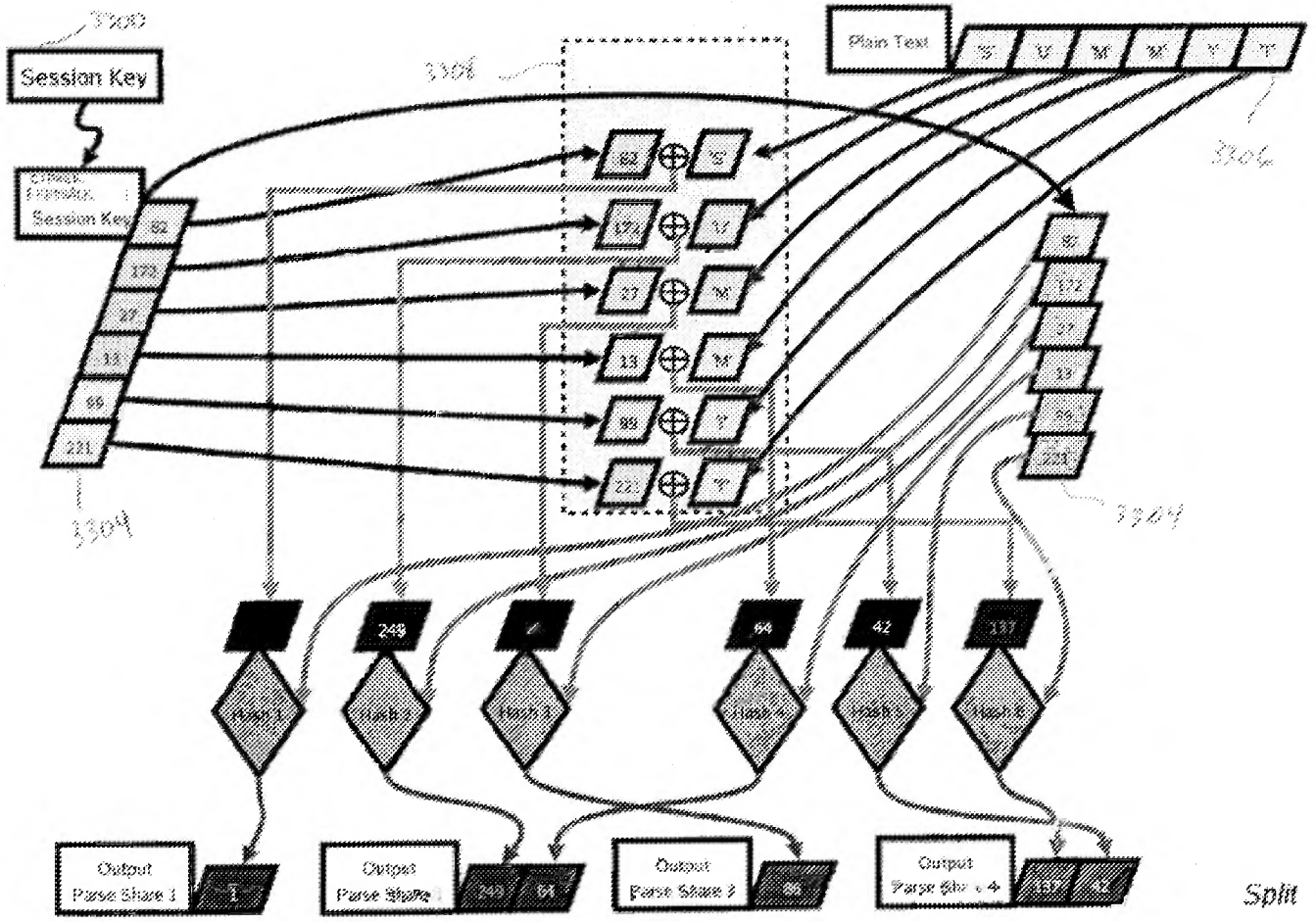


FIGURE 33

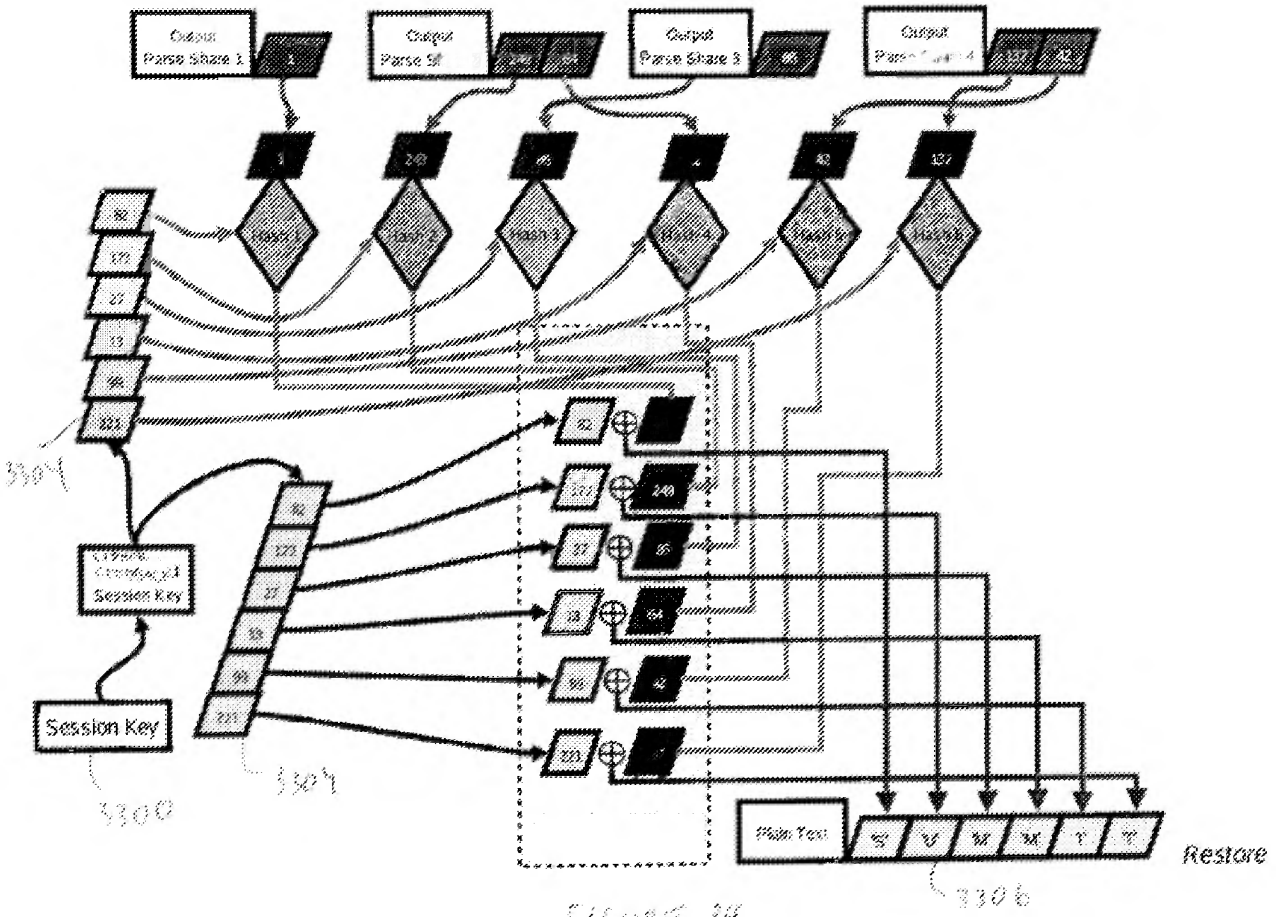


FIGURE 3F

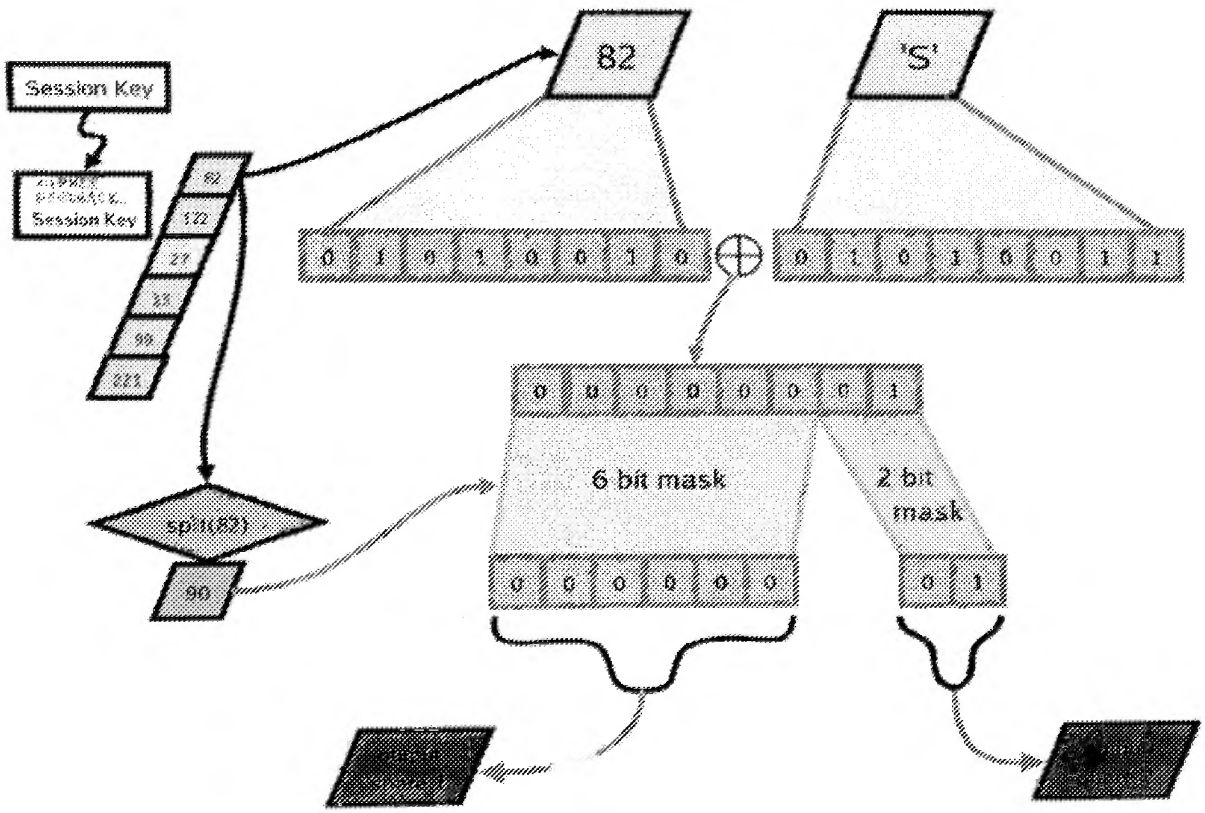

Session Key
Session Key
82
122
27
33
99
221
82
'S'
0 1 0 1 0 0 1 0
0 1 0 1 0 0 1 1
0 0 0 0 0 0 0 1
6 bit mask
2 bit mask
0 0 0 0 0 0
0 1
sp-1(82)
90

FIGURE 35

PTO/SB/05 (08-08)
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.

UTILITY PATENT APPLICATION TRANSMITTAL

(ONLY FOR NEW NONPROVISIONAL APPLICATIONS UNDER 37 CFR 1.53(B))

Attorney Docket No.	104093-0002-105
First Inventor	Rick L. Orsini
Title	SECURE DATA PARSER METHOD AND SYSTEM
Express Mail Label No.	

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

1. [ ] **Fee Transmittal Form** (e.g., PTO/SB/17)
2. [ ] **Applicant claims small entity status.** See 37 CFR 1.27.
3. [X] **Specification** [*Total Pages* 182]
   Both the claims and abstract must start on a new page
   (For information on the preferred arrangement, see MPEP 608.01(a))
4. [X] **Drawing(s)** *(35 U.S.C. 113)* [*Total Sheets* 36]
5. **Oath or Declaration** [*Total Sheets* 16]
   a. [ ] Newly executed (original or copy)
   b. [X] A copy from a prior application (37 CFR 1.63(d))
   (for continuation/divisional with Box 18 completed)
   i. [ ] DELETION OF INVENTOR(S)
   Signed statement attached deleting inventor(s) name in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
6. [X] **Application Data Sheet**. See 37 CFR 1.76
7. [ ] **CD-ROM or CD-R** in duplicate, large table or Computer Program *(Appendix)*
   [ ] Landscape Table on CD
8. **Nucleotide and/or Amino Acid Sequence Submission** *(if applicable, items a. – c. are required)*
   a. [ ] Computer Readable Form (CRF)
   b. Specification Sequence Listing on:
   i. [ ] CD-ROM or CD-R (2 copies); or ii. [ ] Paper
   c. [ ] Statements verifying identity of above copies

ADDRESS TO: **Commissioner for Patents**
P.O. Box 1450
Alexandria, VA 22313-1450

ACCOMPANYING APPLICATION PARTS

9. [ ] **Assignment Papers** (cover sheet & document(s))
   Name of Assignee
10. [X] **37 CFR 3.73(b) Statement** *(when there is an assignee)* [X] **Power of Attorney**
11. [ ] **English Translation Document** *(if applicable)*
12. [ ] **Information Disclosure Statement** (PTO/SB/08 or PTO-1449)
    [ ] Copies of citations attached
13. [ ] **Preliminary Amendment**
14. [ ] **Return Receipt Postcard** (MPEP 503) *(Should be specifically itemized)*
15. [ ] **Certified Copy of Priority Document(s)** *(if foreign priority is claimed)*
16. [ ] **Nonpublication Request** under 35 U.S.C.122 (b)(2)(B)(i). Applicant must attach form PTO/SB/35 or equivalent.
17. [X] Other: Certification and Request for Prioritized Examination (Track I)

18. If a CONTINUING APPLICATION, *check appropriate box, and supply the requisite information below and in the first sentence of the specification following the title, or in an Application Data Sheet under 37 CFR 1.76:*

[X] Continuation [ ] Divisional [ ] Continuation-in-part (CIP) of prior application No.: 11/258,839

Prior application information: Examiner Samson B. Lemma *Art Unit:* 2432

19. CORRESPONDENCE ADDRESS

[X] The address associated with Customer Number: 01473 **OR** [ ] Correspondence address below

Name					
Address					
City		State		Zip Code	
Country		Telephone		Email	

Signature	/Edward A. Gordon/	Date	February 10, 2012
Name (Print/Type)	Edward A. Gordon	Registration No. (Attorney/Agent)	54,130

29533381_1

SECURE DATA PARSER METHOD AND SYSTEM

Cross-reference to Related Applications

[0001] This is a continuation of U.S. Patent Application No. 11/258,839, filed October 25, 2005, which claims the benefit of 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, all of which 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, wirless, 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 diamgram 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.

Detailed Description of the Invention

[0068] 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.

[0069] 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.

[0070] 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.

[0071] 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.

[0072] 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.

[0073] 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.

[0074] 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.

[0075] 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.

[0076] 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.

[0077] 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.

[0078] 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.

[0079] 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.

[0080] 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.

[0081] 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.

[0082] 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.

[0083] 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.

[0084] 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.

[0085] 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.

[0086] 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.

[0087] 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.

[0088] 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.

[0089] 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.

[0090] 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.

[0091] 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.

[0092] 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.

[0093] 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.

[0094] 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.

[0095] 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.

[0096] 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.

[0097] 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.

[0098] 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.

[0099] 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.

[0100] 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.

[0101] 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.

[0102] 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.

[0103] 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.

[0104] 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.

[0105] According to another embodiment, the depository 210 may comprise distinct and physically separated data storage facilities, as disclosed further with reference to FIGURE 7.

[0106] 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.

[0107] 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.

[0108] 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.

[0109] 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.

[0110] 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).

[0111] 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).

[0112] 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.

[0113] 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.

[0114] 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.

[0115] 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.

[0116] 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.

[0117] 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.

[0118] 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.

[0119] 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.

[0120] 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.

[0121] 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.

[0122] 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.

[0123] 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.

[0124] 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.

[0125] 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.

[0126] 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.

[0127] 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.

[0128] 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.

[0129] 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.

[0130] 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.

[0131] 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.

[0132] 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.

[0133] 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.

[0134] 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.

[0135] 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.

[0136] 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.

[0137] 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.

[0138] 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.

[0139] 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.

[0140] 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.

[0141] 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.

[0142] 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.

[0143] 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.

[0144] 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."

[0145] 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.

[0146] 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.

[0147] 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.

[0148] 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.

[0149] 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.

[0150] 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.

[0151] 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.

[0152] 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.

[0153] 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.

[0154] 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.

[0155] 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.

[0156] 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.

[0157] 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.

[0158] 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.

[0159] 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.

[0160] 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.

[0161] 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.

[0162] 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.

[0163] 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.

[0164] 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.

[0165] 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.

[0166] 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.

[0167] 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.

[0168] 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.

[0169] 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.

[0170] 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.

[0171] 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.

[0172] 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.

[0173] 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.

[0174] 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.

[0175] 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.

[0176] 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.

[0177] 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.

[0178] 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.

[0179] 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.

[0180] 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.

[0181] 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.

[0182] 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.

[0183] 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.

[0184] 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.

[0185] 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.

[0186] 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.

[0187] 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.

[0188] 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.

[0189] 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,

[0190] 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.

[0191] 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.

[0192] 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.

[0193] 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.

[0194] 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.

[0195] 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.

[0196] 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.

[0197] 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.

[0198] 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).

[0199] 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.

[0200] 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.

[0201] 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.

[0202] 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.

[0203] 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).

[0204] 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.

[0205] 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.).

[0206] 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.

[0207] 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.

[0208] 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.

[0209] 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.

[0210] 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.

[0211] 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.

[0212] 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.

[0213] 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.

[0214] 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.

[0215] 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.

[0216] 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.

[0217] 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.

[0218] 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.

[0219] 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.

[0220] 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.

[0221] 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.

[0222] 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.

[0223] 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.

[0224] 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.

[0225] 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.

[0226] 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.

[0227] 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.

[0228] 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.

[0229] 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.

[0230] 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.)

[0231] 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.

[0232] 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.)

[0233] 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%.

[0234] 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).

[0235] 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.

[0236] 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.

[0237] 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.

[0238] 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.

[0239] 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.

[0240] 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.

[0241] 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.

[0242] 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.

[0243] 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.

[0244] 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.

[0245] 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.

[0246] 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.

[0247] 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.

[0248] 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).

[0249] 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.

[0250] 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.

[0251] 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.

[0252] 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.

[0253] 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.

[0254] 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.

[0255] 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.

[0256] 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.

[0257] 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.

[0258] 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.

[0259] 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.

[0260] 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.

[0261] 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.

[0262] 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.

[0263] 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.

[0264] 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.

[0265] 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.

[0266] 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.

[0267] 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).

[0268] 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.

[0269] 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.

[0270] 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.

[0271] 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.

[0272] 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.

[0273] 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.

[0274] 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.

[0275] 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.

[0276] 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.

[0277] 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).

[0278] 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.

[0279] 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.

[0280] 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.

[0281] 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.

[0282] 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.

[0283] 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.

[0284] 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.

[0285] 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.

[0286] 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.

[0287] 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.

[0288] 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.

[0289] 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.

[0290] 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.

[0291] 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.

[0292] 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.

[0293] 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.

[0294] 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.

[0295] 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.

[0296] 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;
```

[0297] An example of one embodiment of source code that would perform the cryptosplitting RAID process described herein is:

[0298] 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.

[0299] 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.

[0300] 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.

[0301] 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.

[0302] 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:

[0303] 1. Generating a session master key and encrypt the data using RS1 stream cipher.

[0304] 2. Separating the resulting encrypted data into four shares or portions of parsed data according to the pattern of the session master key.

[0305] 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.

[0306] 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.

[0307] 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.

[0308] To restore the original data format, the steps are reversed.

[0309] 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.

[0310] 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:

[0311] 1. Generating a session master key and encrypt the data using RS1 stream cipher.

[0312] 2. Separating the resulting encrypted data into four shares or portions of parsed data according to the pattern of the session master key.

[0313] 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.

[0314] 4. The resulting four shares of data will contain encrypted portions of the original data and portions of the transaction ID.

[0315] 5. Generating a stream cipher key for each of the four data shares.

[0316] 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.

[0317] To restore the original data format, the steps are reversed.

[0318] 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.

[0319] 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:

[0320] 1. Accessing the parser master key associated with the authenticated user

[0321] 2. Generating a unique Session Master key

[0322] 3. Derive an Intermediary Key from an exclusive OR function of the Parser Master Key and Session Master key

[0323] 4. Optional encryption of the data using an existing or new encryption algorithm keyed with the Intermediary Key.

[0324] 5. Separating the resulting optionally encrypted data into four shares or portions of parsed data according to the pattern of the Intermediary key.

[0325] 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.

[0326] 7. The resulting multiple shares of data will contain optionally encrypted portions of the original data and portions of the session master key.

[0327] 8. Optionally generate an encryption key for each of the four data shares.

[0328] 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.

[0329] To restore the original data format, the steps are reversed.

[0330] 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.

[0331] 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:

[0332] 1. Accessing the Parser Master Key associated with the authenticated user

[0333] 2. Generating a unique Session Master Key

[0334] 3. Derive an Intermediary Key from an exclusive OR function of the Parser Master Key and Session Master key

[0335] 4. Optionally encrypt the data using an existing or new encryption algorithm keyed with the Intermediary Key.

[0336] 5. Separating the resulting optionally encrypted data into four shares or portions of parsed data according to the pattern of the Intermediary Key.

[0337] 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.

[0338] 7. The resulting four shares of data will contain optionally encrypted portions of the original data and portions of the transaction ID.

[0339] 8. Optionally generate an encryption key for each of the four data shares.

[0340] 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.

[0341] To restore the original data format, the steps are reversed.

[0342] 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.

[0343] 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.

[0344] At the bit level is generated:

0 XOR 0 = 0

0 XOR 1 = 1

1 XOR 0 = 1

1 XOR 1 = 0

[0345] 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.

[0346] Note that one can derive "s" via the equation:

s = a XOR b.

[0347] 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.

[0348] 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

[0349] 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.

[0350] 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.

[0351] 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.

[0352] 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.

[0353] 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.

[0354] 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

[0355] 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.

[0356] 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.

[0357] 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.

[0358] 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.

[0359] 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.

[0360] 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:

[0361] 1. All shares or portions of the data set.

[0362] 2. Knowledge of and ability to reproduce the process flow of the method used to secure the data.

[0363] 3. Access to the session master key.

[0364] 4. Access to the Parser Master Key.

[0365] 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).

[0366] 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.

[0367] 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

[0368] 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

[0369] 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

[0370] 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

[0371] 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.

[0372] 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.

[0373] 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

[0374] 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

[0375] 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

[0376] 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

[0377] 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.

[0378] 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

[0379] 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.

[0380] 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.

[0381] 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.

[0382] 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.

[0383] 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.

[0384] 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.

[0385] 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.

[0386] In this example, there are three members in the Senior Staff group. For this group, the actions would be:

[0387] 1. Access Parser Group Master Key for the Senior Staff group (generate a key if not available);

[0388] 2. Generate a digital certificate associating CEO with the Senior Staff group;

[0389] 3. Generate a digital certificate associating CFO with the Senior Staff group;

[0390] 4. Generate a digital certificate associating Vice President, Marketing with the Senior Staff group.

[0391] 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.

[0392] 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.

[0393] 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.

[0394] 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.

[0395] 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.

[0396] 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.

[0397] 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.

[0398] 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).

[0399] 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.

[0400] 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.

[0401] 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.

[0402] 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.

[0403] 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).

[0404] 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.

[0405] 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.

[0406] 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.

[0407] 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

[0408] 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.

[0409] 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.

[0410] 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.

[0411] 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.

[0412] 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.

[0413] 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.

[0414] 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.

[0415] 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.

[0416] 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.

[0417] 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).

[0418] 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.

[0419] 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.

[0420] 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.

[0421] 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.

[0422] 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.

[0423] 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.

[0424] 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.

[0425] 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.

[0426] 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.

[0427] 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.).

[0428] 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.

[0429] 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.

[0430] 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.

[0431] 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.

[0432] 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.

[0433] 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.

[0434] 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.

[0435] 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.

[0436] 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.

[0437] 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.

[0438] 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.

[0439] 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.

[0440] 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.

[0441] 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.

[0442] Any such suitable paradigm may be used that makes use of mandatory shares where fewer than all shares are needed to restore original data.

[0443] 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.

[0444] 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.

[0445] 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.

[0446] 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.

[0447] 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.

[0448] 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.

[0449] 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.

[0450] 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.

[0451] 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.

[0452] 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.

[0453] 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.

[0454] 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.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 13/371,363

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	380
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	620
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	250
TOTAL CLAIMS (37 CFR 1.16(i))	27 minus 20 =	* 7			OR	x 60 =	420
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*				x 250 =	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).						620
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	2290

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	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
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
13/371,363	02/10/2012	Rick L. Orsini	104093-0002-105

CONFIRMATION NO. 7984

1473
ROPES & GRAY LLP
PATENT DOCKETING 39/361
1211 AVENUE OF THE AMERICAS
NEW YORK, NY 10036-8704

FORMALITIES LETTER

OC000000052773394

Date Mailed: 02/29/2012

NOTICE TO FILE CORRECTED APPLICATION PAPERS

Filing Date Granted

An application number and filing date have been accorded to this application. The application is informal since it does not comply with the regulations for the reason(s) indicated below. Applicant is given TWO MONTHS from the date of this Notice within which to correct the informalities indicated below. 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 required item(s) identified below must be timely submitted to avoid abandonment:

- Replacement drawings in compliance with 37 CFR 1.84 and 37 CFR 1.121(d) are required. The drawings submitted are not acceptable because:
  - Numbers, letters, and reference characters on the drawings must measure at least 0.32 cm (1/8 inch) in height. See Figure(s) 21,22,23,24,30-35.
  - The drawings submitted to the Office are not electronically reproducible because portions of figures 1-24,30-35 are missing and/or blurry.

Applicant is cautioned that correction of the above items may cause the specification and drawings page count to exceed 100 pages. If the specification and drawings exceed 100 pages, applicant will need to submit the required application size fee.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.
https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

/tnegash/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 14

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2827
Examiner Name	Not Yet Assigned
Attorney Docket Number	104093-0002-105

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
		US-7,577,689	08-18-2009	Masinter et al.	
		US-7,546,427	06-09-2009	Gladwin et al.	
		US-7,203,871	04-10-2007	Turner et al.	
		US-7,187,771	03-06-2007	Dickinson et al.	
		US-7,003,531	02-21-2006	Holenstein et al.	
		US-6,852,988	02-08-2005	Li	
		US-6,687,375	02-03-2004	Matyas, Jr. et al.	
		US-6,453,416	09-17-2002	Epstein	
		US-6,446,204	09-03-2002	Pang et al.	
		US-6,411,716	06-25-2002	Brickell	
		US-6,385,318	05-07-2002	Oishi	
		US-6,307,940	10-23-2001	Yamamoto et al.	
		US-6,292,782	09-18-2001	Weideman	
		US-6,292,568	09-18-2001	Akins, III et al.	
		US-6,289,455	09-11-2001	Kocher et al.	
		US-6,266,413	07-24-2001	Shefi	
		US-6,260,125	07-10-2001	McDowell	
		US-6,256,737	07-03-2001	Bianco et al.	
		US-6,061,790	05-09-2000	Bodnar	

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]
	**	AU-2004248616	06-04-2009	Security First Corporation		
	**	EP-0485090-A2	05-13-1992	Visa Int Service Ass		
	**	EP-0821504	01-28-1998	Nippon Telegraph and Telephone Corporation		
	**	EP-0862301	09-02-1998	Fujitsu Limited		
	**	EP-1011222	06-21-2000	Fujitsu Limited		
	**	EP-1239384-A2	09-11-2002	Pkware Inc		

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. ** CITE NO.: Those document(s) which are marked with an double asterisk (**) next to the Cite No. are not supplied because they were previously cited by or submitted to the Office in a prior application relied upon in this application for an earlier filing date under 35 U.S.C. 120. [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.

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 14

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2827
Examiner Name	Not Yet Assigned
Attorney Docket Number	104093-0002-105

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
		US-5,995,630	11-30-1999	Borza	
		US-5,987,232	11-16-1999	Tabuki	
		US-5,917,913	06-29-1999	Wang	
		US-5,915,019	06-22-1999	Ginter et al.	
		US-5,163,096	11-10-1992	Clark et al.	
		US-5,150,407	09-22-1992	Chan	
		US-2011/0246817	10-06-2011	Orsini et al.	
		US-2011/0246766	10-06-2011	Orsini et al.	
		US-2011/0179287	07-21-2011	Orsini et al.	
		US-2011/0179271	07-21-2011	Orsini et al.	
		US-2010/0299313	11-25-2010	ORSINI et al.	
		US-20090254572	10-08-2009	Redlich et al.	
		US-20080147821	06-19-2008	Dietrich et al.	
		US-2008/281879	11-13-2008	KAWAMURA	
		US-2008/0183975	07-31-2008	Foster et al.	
		US-2004/0267832	12-30-2004	Wong et al.	
		US-4,453,074	06-05-1984	Weinstein	
		US-4,924,513	05-08-1990	Herbison et al.	
		US-4,932,057	06-05-1990	Kolbert	

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]
	**	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.		
	**	GB-2237670-A	05-08-1991	De La Rue Syst et al.		
	**	JP-04297157-A	10-21-1992	Mitsubishi Electric Corp		

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. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. ** CITE NO.: Those document(s) which are marked with an double asterisk (**) next to the Cite No. are not supplied because they were previously cited by or submitted to the Office in a prior application relied upon in this application for an earlier filing date under 35 U.S.C. 120. [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.

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 3 of 14

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2827
Examiner Name	Not Yet Assigned
Attorney Docket Number	104093-0002-105

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
		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-5,268,963	12-07-1993	Monroe et al.	
		US-5,375,244	12-20-1994	McNair	
		US-5,386,104	01-31-1995	Sime	
		US-5,485,474	01-16-1996	Rabin	
		US-5,524,073	06-04-1996	Stambler	
		US-5,615,269	03-25-1997	Micali	
		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-5,682,425	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-5,768,382	06-16-1998	Schneier et al.	
		US-5,768,519	06-16-1998	Swift et al.	

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]
	**	RU-2124814	01-10-1999	A.A. Moldovjan		
	**	WO-00/36786-A1	06-22-2000	Philips Electronics Na		
	**	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		

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. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. ** CITE NO.: Those document(s) which are marked with an double asterisk (**) next to the Cite No. are not supplied because they were previously cited by or submitted to the Office in a prior application relied upon in this application for an earlier filing date under 35 U.S.C. 120. [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.

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 4 of 14

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2827
Examiner Name	Not Yet Assigned
Attorney Docket Number	104093-0002-105

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
		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-5,940,507	08-1999	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-5,991,414	11-23-1999	Garay et al.	
		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-6,073,237	06-06-2000	Ellison	
		US-6,092,201	07-18-2000	Turnbull et al.	
		US-6,094,485	07-25-2000	Weinstein et al.	
		US-6,192,472	02-20-2001	Garay et al.	

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]
	**	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-02/21283-A1	03-14-2002	Sanctuary Systems Pty Ltd.		
	**	WO-02/21761-A2	03-14-2002	Widevine Technologies Inc		
	**	WO-02/21761-A2	03-14-2002	Widevine Technologies Inc		

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. ** CITE NO.: Those document(s) which are marked with an double asterisk (**) next to the Cite No. are not supplied because they were previously cited by or submitted to the Office in a prior application relied upon in this application for an earlier filing date under 35 U.S.C. 120. [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.

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 5 of 14

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2827
Examiner Name	Not Yet Assigned
Attorney Docket Number	104093-0002-105

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
		US-6,134,550	10-17-2000	Van Oorschot 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-6,289,509	09-11-2001	Kryloff	
		US-6,301,659	10-09-2001	Micali	
		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-6,356,941	03-12-2002	Cohen	
		US-6,363,425	03-26-2002	Hook et al.	
		US-6,386,451	05-14-2002	Sehr	
		US-6,424,718	07-23-2002	Holloway	
		US-6,438,690	08-20-2002	Patel et al.	
		US-6,449,730	09-10-2002	Mann et al.	
		US-6,483,921	11-19-2002	Harkins	
		US-6,553,493	04-22-2003	Okumura et al.	

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]
	**	WO-04/111791-A2	12-23-2004	Security First Corp.		
	**	WO-06/047694-A1	05-04-2006	Orsini Rick L et al.		
	**	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	Surfcontrol On Demand Ltd.		

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. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. ** CITE NO.: Those document(s) which are marked with an double asterisk (**) next to the Cite No. are not supplied because they were previously cited by or submitted to the Office in a prior application relied upon in this application for an earlier filing date under 35 U.S.C. 120. [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.

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 6 of 14

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2827
Examiner Name	Not Yet Assigned
Attorney Docket Number	104093-0002-105

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
		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-6,789,198	09-07-2004	Chan	
		US-6,856,383	02-15-2005	Vachris et al.	
		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-7,050,580	05-23-2006	Ferre Herrero	
		US-7,050,583	05-23-2006	Montgomery	
		US-7,069,451	06-27-2006	Ginter et al.	
		US-7,096,494	08-22-2006	Chen	
		US-7,117,365	10-03-2006	Rump et al.	
		US-7,133,845	11-07-2006	Ginter et al.	
		US-7,218,736	05-15-2007	Nishimura et al.	
		US-7,225,158	05-29-2007	Toshikage et al.	
		US-7,337,320	02-26-2008	Tada et al.	

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]
	**	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-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.		

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. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. ** CITE NO.: Those document(s) which are marked with an double asterisk (**) next to the Cite No. are not supplied because they were previously cited by or submitted to the Office in a prior application relied upon in this application for an earlier filing date under 35 U.S.C. 120. [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.

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 7 of 14

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2827
Examiner Name	Not Yet Assigned
Attorney Docket Number	104093-0002-105

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
		US-7,349,539	03-25-2008	Wee et al.	
		US-7,391,865	06-24-2008	Orsini et al.	
		US-7,627,125	12-01-2009	Lumsden et al.	
		US-7,649,992	01-19-2010	Raju et al.	
		US-7,869,597	01-11-2011	Nakai et al.	
		US-2001/0001876	05-24-2001	Morgan et al.	
		US-2001/0051902	12-13-2001	Messner	
		US-20020010679	01-24-2002	Felsher	
		US-2002/0032663	03-14-2002	Messner	
		US-2002/0046359	04-18-2002	Boden	
		US-2002/0071566	06-13-2002	Kurn	
		US-2002/0091640	07-11-2002	Gupta	
		US-2002/0129235	09-12-2002	Okamoto et al.	
		US-2002/0162047	10-31-2002	Peters et al.	
		US-2002/0172358	11-21-2002	Hurich	
		US-2003/0051054	03-13-2003	Redlich et al.	
		US-2003/0058274	03-27-2003	Hill et al.	
		US-2003/0070077	04-10-2003	Redlich et al.	
		US-2003/0167408	09-04-2003	Fitzpatrick et al.	

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]
	**	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		

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. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. ** CITE NO.: Those document(s) which are marked with an double asterisk (**) next to the Cite No. are not supplied because they were previously cited by or submitted to the Office in a prior application relied upon in this application for an earlier filing date under 35 U.S.C. 120. [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.

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 8 of 14

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2827
Examiner Name	Not Yet Assigned
Attorney Docket Number	104093-0002-105

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
		US-2003/0051159	03-13-2003	McCown et al.	
		US-7,391,865	06-24-2008	Orsini et al.	
		US-20040111608	06-10-2004	Oom Temudo de Castro et al.	
		US-2004/0122863	06-24-2004	Sidman	
		US-2006/0177061	08-10-2006	Orsini et al.	
		US-2006/0184764	08-17-2006	Osaki	
		US-2006/0282681	12-14-2006	Scheidt et al.	
		US-2006/0294378	12-28-2006	Lumsden et al.	
		US-20070192586	08-16-2007	McNeely	
		US-8,009,830	08-30-2011	Orsini et al.	
		US-2008/0137857	06-12-2008	Bellare et al.	
		US-2008/0170693	07-17-2008	Spies et al.	
		US-2008/0183992	07-31-2008	Martin et al.	
		US-20080199003	08-21-2008	Hennessey et al.	
		US-20080244277	10-02-2008	Orsini et al.	
		US-20090077379	03-19-2009	Geyzel et al.	
		US-2009/0097661	04-16-2009	Orsini et al.	
		US-2009/0177894	07-09-2009	Orsini et al.	
		US-2009/0254750	10-08-2009	Bono et al.	

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]

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. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. ** CITE NO.: Those document(s) which are marked with an double asterisk (**) next to the Cite No. are not supplied because they were previously cited by or submitted to the Office in a prior application relied upon in this application for an earlier filing date under 35 U.S.C. 120. [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.

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 9 of 14

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2827
Examiner Name	Not Yet Assigned
Attorney Docket Number	104093-0002-105

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
		US-2010/0150341	06-17-2010	Dodgson et al.	
		US-2010/0153670	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-2011/0202763	08-18-2011	Martin et al.	
		US-2011/0202755	08-18-2011	ORSINI et al.	

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]

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. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. ** CITE NO.: Those document(s) which are marked with an double asterisk (**) next to the Cite No. are not supplied because they were previously cited by or submitted to the Office in a prior application relied upon in this application for an earlier filing date under 35 U.S.C. 120. [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.

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 10 of 14

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2827
Examiner Name	Not Yet Assigned
Attorney Docket Number	104093-0002-105

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	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[2]
	**	"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.	
	**	"Lancope Announces Stealthwatch 3.0 for Enhanced Enterprise-Wide Security and Improved Manageability", Business Wire (Newswire Association, Inc.), 14 April 2003.	
	**	"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.	
	**	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.	
	**	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.	

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. ** CITE NO.: Those document(s) which are marked with an double asterisk (**) next to the Cite No. are not supplied because they were previously cited by or submitted to the Office in a prior application relied upon in this application for an earlier filing date under 35 U.S.C. 120.

[1]Applicant's unique citation designation number (optional). [2]Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 11 of 14

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2827
Examiner Name	Not Yet Assigned
Attorney Docket Number	104093-0002-105

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	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[2]
	**	Damgard et. al., "Non-interactive and Reusable Non-malleable Commitment Schemes," ACM STOC '03; pgs. 427-428; June 9-11, 2003.	
	**	Decleene et al., "Secure group communications for wireless networks," MILCOM 2001 Proceedings, Communications for Network-Centric Operations: Creating the Information Force; IEEE, US, vol. 1, 28 October 2001, pages 113-117	
	**	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	
	**	Gibson, "Opinion", eWeek - Enterprise News & Reviews, 14 April 2003.	
	**	Grant et. al., "Secret Sharing and Splitting", (White Paper) Notre Dame, Indiana, 16 December 2002.	

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. ** CITE NO.: Those document(s) which are marked with an double asterisk (**) next to the Cite No. are not supplied because they were previously cited by or submitted to the Office in a prior application relied upon in this application for an earlier filing date under 35 U.S.C. 120.

[1]Applicant's unique citation designation number (optional). [2]Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 12 of 14

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2827
Examiner Name	Not Yet Assigned
Attorney Docket Number	104093-0002-105

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	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[2]
	**	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.	
	**	International Search Report - International Application No. PCT/US/06/45066, dated July 17, 2008	
	**	International Search Report and Written Opinion dated December 14, 2010 in International Application No. PCT/US2010/035377	
	**	International Search Report and Written Opinion dated September 8, 2009 in International Application No. PCT/US2009/001158	
	**	International Search Report dated December 16, 2008, International Application No. PCT/US07/023626	
	**	International Search Report dated March 10, 2009, International Application No. PCT/US09/000083	
	**	International Search Report dated November 21, 2008, International Application No. PCT/US08/010677	
	**	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]	

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. ** CITE NO.: Those document(s) which are marked with an double asterisk (**) next to the Cite No. are not supplied because they were previously cited by or submitted to the Office in a prior application relied upon in this application for an earlier filing date under 35 U.S.C. 120.

[1]Applicant's unique citation designation number (optional). [2]Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 13 of 14

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2827
Examiner Name	Not Yet Assigned
Attorney Docket Number	104093-0002-105

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	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[2]
	**	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" 1997, 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	
	**	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	
	**	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	
	**	Savage, "RSA Unveils Nightingale Technology", CRN.com, 14 April 2003.	

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. ** CITE NO.: Those document(s) which are marked with an double asterisk (**) next to the Cite No. are not supplied because they were previously cited by or submitted to the Office in a prior application relied upon in this application for an earlier filing date under 35 U.S.C. 120.

[1]Applicant's unique citation designation number (optional). [2]Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 14 of 14

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2827
Examiner Name	Not Yet Assigned
Attorney Docket Number	104093-0002-105

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	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[2]
	**	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.	
	**	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.	

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. ** CITE NO.: Those document(s) which are marked with an double asterisk (**) next to the Cite No. are not supplied because they were previously cited by or submitted to the Office in a prior application relied upon in this application for an earlier filing date under 35 U.S.C. 120.

[1]Applicant's unique citation designation number (optional). [2]Applicant is to place a check mark here if English language Translation is attached.

Docket No.: 104093-0002-105
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Orsini et al.

Application No.: 13/371,363 | Confirmation No.: 7984

Filed: February 10, 2012 | Art Unit: 2827

For: SECURE DATA PARSER METHOD AND SYSTEM | Examiner: Not Yet Assigned

INFORMATION DISCLOSURE STATEMENT (IDS)

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

Dear Madam:

Pursuant to 37 CFR 1.56, 1.97 and 1.98, the attention of the Patent and Trademark Office is hereby directed to the references listed on the attached PTO/SB/08. It is respectfully requested that the information be expressly considered during the prosecution of this application, and that the references be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Information Disclosure Statement is filed within three months of the U.S. filing date (37 CFR 1.97(b)(1)).

In accordance with 37 CFR 1.98(a)(2)(ii), Applicants have not submitted copies of U.S. patents and U.S. patent applications. Those documents which are marked with a double asterisk (**) next to the Cite No. in the attached form PTO/SB/08 are not supplied because they were previously cited by or submitted to the Office in prior application number 11/258,839 filed October 25, 2005 and relied upon in this application for an earlier filing date under 35 U.S.C. 120.

29678444_1

In accordance with 37 CFR 1.97(g), the filing of this Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 CFR 1.56(a) exists. In accordance with 37 CFR 1.97(h), the filing of this Information Disclosure Statement shall not be construed to be an admission that any patent, publication or other information referred to therein is "prior art" for this invention unless specifically designated as such.

It is submitted that the Information Disclosure Statement is in compliance with 37 CFR 1.98 and the Examiner is respectfully requested to consider the listed references.

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, under Order No. 104093-0002-105.

Dated: February 29, 2012

Respectfully submitted,

Electronic signature: /Edward A. Gordon/
Edward A. Gordon
Registration No.: 54,130
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, Massachusetts 02199
(617) 951-7000
(617) 235-9492 (Fax)
Attorneys/Agents 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 NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/371,363	02/10/2012	Rick L. Orsini	104093-0002-105

CONFIRMATION NO. 7984

1473
ROPES & GRAY LLP
PATENT DOCKETING 39/361
1211 AVENUE OF THE AMERICAS
NEW YORK, NY 10036-8704

POA ACCEPTANCE LETTER

OC000000052767330

Date Mailed: 02/29/2012

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 02/10/2012.

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.

/qtran/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Electronic Acknowledgement Receipt

EFS ID:	12188907
Application Number:	13371363
International Application Number:	
Confirmation Number:	7984
Title of Invention:	SECURE DATA PARSER METHOD AND SYSTEM
First Named Inventor/Applicant Name:	Rick L. Orsini
Customer Number:	1473
Filer:	Edward A. Gordon/Joanne Ryan
Filer Authorized By:	Edward A. Gordon
Attorney Docket Number:	104093-0002-105
Receipt Date:	29-FEB-2012
Filing Date:	10-FEB-2012
Time Stamp:	16:30:23
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	Transmittal Letter	104093-0002-105_IDS.pdf	19696 a881ec1e0434286fb3a376a42bd43d862799d6f2	no	2

Warnings:	
Information:	

2	Information Disclosure Statement (IDS) Form (SB08)	104093-0002-105_SB08.pdf	209468 650a5c716faf45ebb69f20697fd2612afd6d75e2	no	14

Warnings:

Information:

This is not an USPTO supplied IDS fillable form

Total Files Size (in bytes):	229164

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/371,363	02/10/2012	2827	2590	104093-0002-105	27	3

CONFIRMATION NO. 7984

1473
ROPES & GRAY LLP
PATENT DOCKETING 39/361
1211 AVENUE OF THE AMERICAS
NEW YORK, NY 10036-8704

FILING RECEIPT



Date Mailed: 02/29/2012

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

Applicant(s)

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

Assignment For Published Patent Application

Security First Corp., Rancho Santa Margarita, CA

Power of Attorney: The patent practitioners associated with Customer Number 1473

Domestic Priority data as claimed by applicant

This application is a CON of 11/258,839 10/25/2005
which claims benefit of 60/718,185 09/16/2005
and claims benefit of 60/622,146 10/25/2004

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)

If Required, Foreign Filing License Granted: 02/24/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/371,363**

Projected Publication Date: To Be Determined - pending completion of Corrected Papers

Non-Publication Request: No

Early Publication Request: No

Title

SECURE DATA PARSER METHOD AND SYSTEM

Preliminary Class

365

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

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

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

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

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

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as

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 USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage, facilitate, and accelerate 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.

Electronic Acknowledgement Receipt

EFS ID:	12260160
Application Number:	13371363
International Application Number:	
Confirmation Number:	7984
Title of Invention:	SECURE DATA PARSER METHOD AND SYSTEM
First Named Inventor/Applicant Name:	Rick L. Orsini
Customer Number:	1473
Filer:	Matthew Sammuel Bertenthal/Lily Jiang
Filer Authorized By:	Matthew Sammuel Bertenthal
Attorney Docket Number:	104093-0002-105
Receipt Date:	08-MAR-2012
Filing Date:	10-FEB-2012
Time Stamp:	17:25:40
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	Drawings-only black and white line drawings	104093-0002-105_Replacement_Drawings.pdf	230961 e1b2492a8db943cbb71b15a6525941725abe38b2	no	36
Warnings:					
Information:					

2	Applicant Response to Pre-Exam Formalities Notice	104093-0002-105_Reply.pdf	59738 5844813117362b1037c3efc492ea237670d2df2b	no	1

Warnings:	
Information:	
Total Files Size (in bytes):	290699

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.

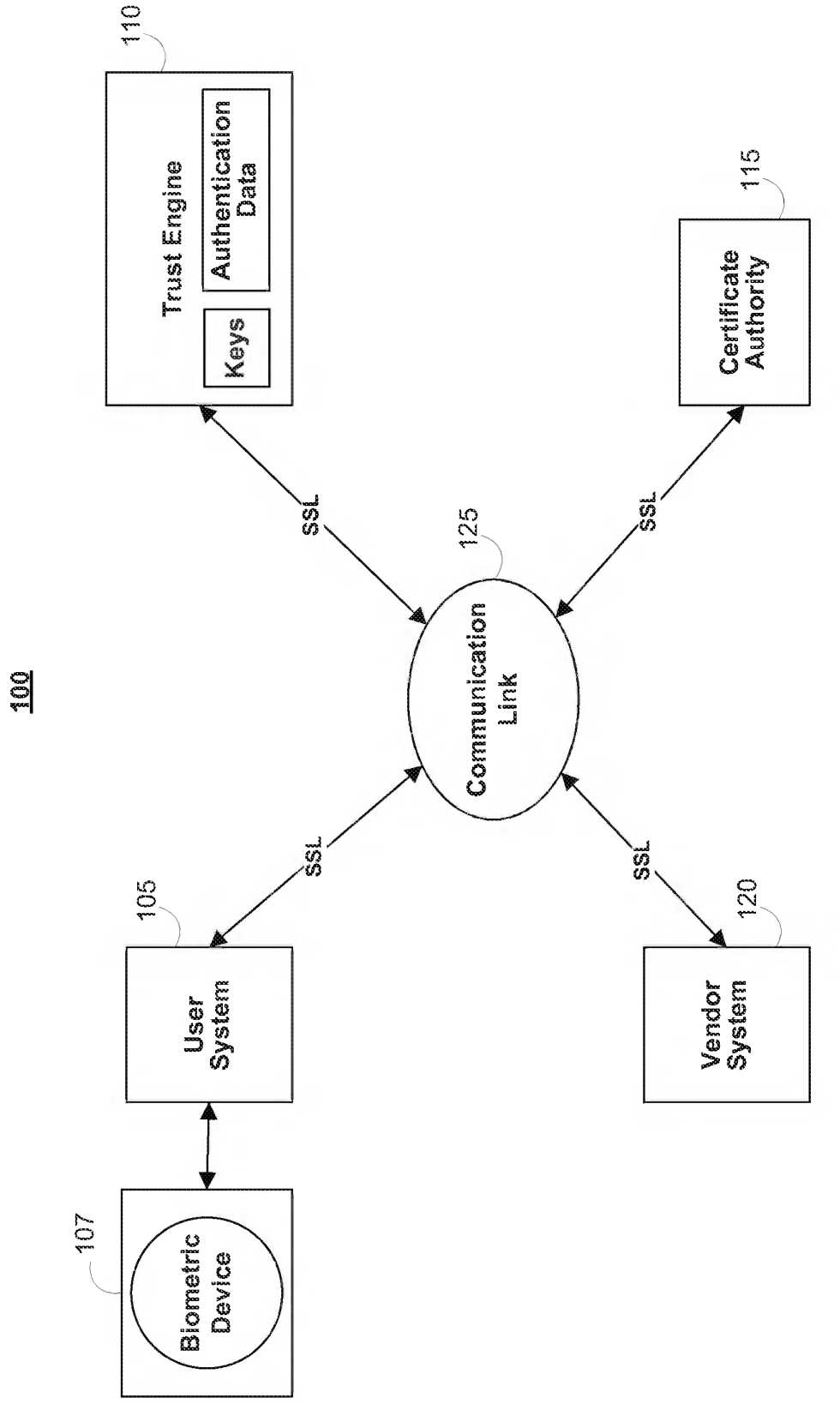

100
110
Trust Engine
Authentication Data
Keys
115
Certificate Authority
SSL
SSL
125
Communication Link
SSL
SSL
105
User System
120
Vendor System
107
Biometric Device

FIG. 1

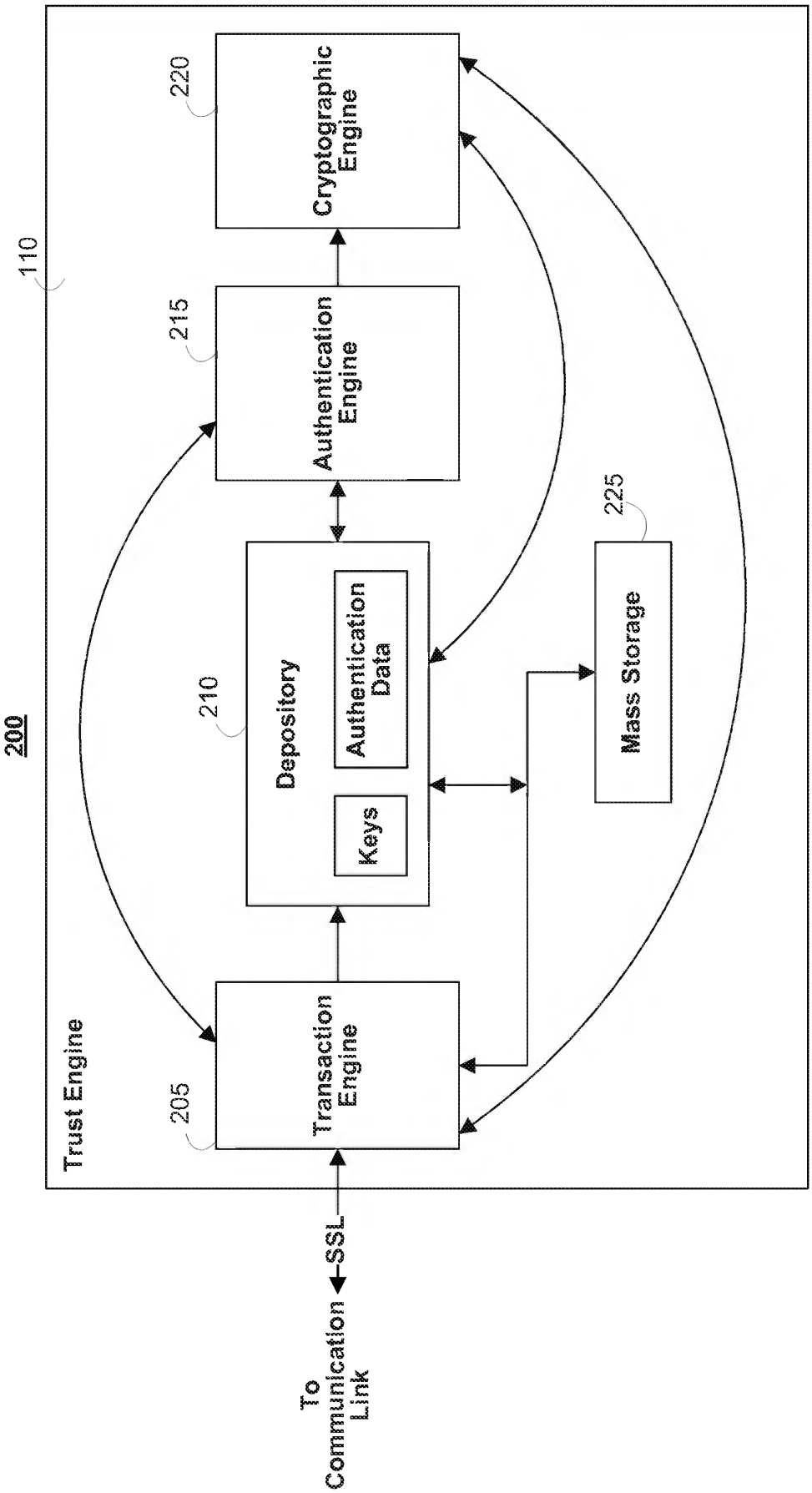

200
110
Trust Engine
220
Cryptographic Engine
215
Authentication Engine
210
Depository
Authentication Data
Keys
225
Mass Storage
205
Transaction Engine
SSL
To Communication Link

FIG. 2

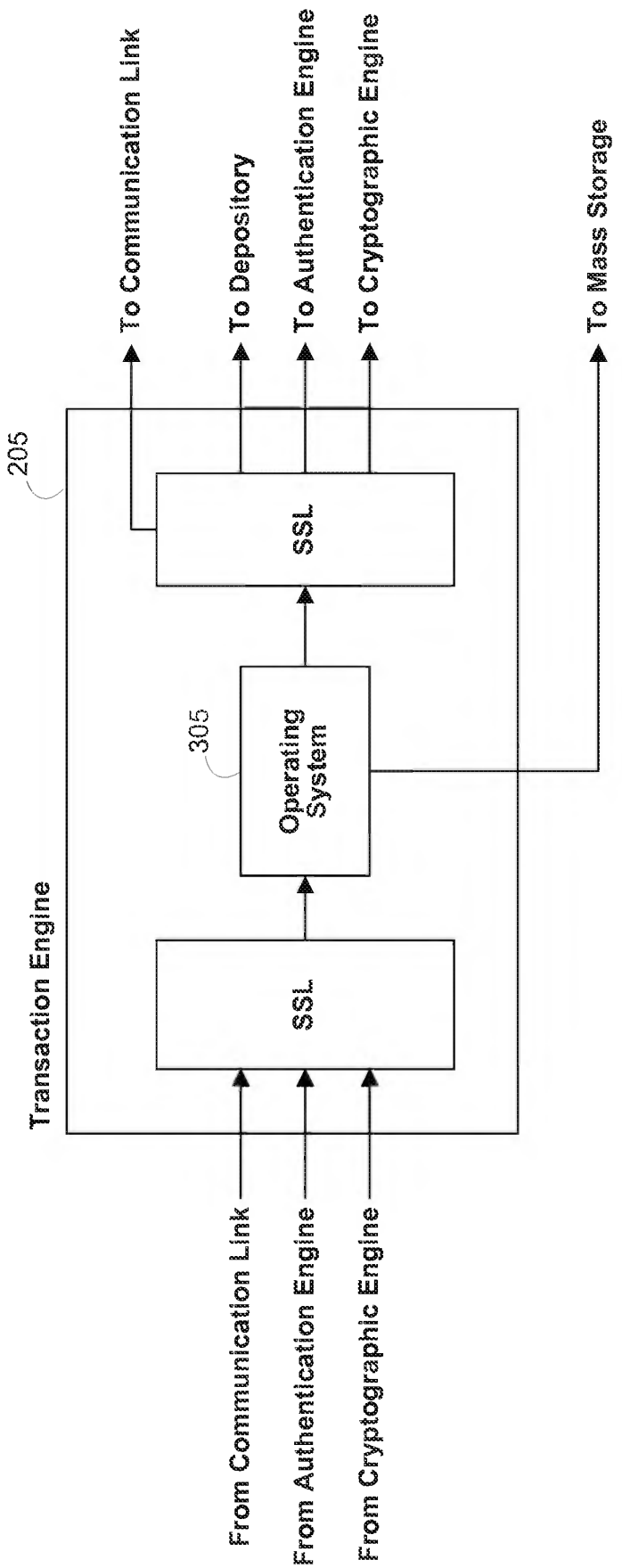

To Communication Link
To Depository
To Authentication Engine
To Cryptographic Engine
To Mass Storage
205
SSL
305
Operating System
SSL
Transaction Engine
From Communication Link
From Authentication Engine
From Cryptographic Engine

FIG. 3

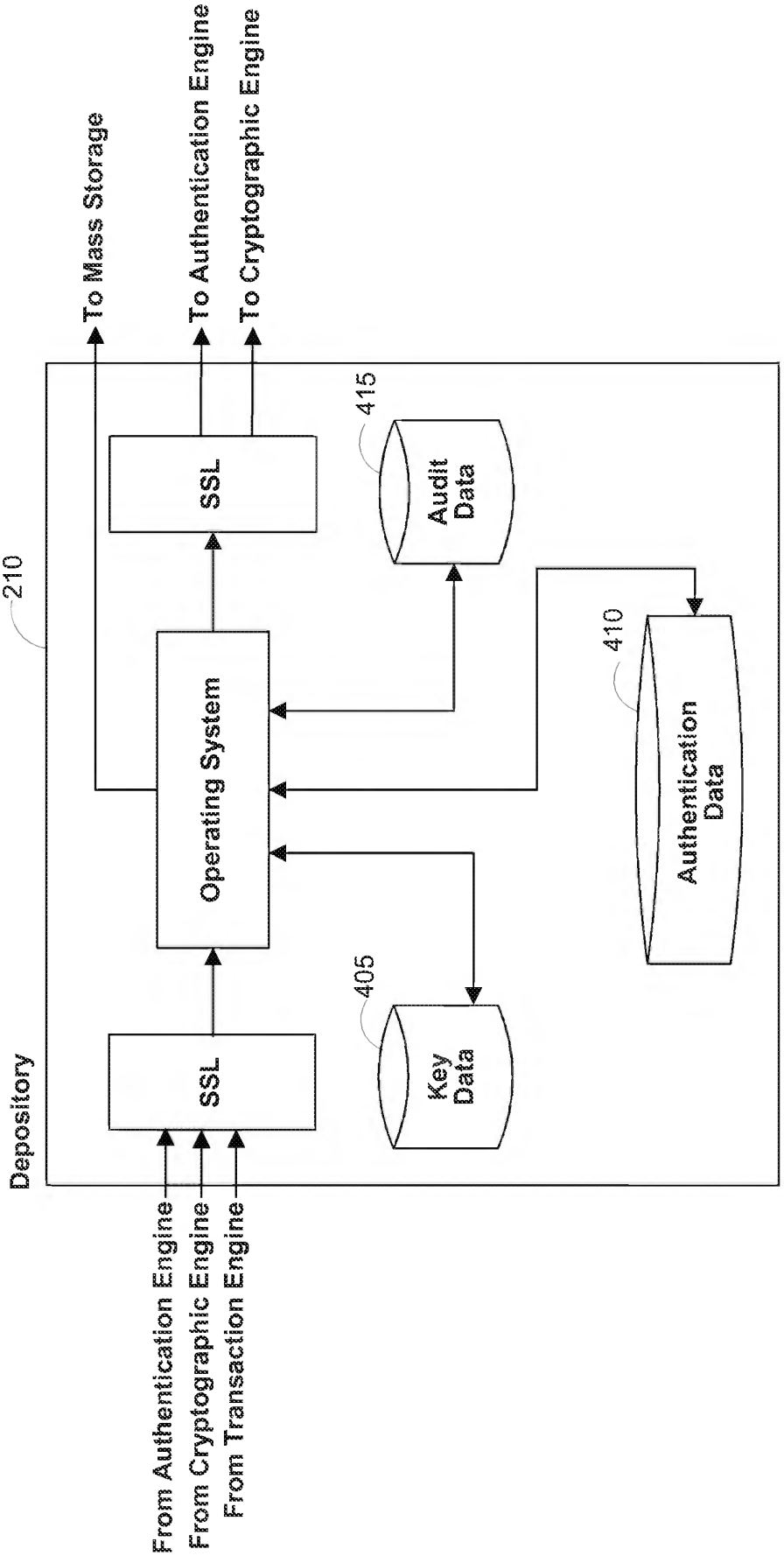

To Mass Storage
To Authentication Engine
To Cryptographic Engine
210
SSL
415
Audit Data
Operating System
410
Authentication Data
405
Key Data
SSL
Depository
From Authentication Engine
From Cryptographic Engine
From Transaction Engine

FIG. 4

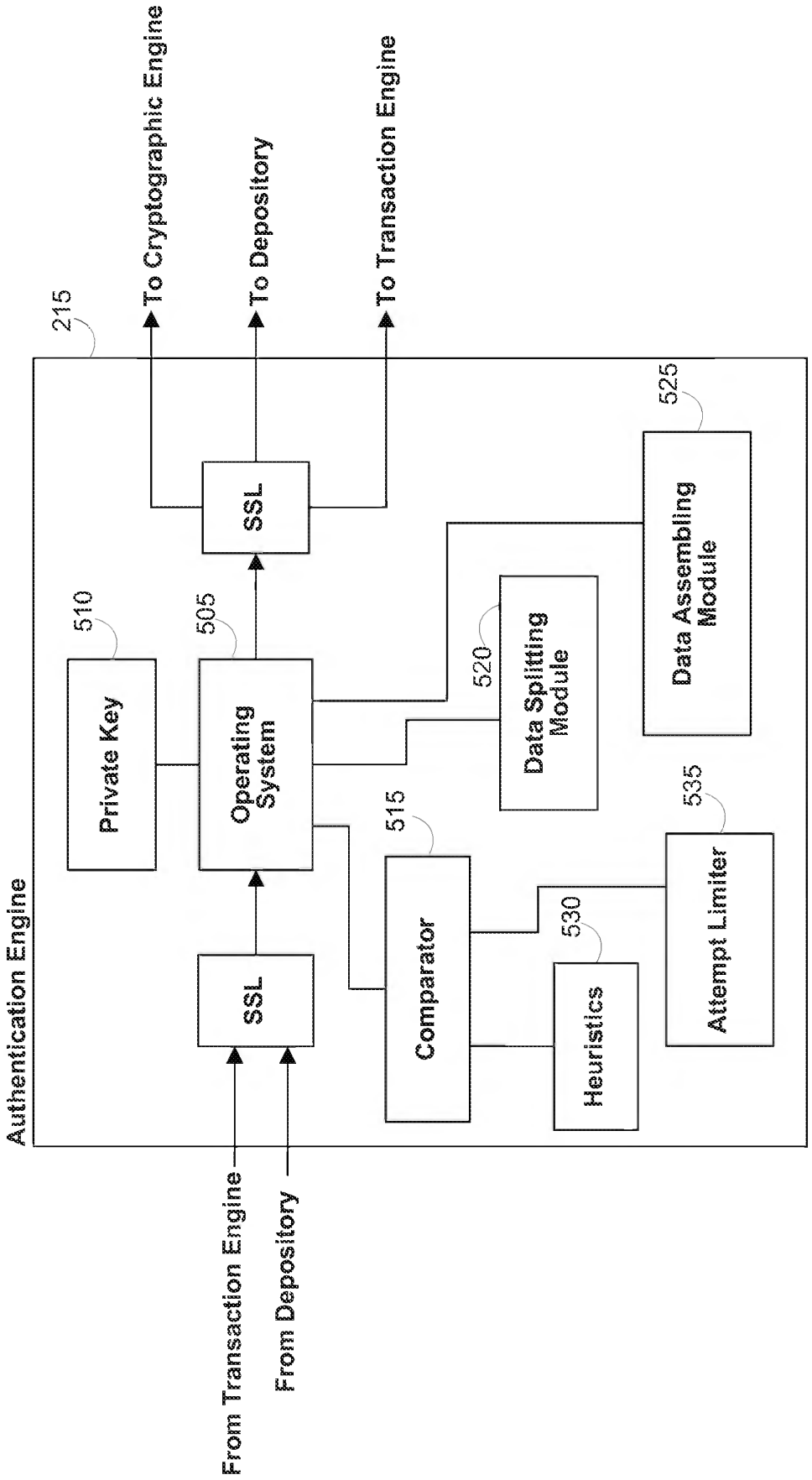

215
To Cryptographic Engine
To Depository
To Transaction Engine
SSL
525
Data Assembling Module
510
505
520
Private Key
Operating System
Data Splitting Module
515
535
Comparator
Attempt Limiter
530
Heuristics
SSL
Authentication Engine
From Transaction Engine
From Depository

FIG. 5

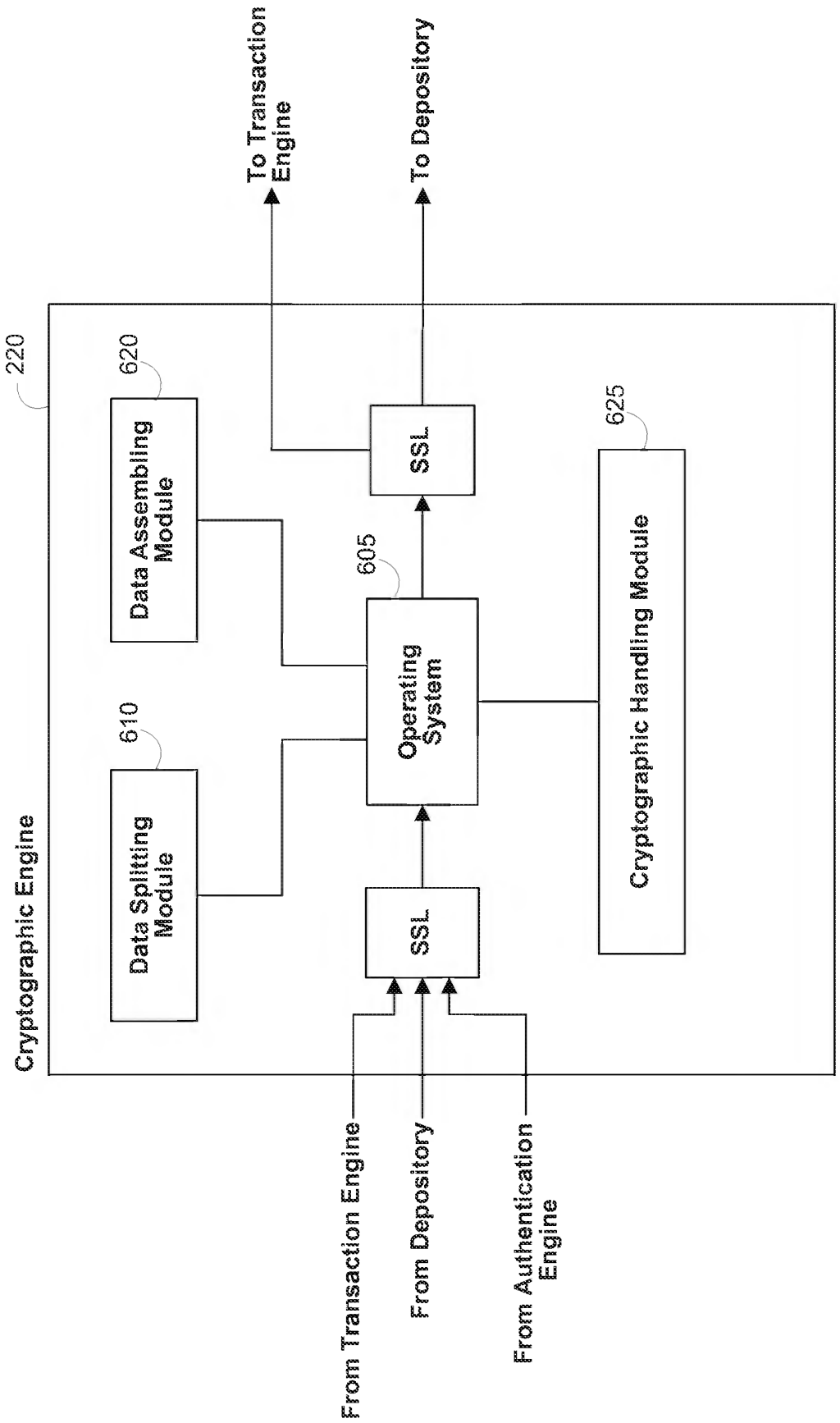

To Transaction Engine
To Depository
220
620
625
Data Assembling Module
SSL
605
Operating System
610
Data Splitting Module
SSL
Cryptographic Handling Module
Cryptographic Engine
From Transaction Engine
From Depository
From Authentication Engine

FIG. 6

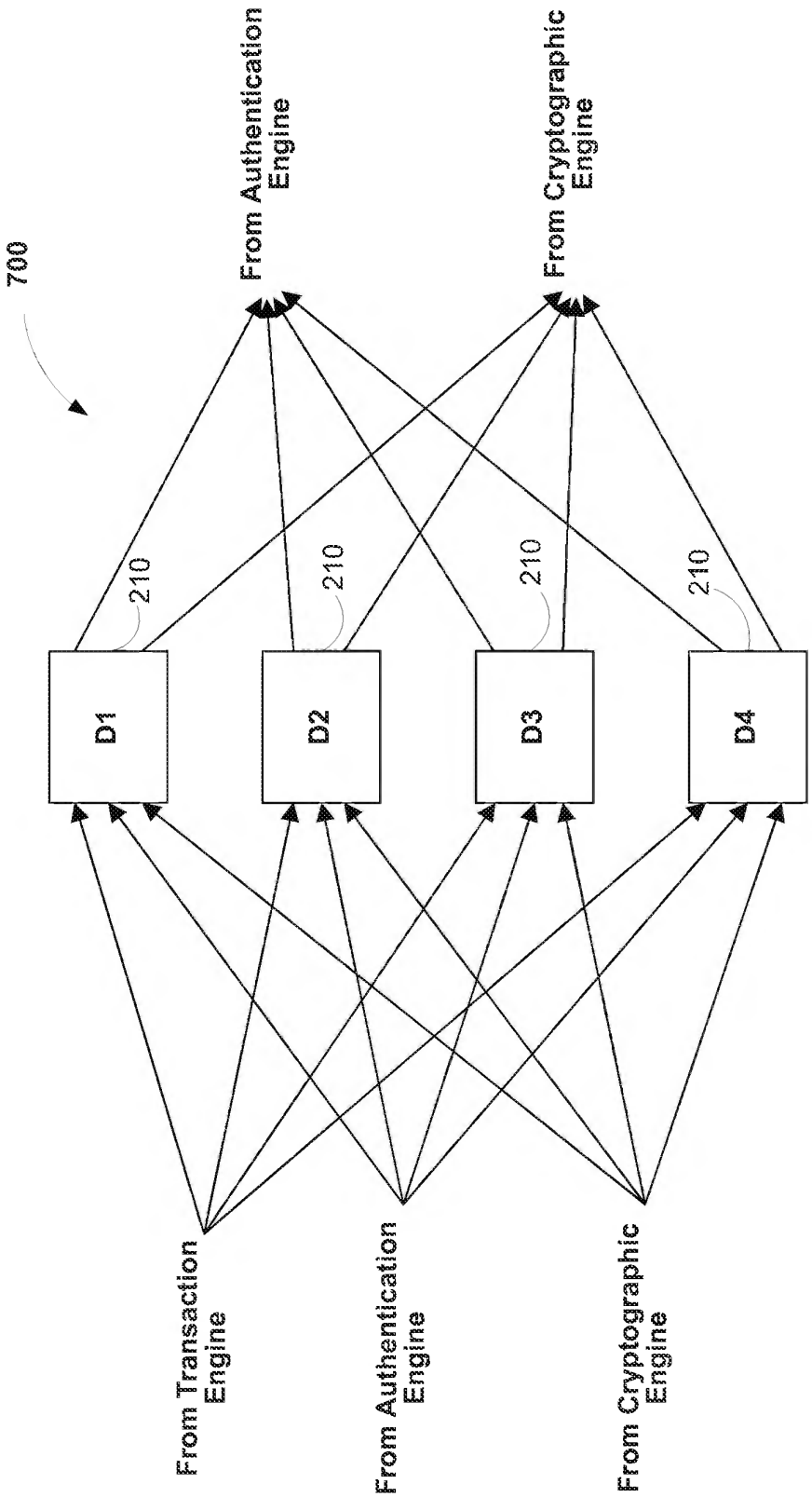

700
From Authentication Engine
From Cryptographic Engine
210
210
210
210
D1
D2
D3
D4
From Transaction Engine
From Authentication Engine
From Cryptographic Engine

FIG. 7

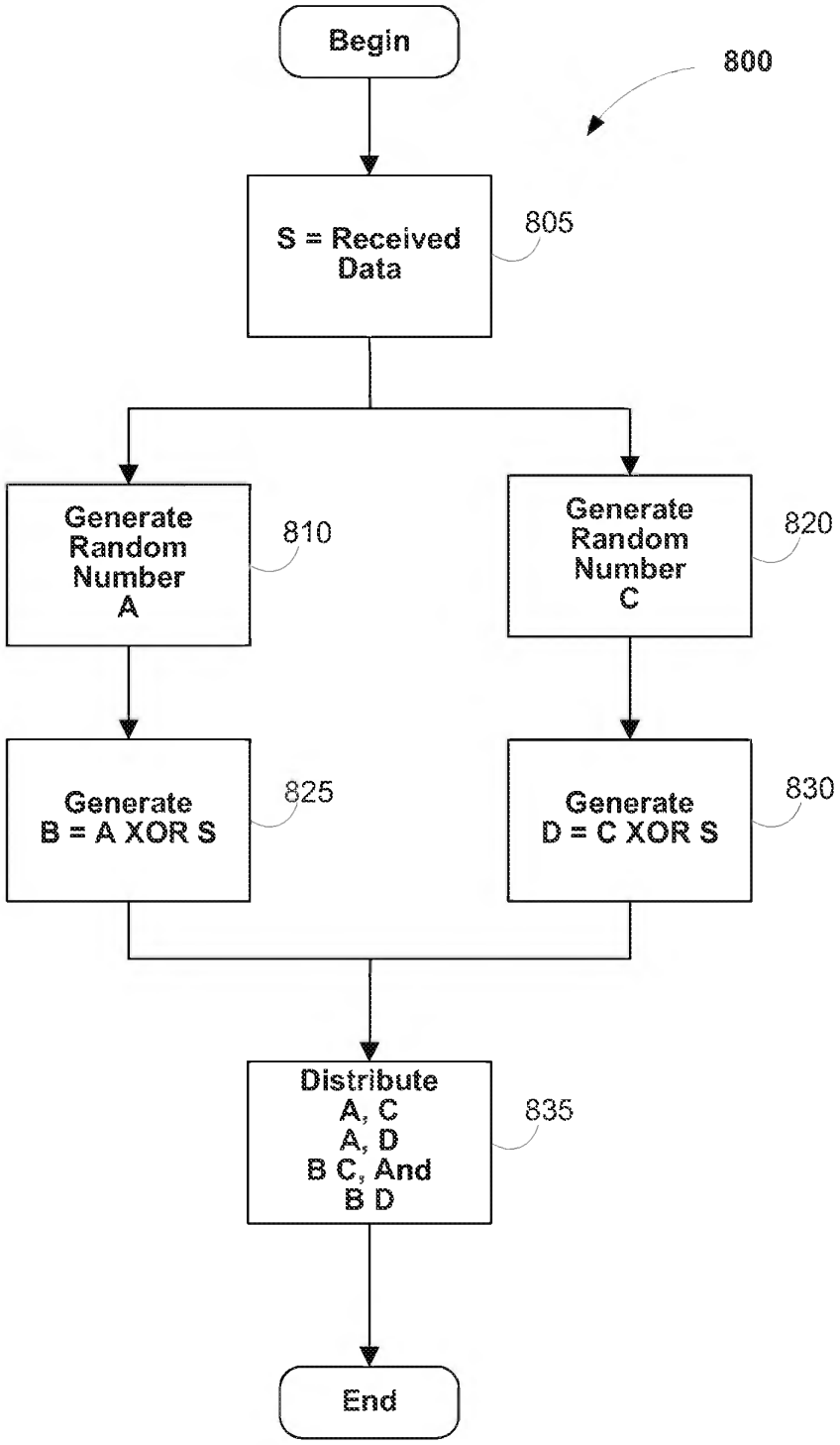
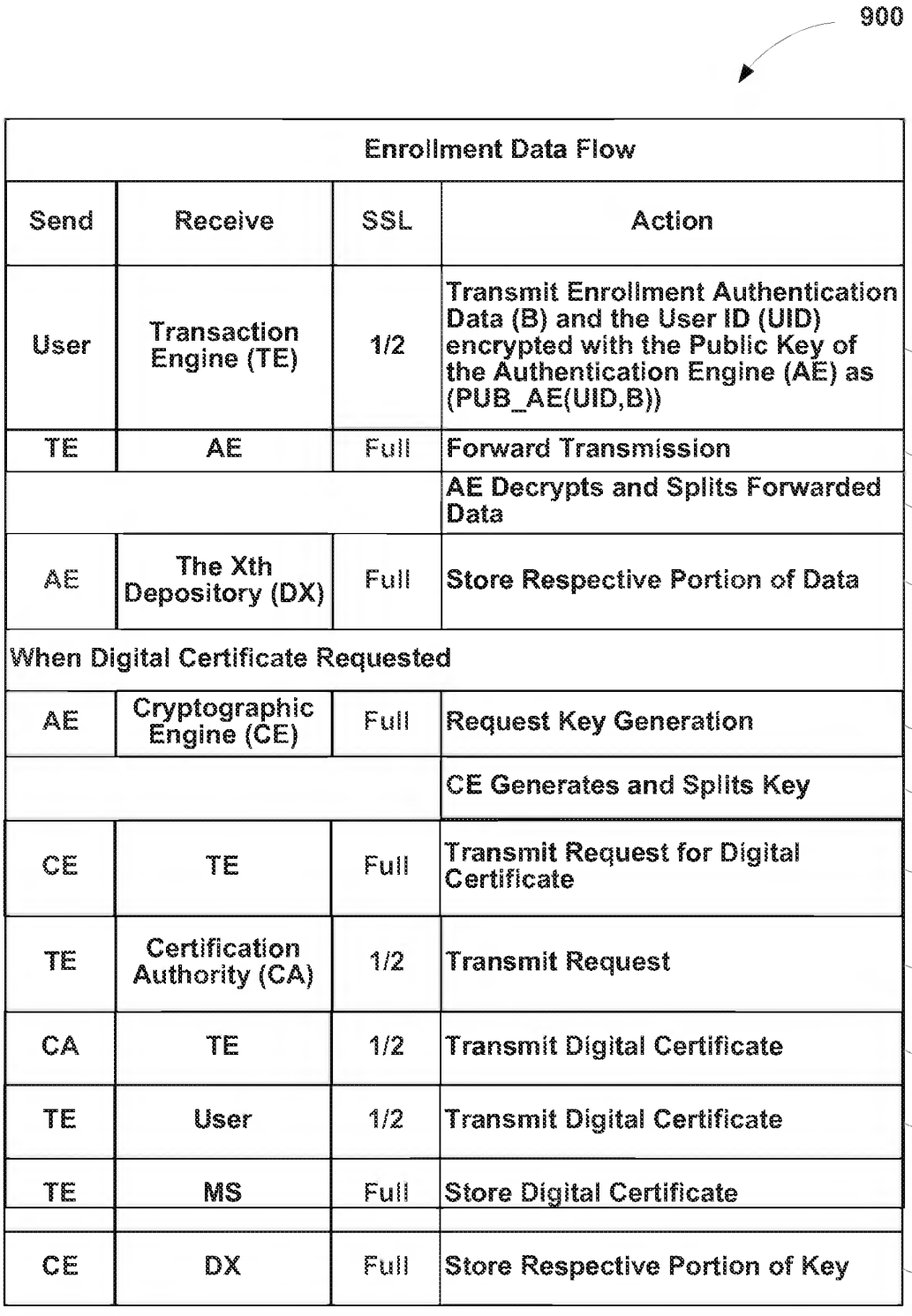

Begin
800
S = Received Data
805
Generate Random Number A
810
Generate Random Number C
820
Generate B = A XOR S
825
Generate D = C XOR S
830
Distribute A, C A, D B C, And B D
835
End

FIG. 8



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. 9, Panel A

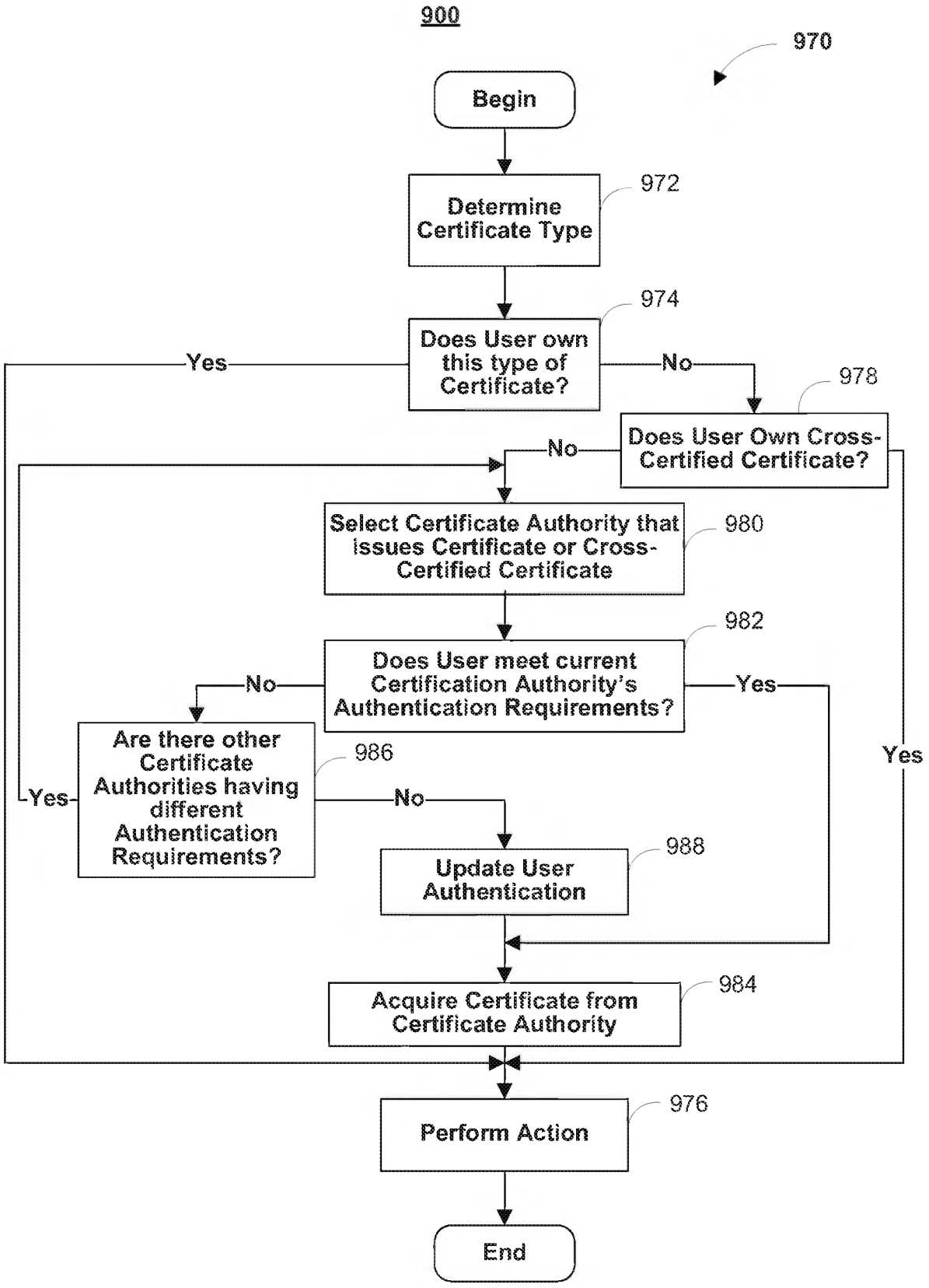
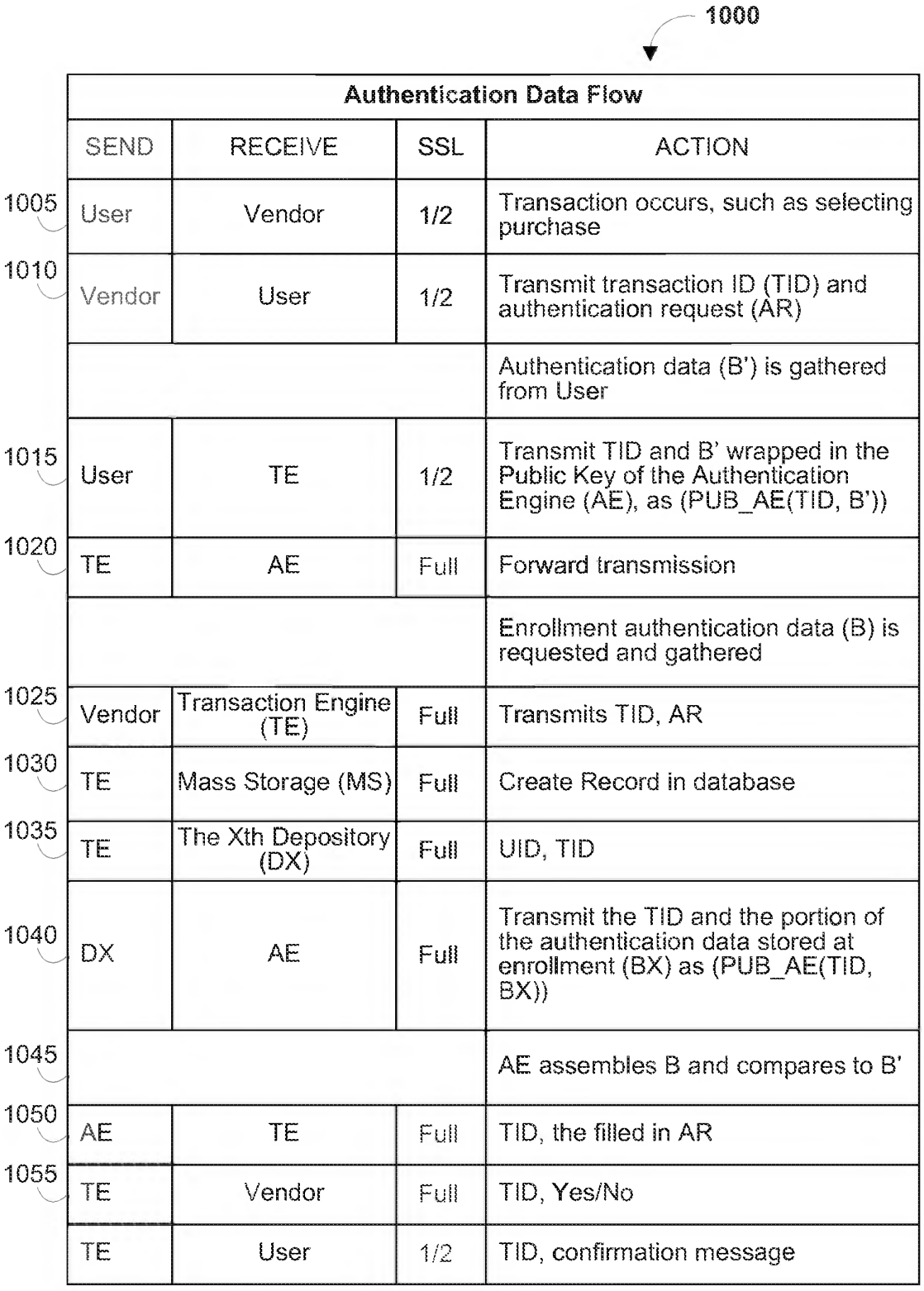

900
970
Begin
Determine Certificate Type
972
Does User own this type of Certificate?
974
Yes
No
Does User Own Cross-Certified Certificate?
978
No
Yes
Select Certificate Authority that issues Certificate or Cross-Certified Certificate
980
Does User meet current Certification Authority's Authentication 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



Authentication Data Flow			
SEND	RECEIVE	SSL	ACTION
User	Vendor	1/2	Transaction occurs, such as selecting purchase
Vendor	User	1/2	Transmit transaction ID (TID) and authentication request (AR)
			Authentication data (B') is gathered from User
User	TE	1/2	Transmit TID and B' wrapped in the Public Key of the Authentication Engine (AE), as (PUB_AE(TID, B'))
TE	AE	Full	Forward transmission
			Enrollment authentication data (B) is requested and gathered
Vendor	Transaction Engine (TE)	Full	Transmits TID, AR
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))
			AE assembles B and compares to B'
AE	TE	Full	TID, the filled in AR
TE	Vendor	Full	TID, Yes/No
TE	User	1/2	TID, confirmation message

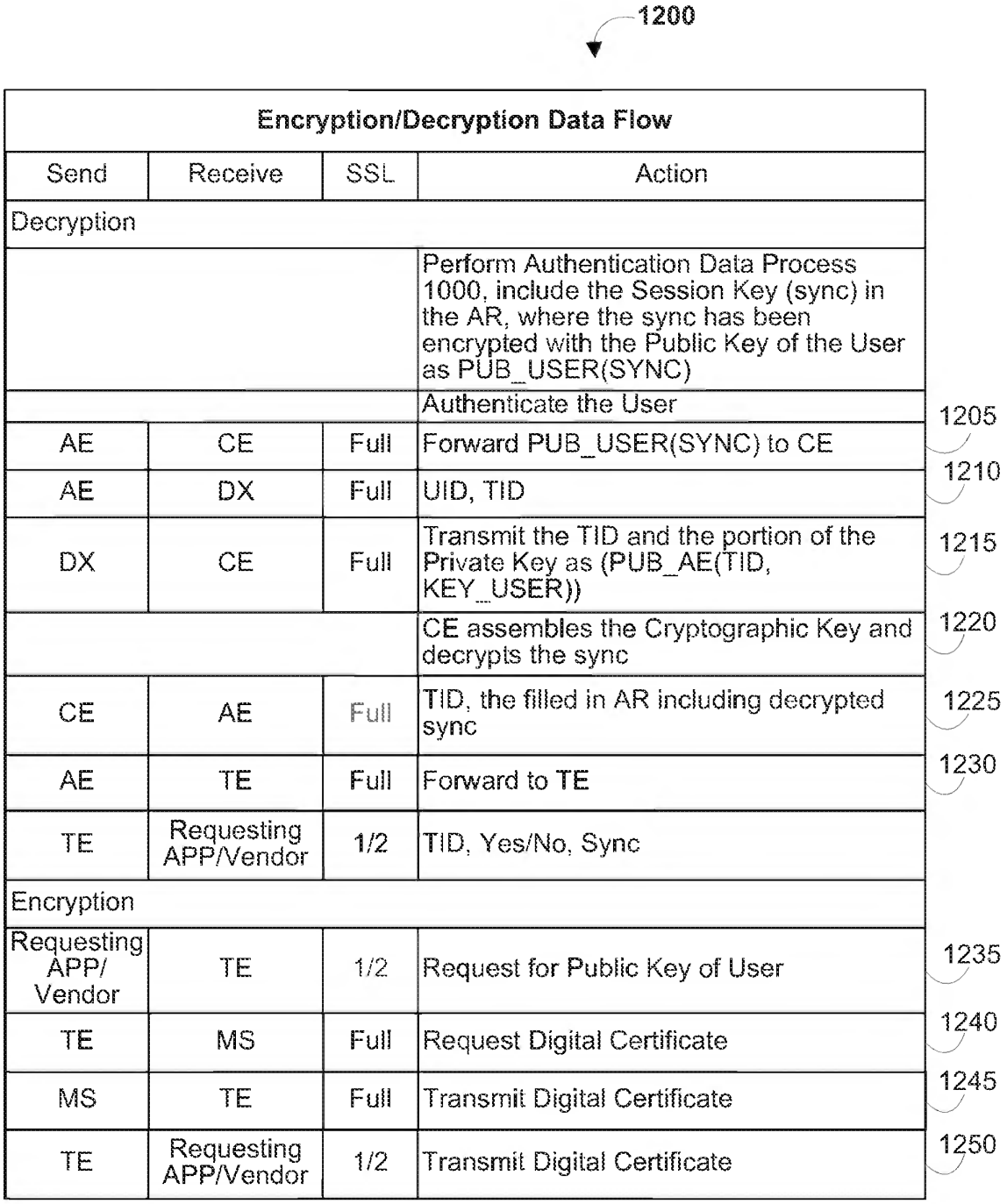
FIG. 10

1100

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				
Requesting APP/ Vendor	TE	1/2	Request for Public Key of User	1235
TE	MS	Full	Request Digital Certificate	1240
MS	TE	Full	Transmit Digital Certificate	1245
TE	Requesting APP/Vendor	1/2	Transmit Digital Certificate	1250

FIG. 12

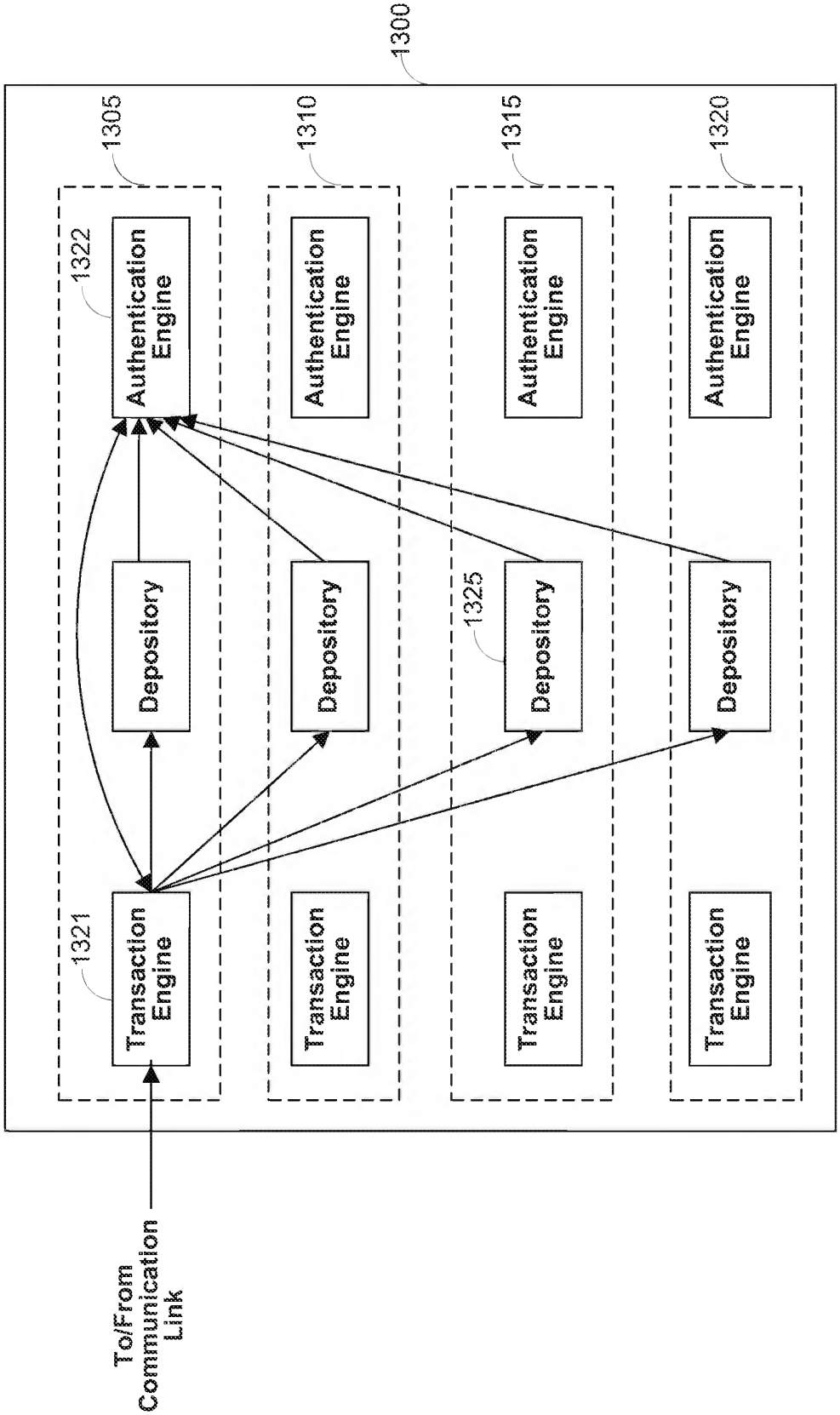

1300
1305
1310
1315
1320
1322
Authentication Engine
Authentication Engine
Authentication Engine
Authentication Engine
Depository
Depository
1325
Depository
Depository
1321
Transaction Engine
Transaction Engine
Transaction Engine
Transaction Engine
To/From Communication Link

FIG. 13

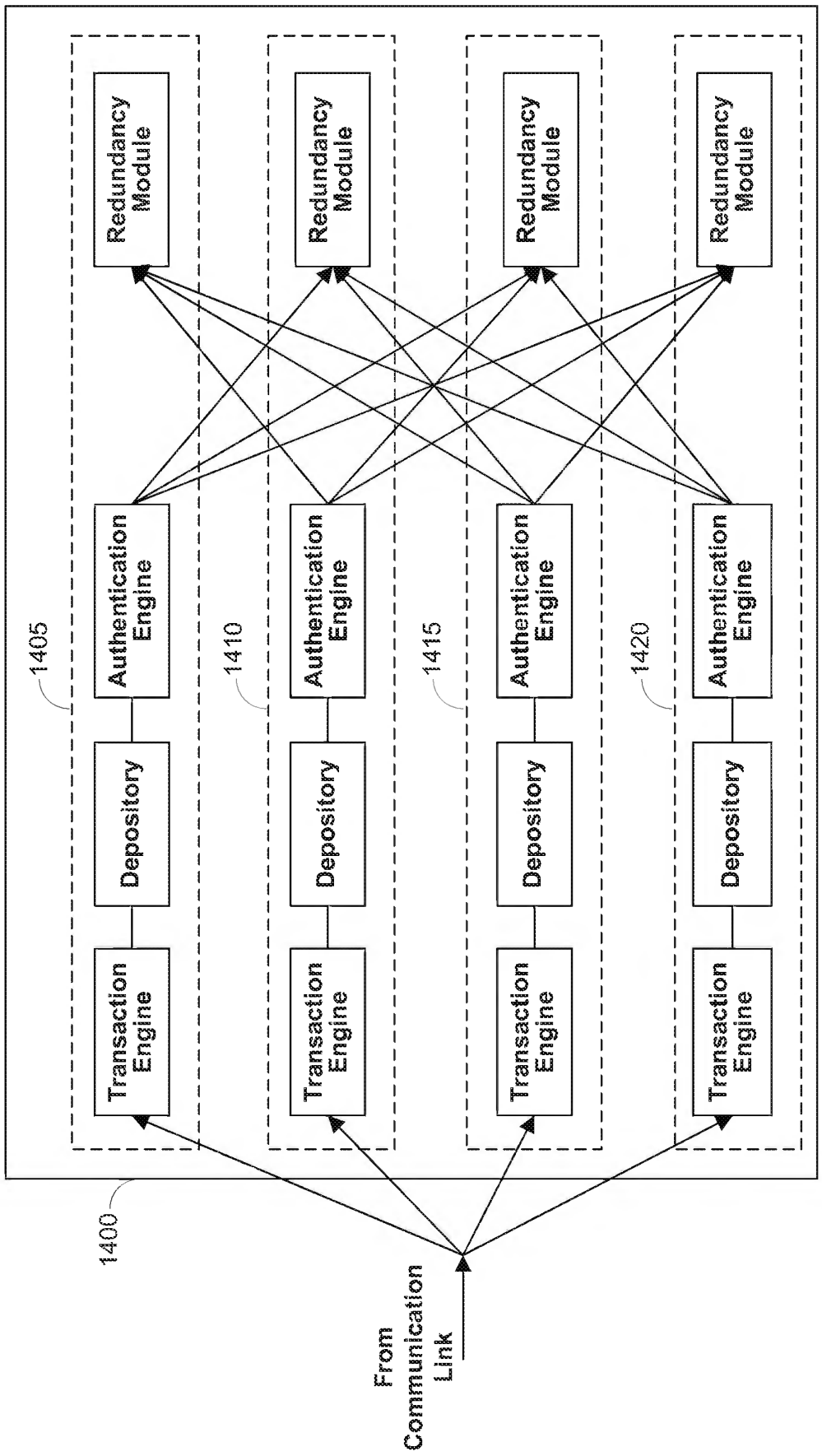

From Communication Link
1400
1405
1410
1415
1420
Transaction Engine
Depository
Authentication Engine
Redundancy Module

FIG. 14

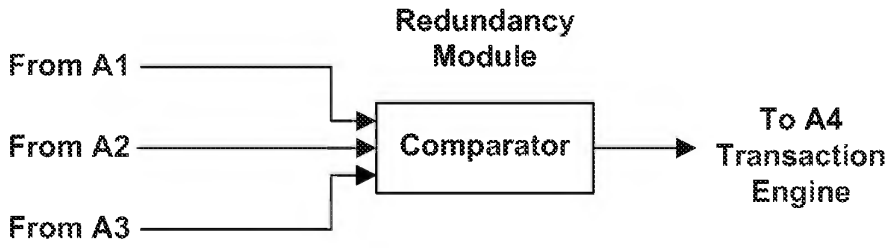

Redundancy
Module
From A1
From A2
From A3
Comparator
To A4
Transaction
Engine

FIG. 15

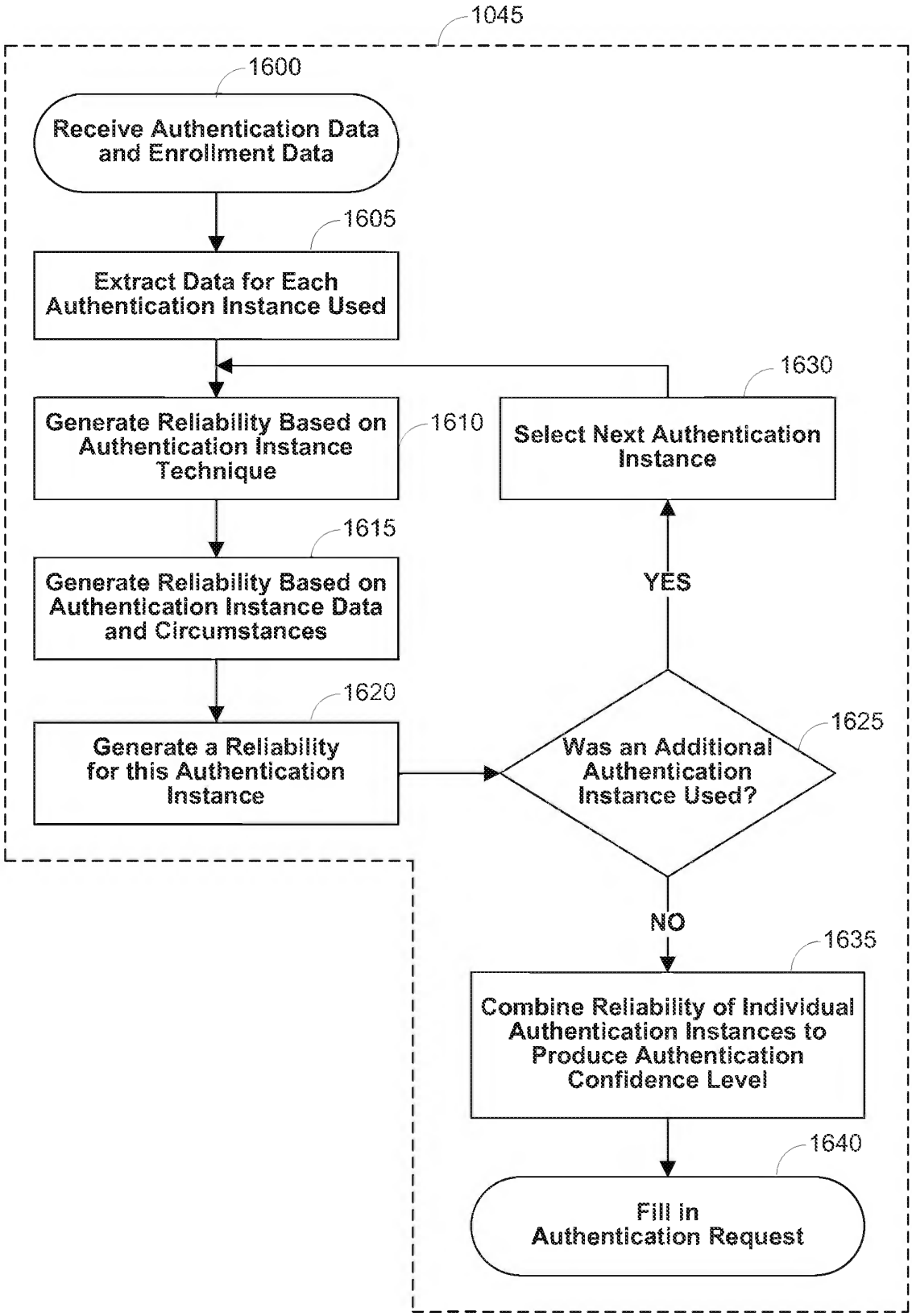

1045
1600
Receive Authentication Data and Enrollment Data
1605
Extract Data for Each Authentication Instance Used
1630
Select Next Authentication Instance
Generate Reliability Based on Authentication Instance Technique
1610
Generate Reliability Based on Authentication Instance Data and Circumstances
1615
YES
Generate a Reliability for this Authentication Instance
1620
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

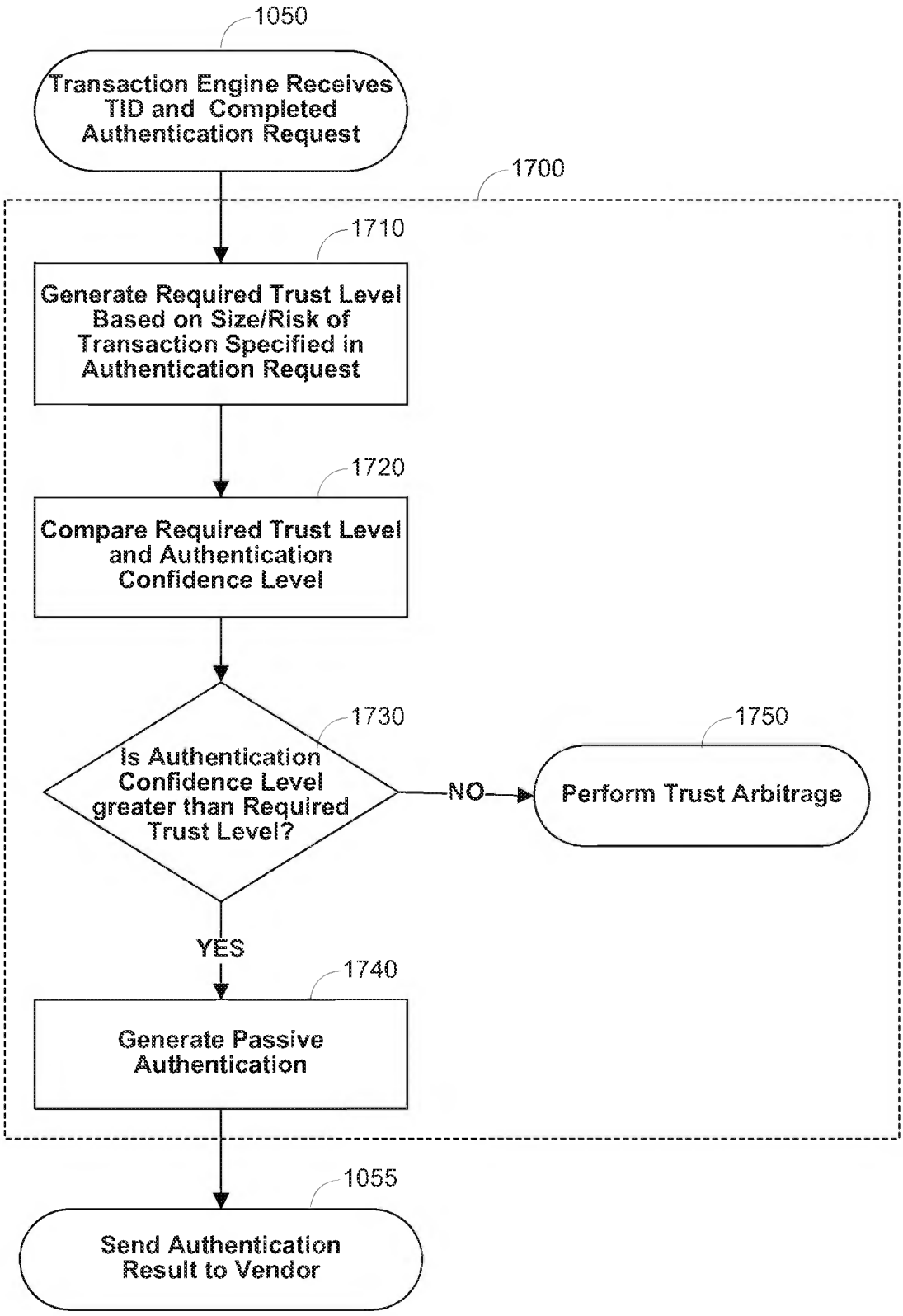

1050
Transaction Engine Receives TID and Completed Authentication Request
1700
1710
Generate Required Trust Level Based on Size/Risk of Transaction Specified in Authentication Request
1720
Compare Required Trust Level and Authentication Confidence Level
1730
Is Authentication Confidence Level greater than Required Trust Level?
NO
1750
Perform Trust Arbitrage
YES
1740
Generate Passive Authentication
1055
Send Authentication Result to Vendor

FIG. 17

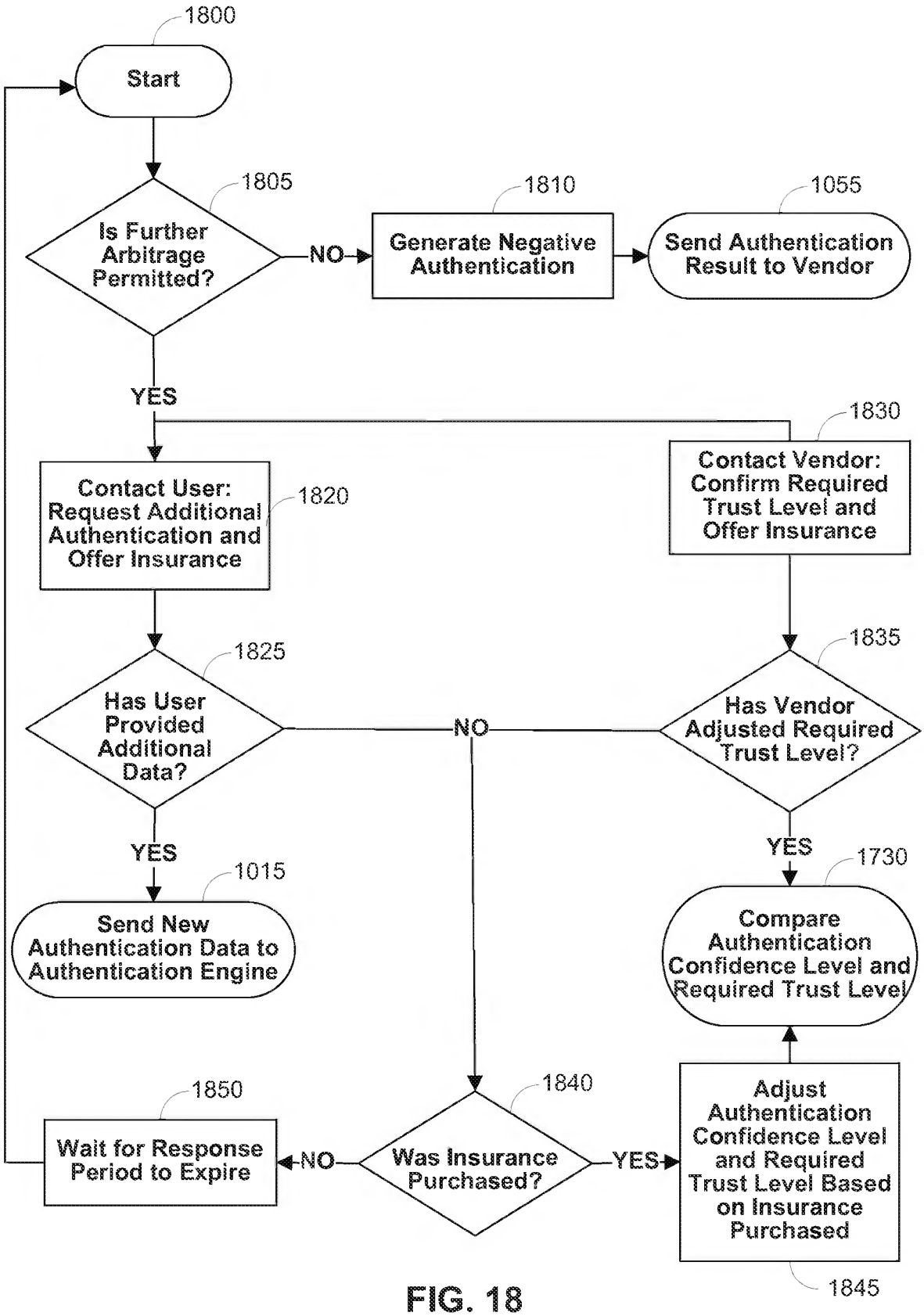

1800
Start
1805
Is Further Arbitrage Permitted?
NO
1810
Generate Negative Authentication
1055
Send Authentication Result to Vendor
YES
1830
Contact Vendor: Confirm Required Trust Level and Offer Insurance
Contact User: Request Additional Authentication and Offer Insurance
1820
1825
Has User Provided 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

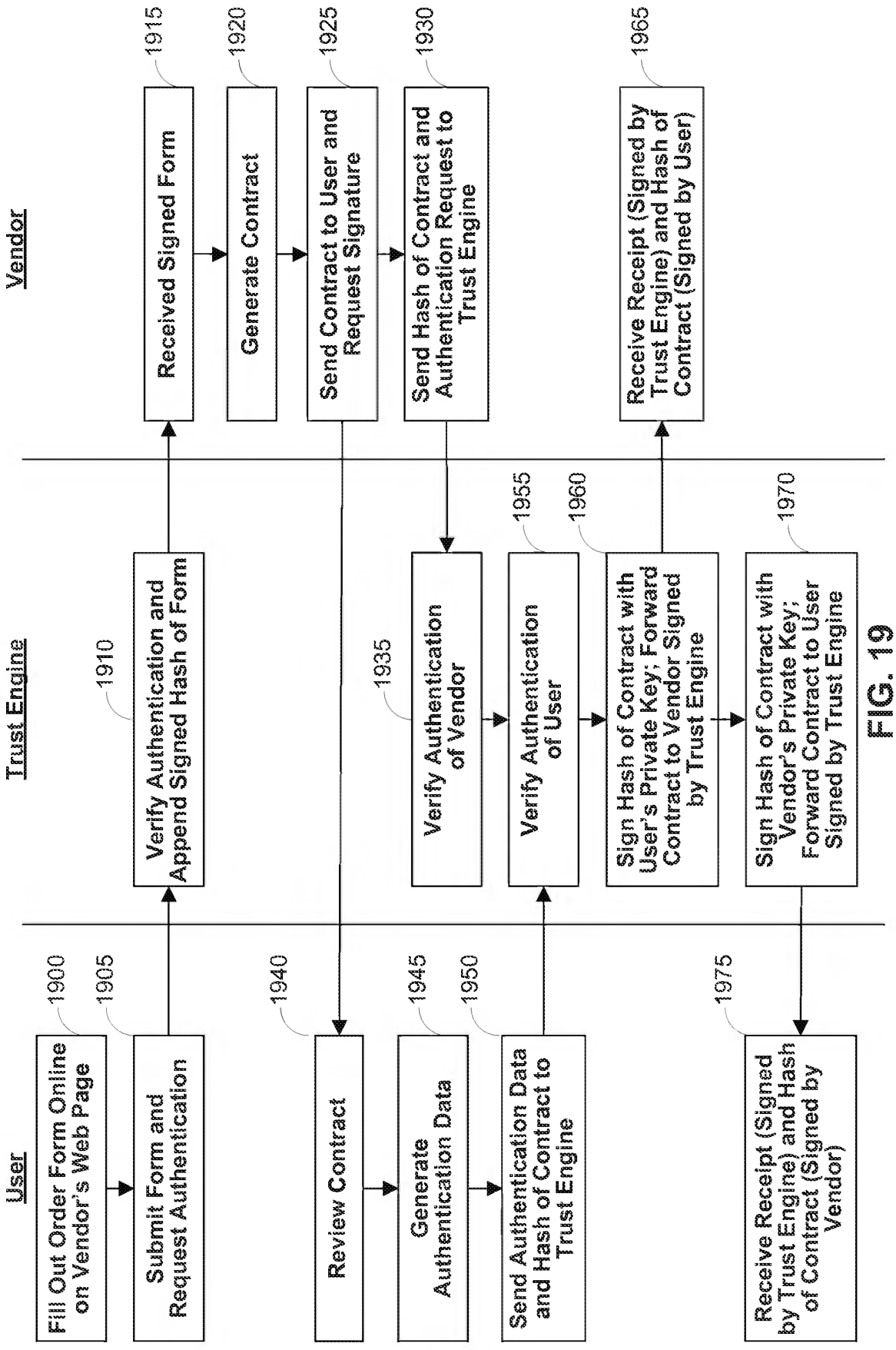

User
Trust Engine
Vendor
Fill Out Order Form Online on Vendor's Web Page
1900
Submit Form and Request Authentication
1905
Verify Authentication and Append Signed Hash of Form
1910
Received Signed Form
1915
Generate Contract
1920
Send Contract to User and Request Signature
1925
Send Hash of Contract and Authentication Request to Trust Engine
1930
Review Contract
1940
Generate Authentication Data
1945
Send Authentication Data and Hash of Contract to Trust Engine
1950
Verify Authentication of Vendor
1935
Verify Authentication of User
1955
Sign Hash of Contract with User's Private Key; Forward Contract to Vendor Signed by Trust Engine
1960
Receive Receipt (Signed by Trust Engine) and Hash of Contract (Signed by User)
1965
Sign Hash of Contract with Vendor's Private Key; Forward Contract to User Signed by Trust Engine
1970
Receive Receipt (Signed by Trust Engine) and Hash of Contract (Signed by Vendor)
1975

FIG. 19

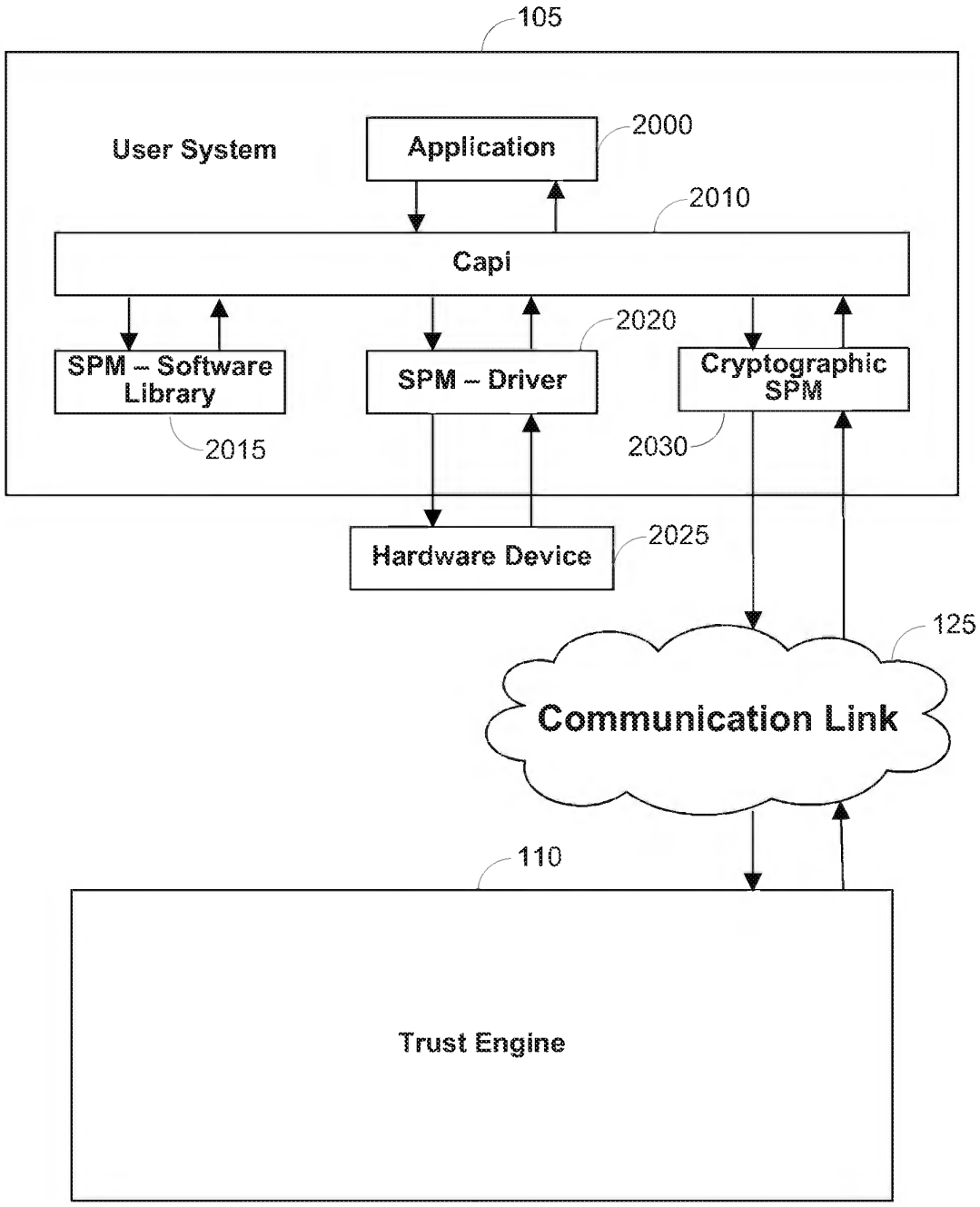

105
User System
Application
2000
2010
Capi
2020
SPM – Software Library
SPM – Driver
Cryptographic SPM
2015
2030
Hardware Device
2025
125
Communication Link
110
Trust Engine

FIG. 20

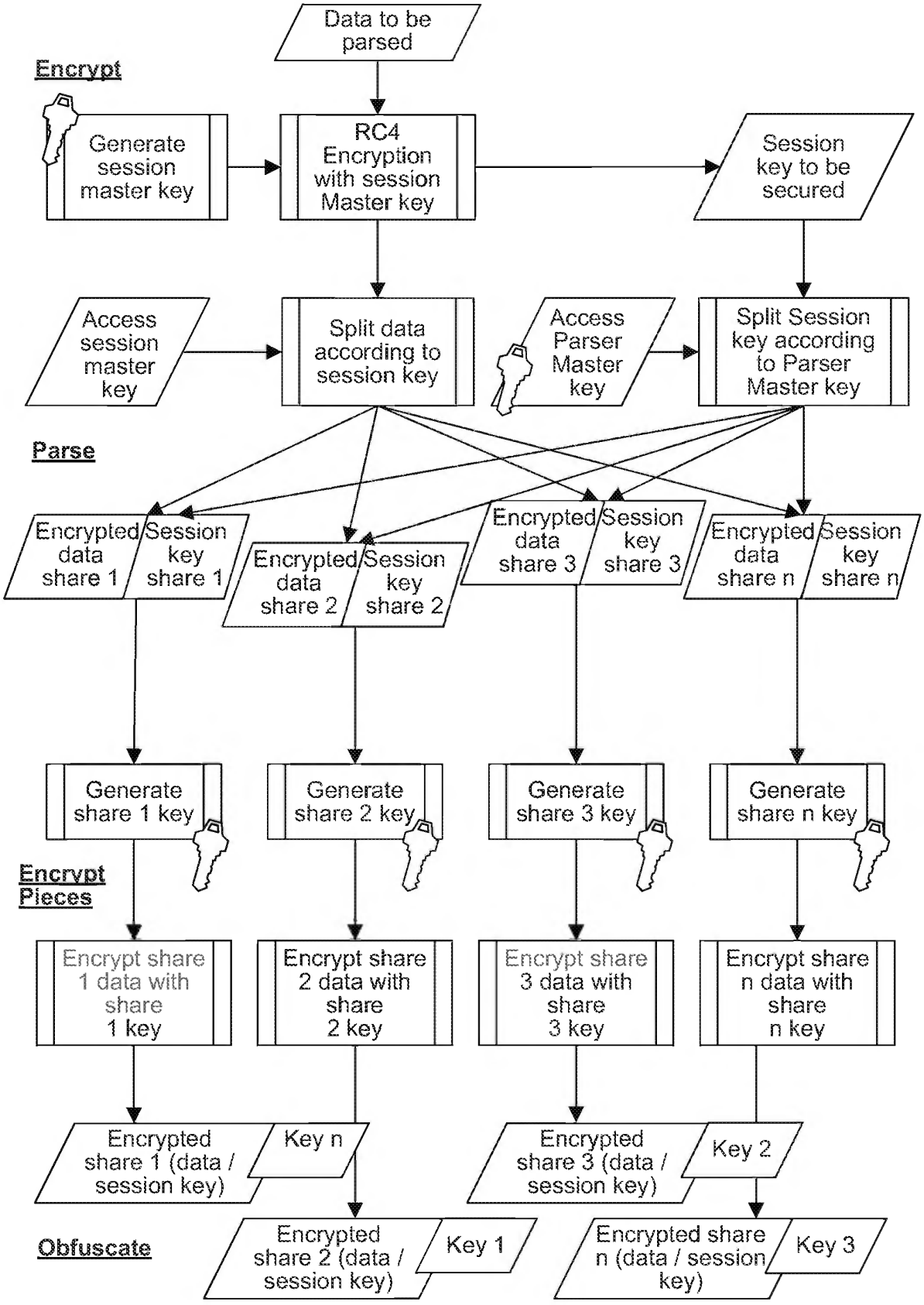

Data to be parsed
Encrypt
Generate session master key
RC4 Encryption with session Master key
Session key to be secured
Access session master key
Split data according to session key
Access Parser Master key
Split Session key according to Parser Master key
Parse
Encrypted data share 1
Session key share 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

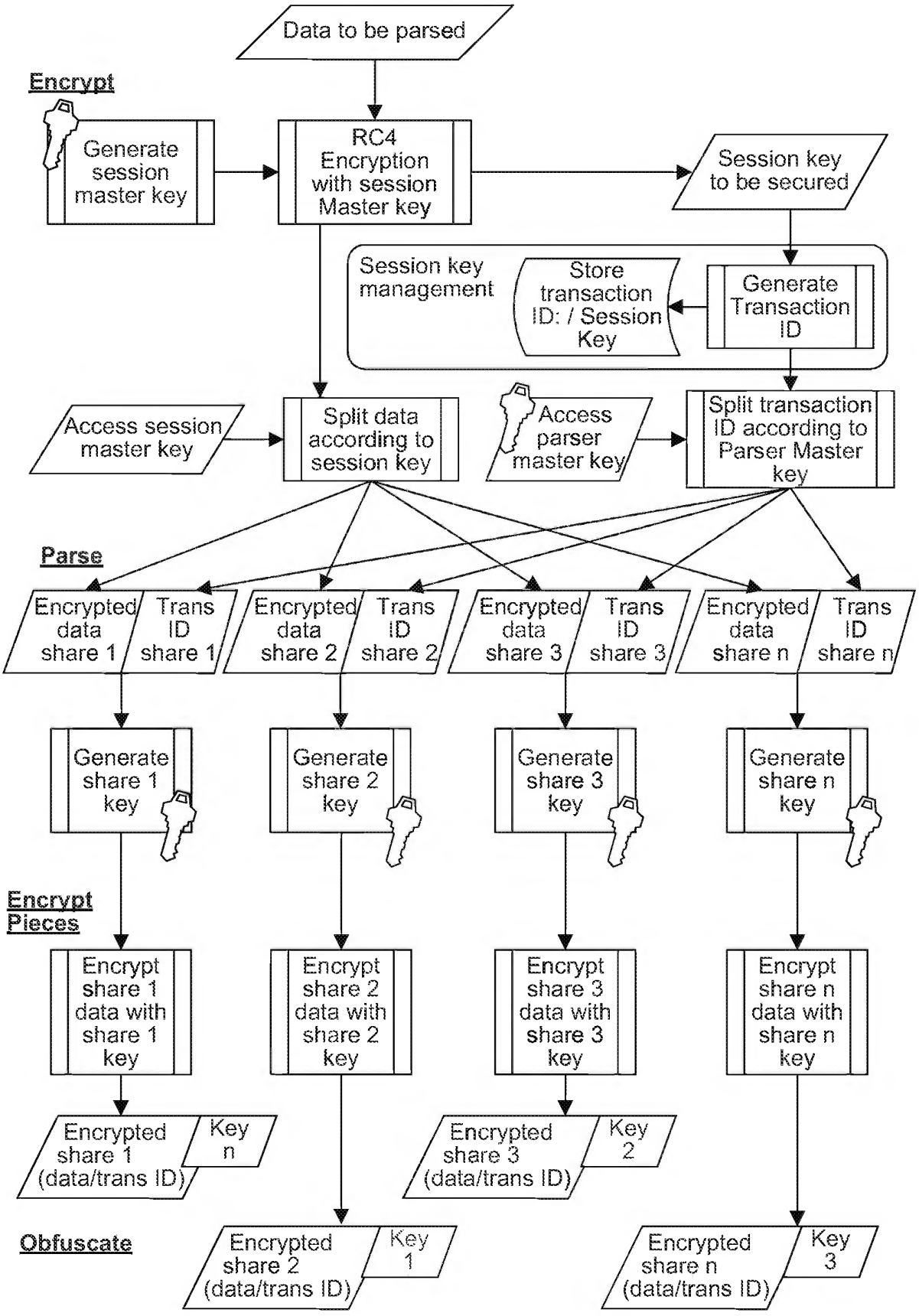

Data to be parsed
Encrypt
Generate session master key
RC4 Encryption with session Master key
Session key to be secured
Session key management
Store transaction ID: / Session Key
Generate Transaction ID
Access session master key
Split data according to session key
Access parser master key
Split transaction 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

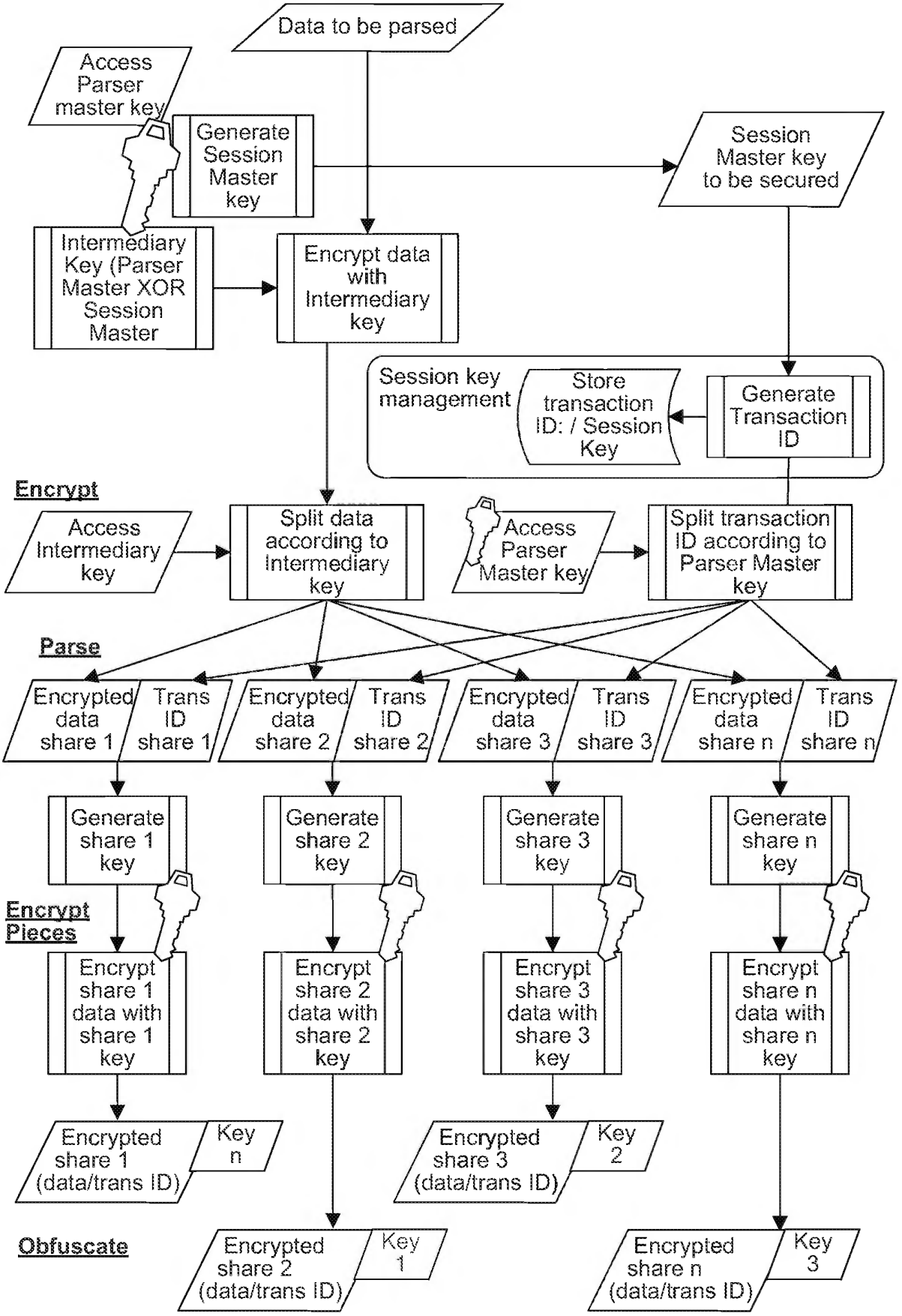

Data to be parsed
Access Parser master key
Generate Session Master key
Session Master key to be secured
Intermediary Key (Parser Master XOR Session Master
Encrypt data with Intermediary key
Session key management
Store transaction ID: / Session Key
Generate Transaction ID
Encrypt
Access Intermediary 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

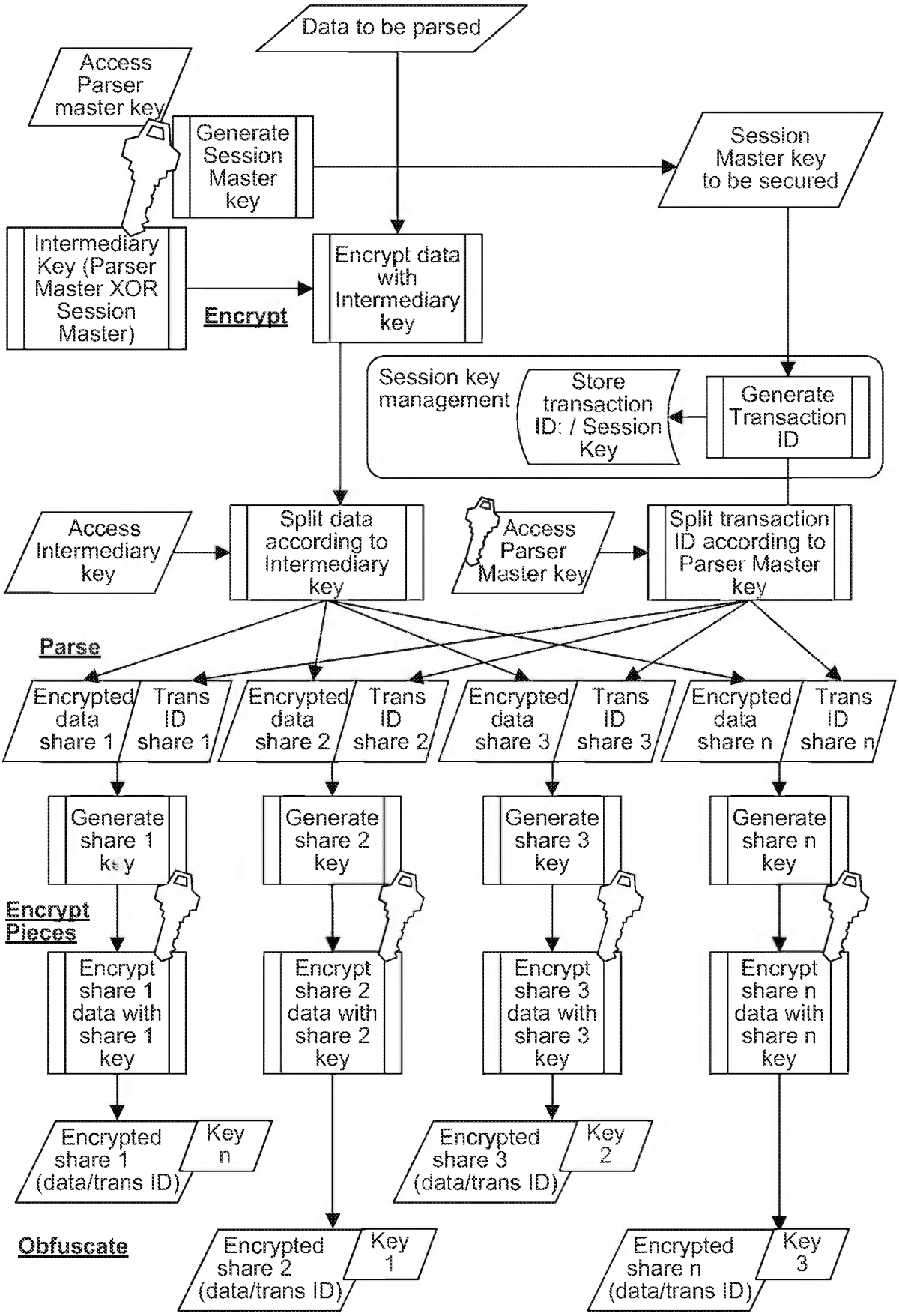

Data to be parsed
Access Parser master key
Generate Session Master key
Session Master key to be secured
Intermediary Key (Parser Master XOR Session Master)
Encrypt
Encrypt data with Intermediary key
Session key management
Store transaction ID: / Session Key
Generate Transaction ID
Access Intermediary 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

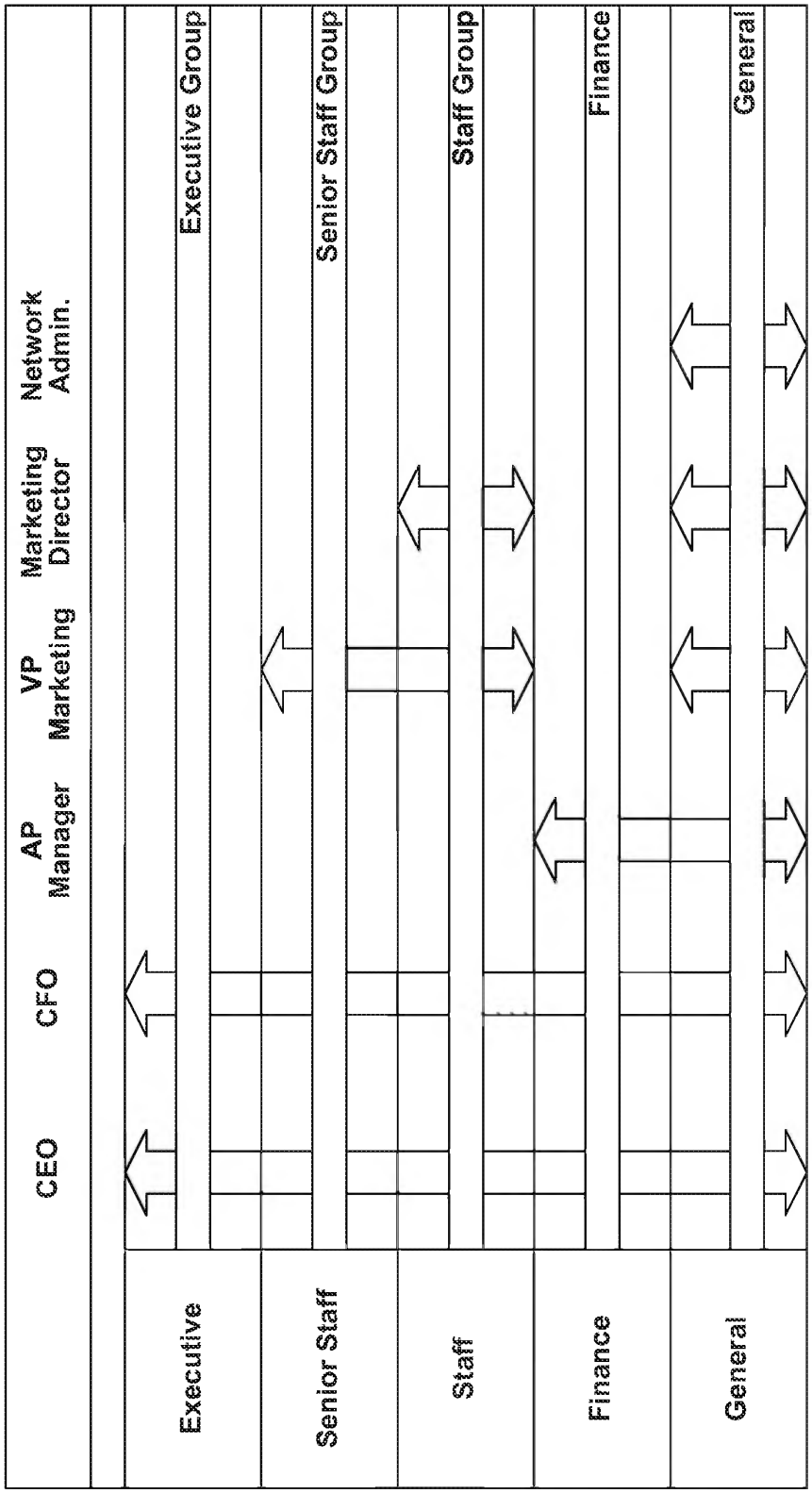

CEO
CFO
AP Manager
VP Marketing
Marketing Director
Network Admin.
Executive
Executive Group
Senior Staff
Senior Staff Group
Staff
Staff Group
Finance
Finance
General
General

FIG. 25

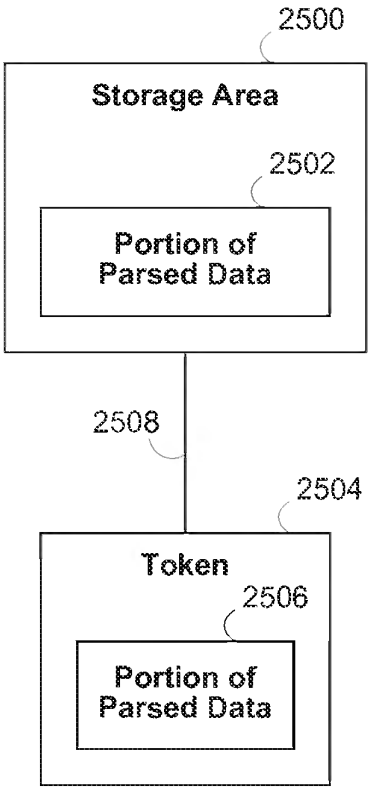

2500
Storage Area
2502
Portion of Parsed Data
2508
2504
Token
2506
Portion of Parsed Data

FIG. 26

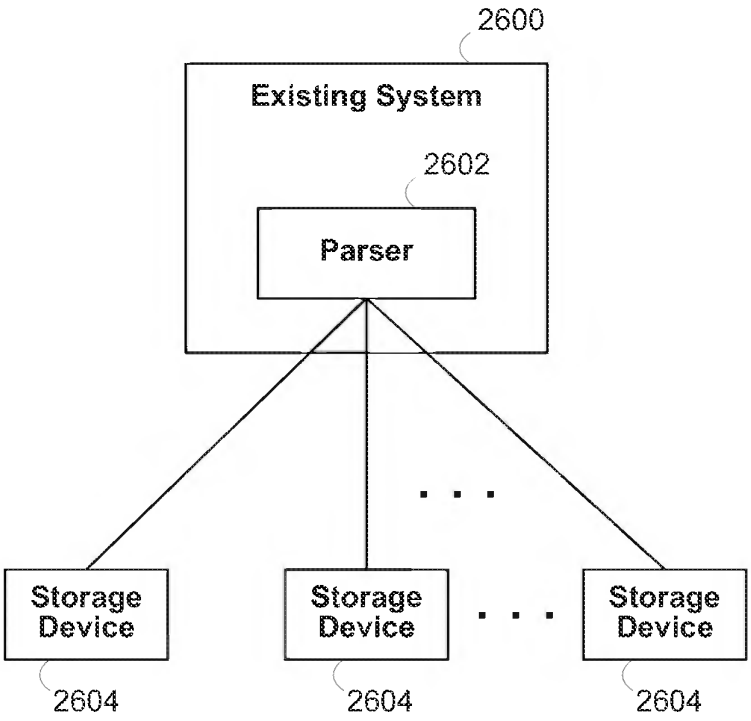

2600
Existing System
2602
Parser
Storage Device
2604
Storage Device
2604
Storage Device
2604

FIG. 27

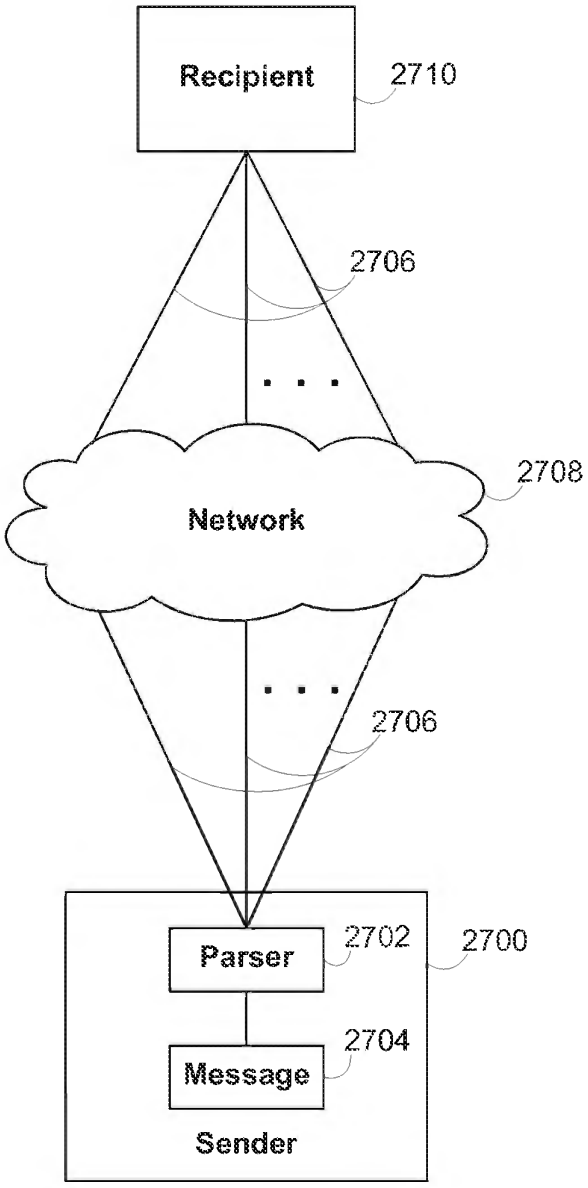

Recipient
2710
2706
2708
Network
2706
Parser
2702
2700
2704
Message
Sender

FIG. 28

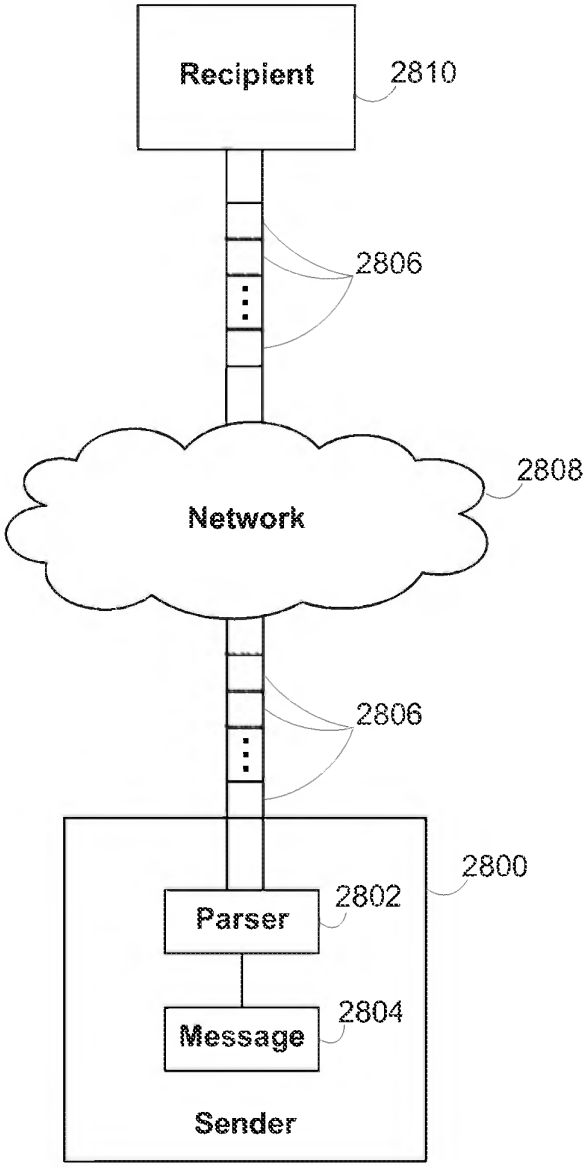

Recipient
2810
2806
Network
2808
2806
2800
Parser
2802
Message
2804
Sender

FIG. 29

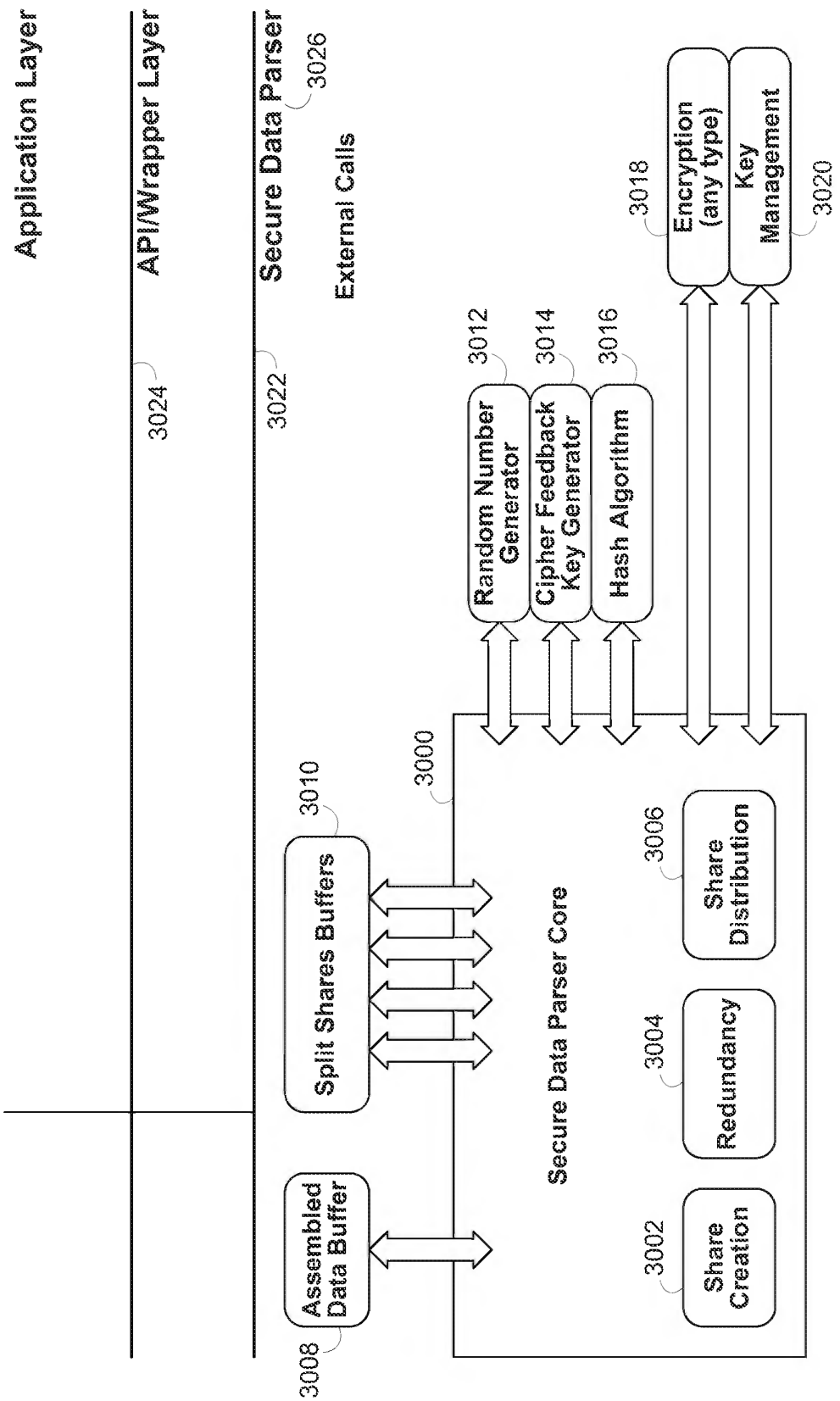

Application Layer
API/Wrapper Layer
Secure Data Parser
3026
External Calls
3024
3022
3012
3014
3016
3018
3020
Random Number Generator
Cipher Feedback Key Generator
Hash Algorithm
Encryption (any type)
Key Management
3000
3010
Split Shares Buffers
Secure Data Parser Core
3006
Share Distribution
3004
Redundancy
3002
Share Creation
3008
Assembled Data Buffer

FIG. 30

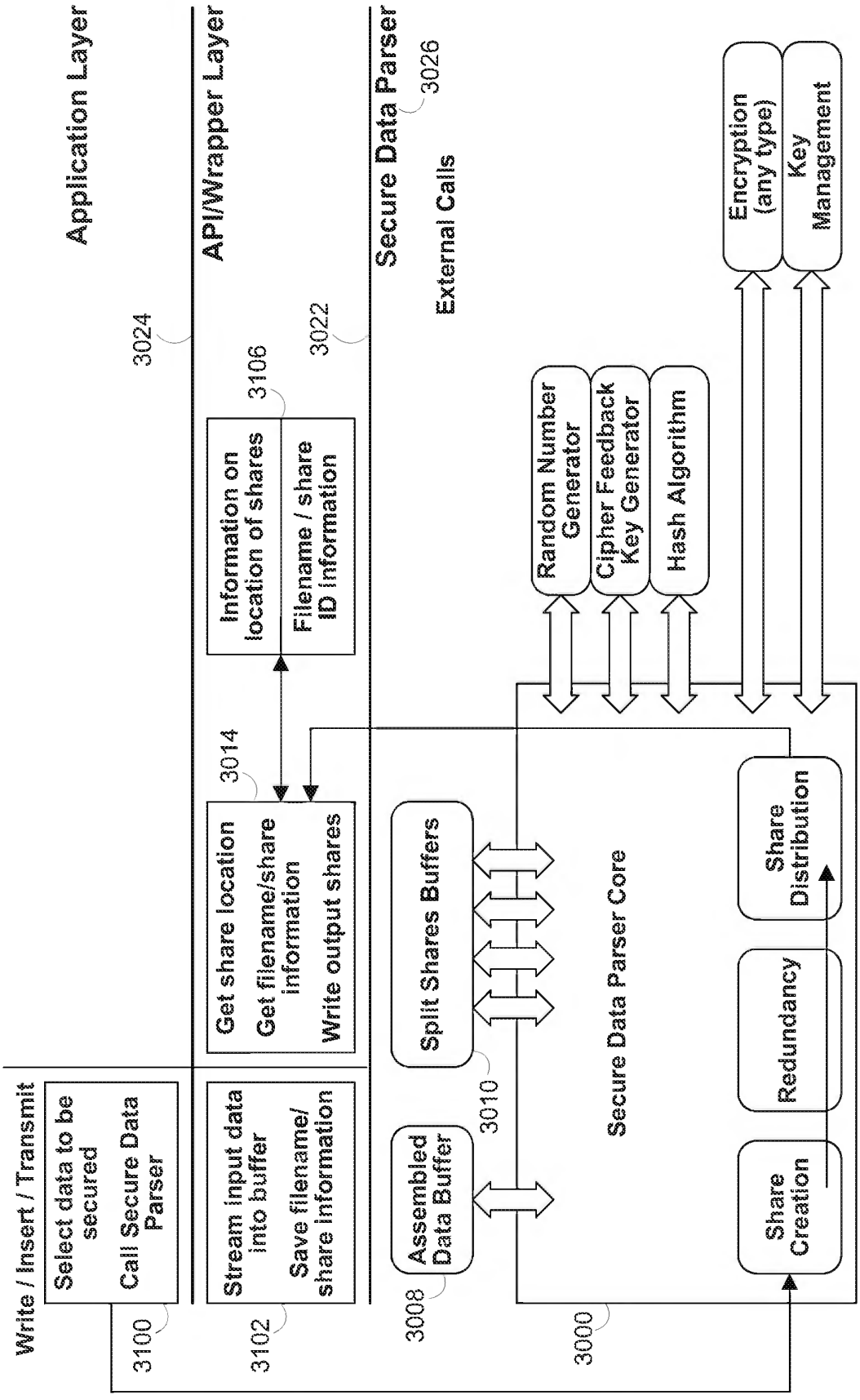

Application Layer
API/Wrapper Layer
Secure Data Parser
3026
External Calls
3024
3022
3106
3014
Write / Insert / Transmit
Select data to be secured
Call Secure Data Parser
3100
Stream input data into buffer
Save filename/ share information
3102
Get share location
Get filename/share information
Write output shares
Information on location of shares
Filename / share ID information
Split Shares Buffers
Assembled Data Buffer
3010
3008
Secure Data Parser Core
3000
Share Creation
Redundancy
Share Distribution
Random Number Generator
Cipher Feedback Key Generator
Hash Algorithm
Encryption (any type)
Key Management

FIG. 31

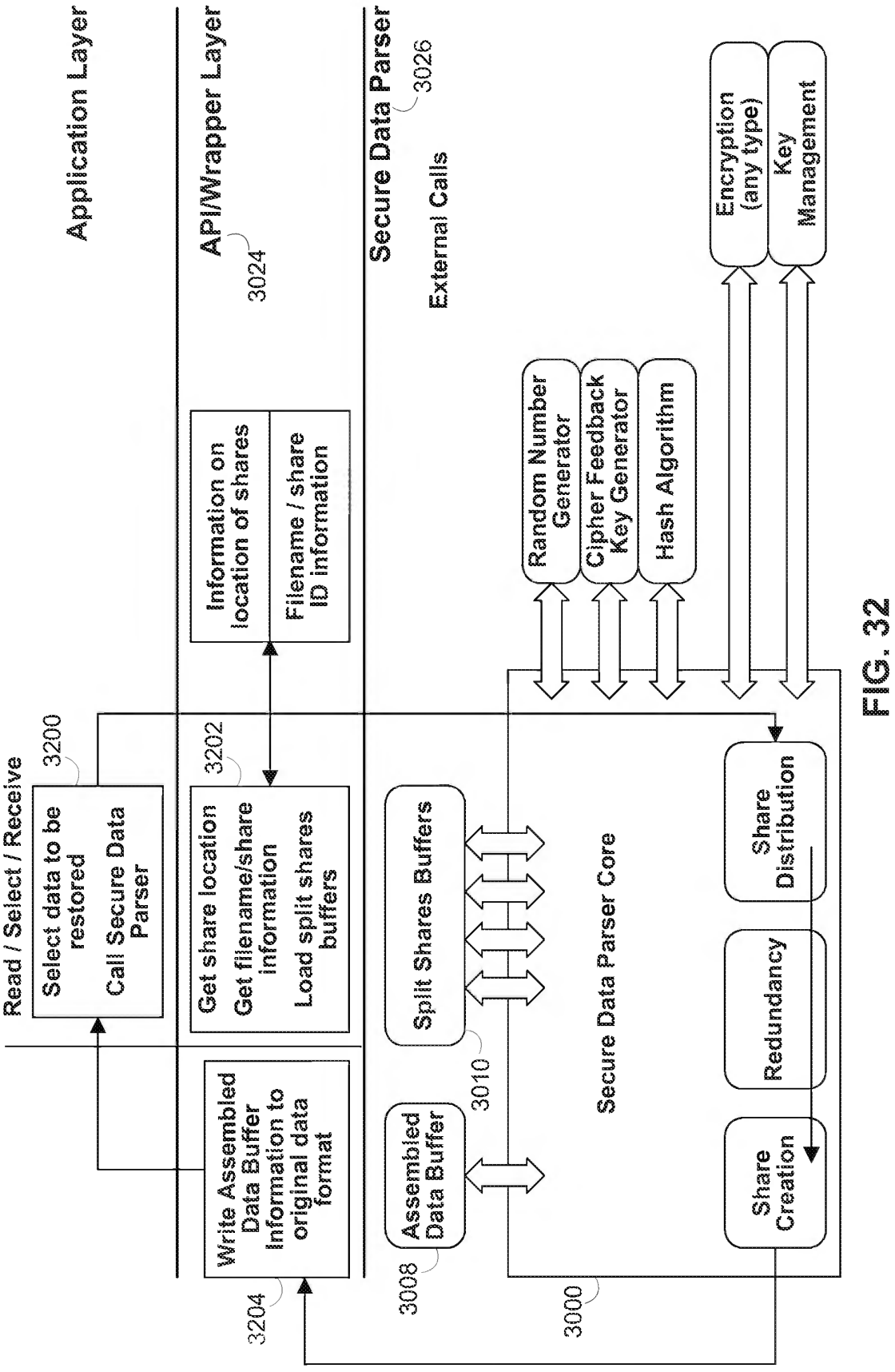

Application Layer
API/Wrapper Layer
3024
Secure Data Parser
3026
External Calls
Read / Select / Receive
3200
Select data to be restored
Call Secure Data Parser
3202
Get share location
Get filename/share information
Load split shares buffers
Information on location of shares
Filename / share ID information
Write Assembled Data Buffer Information to original data format
3204
Split Shares Buffers
3010
Assembled Data Buffer
3008
Secure Data Parser Core
3000
Random Number Generator
Cipher Feedback Key Generator
Hash Algorithm
Encryption (any type)
Key Management
Share Distribution
Redundancy
Share Creation

FIG. 32

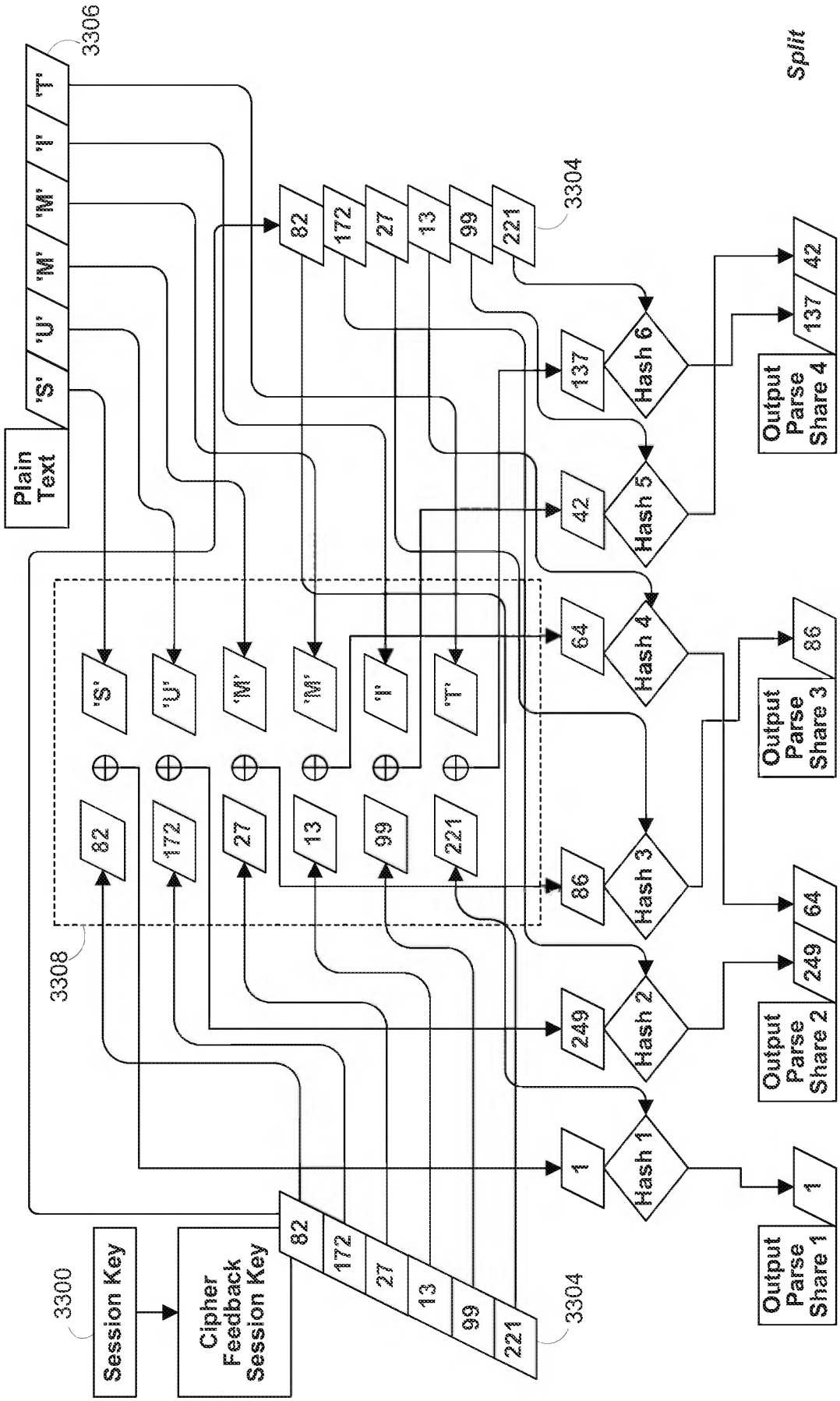

3306
Plain Text
'S' 'U' 'M' 'M' 'I' 'T'
3304
82 172 27 13 99 221
3308
'S' 'U' 'M' 'M' 'I' 'T'
82 172 27 13 99 221
3300
Session Key
Cipher Feedback Session Key
82 172 27 13 99 221
3304
Split
1 249 86 64 42 137
Hash 1
Hash 2
Hash 3
Hash 4
Hash 5
Hash 6
Output Parse Share 1
1
Output Parse Share 2
249 64
Output Parse Share 3
86
Output Parse Share 4
137 42

FIG. 33

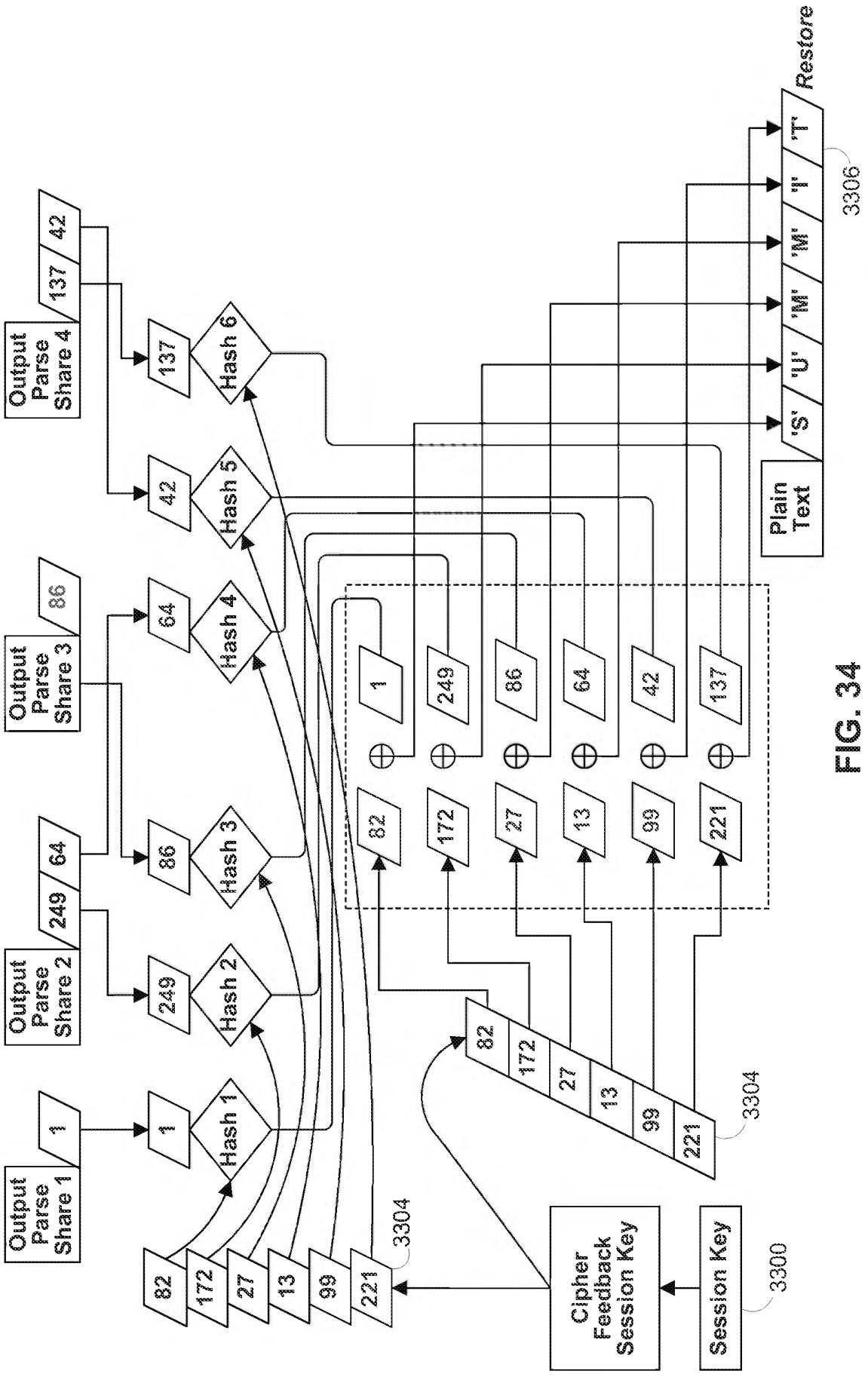

Output Parse Share 1
Output Parse Share 2
Output Parse Share 3
Output Parse Share 4
Hash 1
Hash 2
Hash 3
Hash 4
Hash 5
Hash 6
Cipher Feedback Session Key
Session Key
Plain Text
Restore
3300
3304
3306
82
172
27
13
99
221
1
249
86
64
42
137
'S'
'U'
'M'
'M'
'I'
'T'

FIG. 34

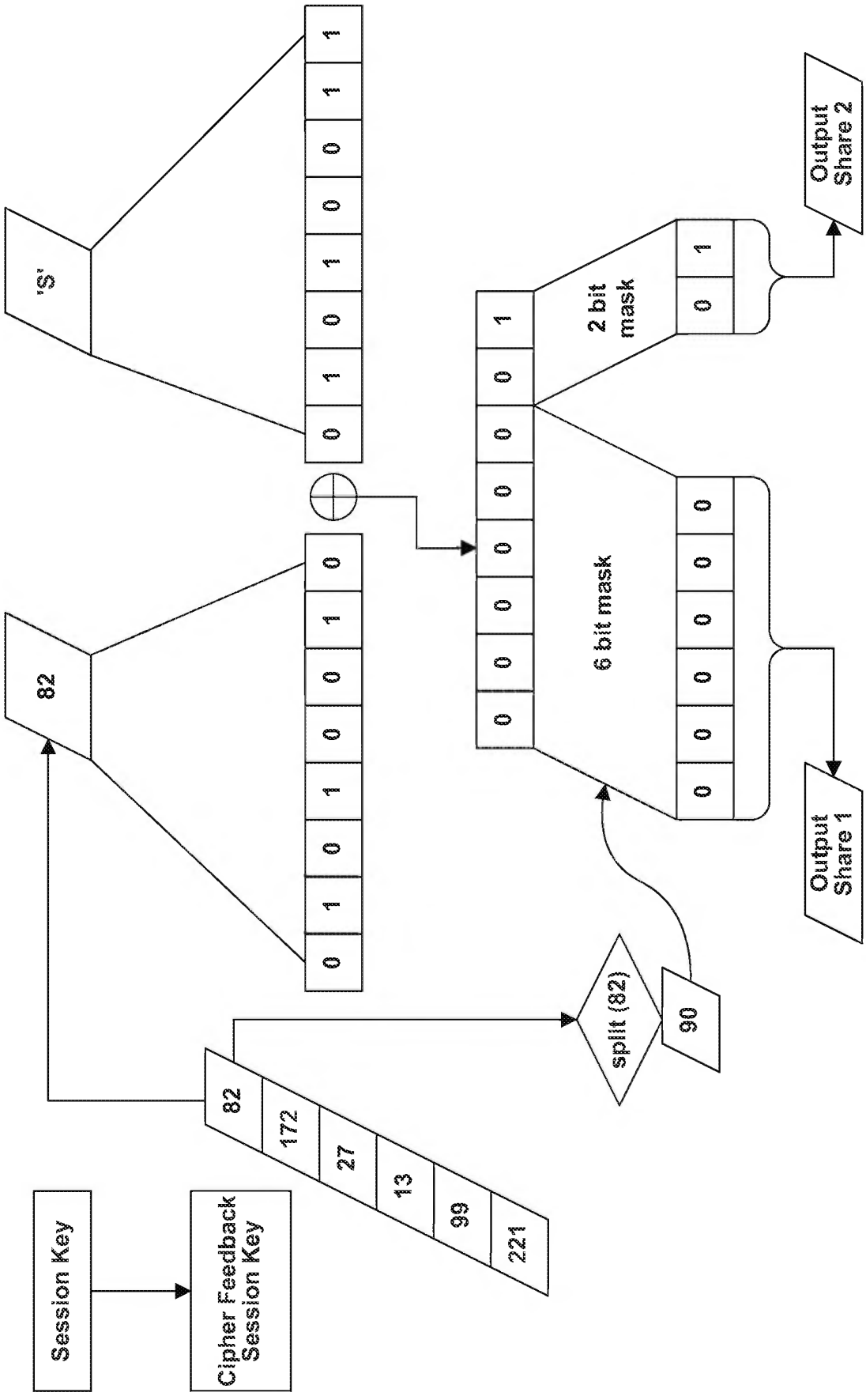

Session Key
Cipher Feedback Session Key
82
172
27
13
99
221
split (82)
90
82
'S'
0 1 0 1 0 0 1 0
0 1 1 0 1 0 0 1
6 bit mask
2 bit mask
0 0 0 0 0 0
0 0 0 0 0 1
0 0 0 0 0 0
0 0 0 0 0 1
Output Share 1
Output Share 2

FIG. 35

PATENTS
104093-0002-105

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

PATENT APPLICATION

Applicants	:	Rick L. Orsini et al.		
Application No.:	:	13/371,363	Confirmation No.:	7984
Filed	:	February 10, 2012		
For	:	SECURE DATA PARSER METHOD AND SYSTEM		
Art Unit	:	2827		

East Palo Alto, CA
March 8, 2012

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

REPLY TO NOTICE TO FILE CORRECTED APPLICATION PAPERS

Sir:

In reply to the Notice to File Corrected Application Papers mailed February 29, 2012, applicants hereby submit 36 Replacement Drawing Sheets (Figures 1-35) in compliance with 37 C.F.R. 1.84 and 37 C.F.R. 1.121(d).

Respectfully submitted,

/Matthew S. Bertenthal/
Matthew S. Bertenthal
Agent for Applicants
Registration No. 61,129
Ropes & Gray LLP
Customer No. 1473

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/371,363	02/10/2012	2827	2590	104093-0002-105	27	3

CONFIRMATION NO. 7984

UPDATED FILING RECEIPT

1473
ROPES & GRAY LLP
PATENT DOCKETING 39/361
1211 AVENUE OF THE AMERICAS
NEW YORK, NY 10036-8704

OC000000053101468

Date Mailed: 03/19/2012

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

Applicant(s)

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

Assignment For Published Patent Application

Security First Corp., Rancho Santa Margarita, CA

Power of Attorney: The patent practitioners associated with Customer Number 1473

Domestic Priority data as claimed by applicant

This application is a CON of 11/258,839 10/25/2005
which claims benefit of 60/718,185 09/16/2005
and claims benefit of 60/622,146 10/25/2004

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)

If Required, Foreign Filing License Granted: 02/24/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/371,363**

Projected Publication Date: 06/28/2012

Non-Publication Request: No

Early Publication Request: No

Title

SECURE DATA PARSER METHOD AND SYSTEM

Preliminary Class

365

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

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

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

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

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

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as

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 USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage, facilitate, and accelerate 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.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 13/371,363

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	380
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	620
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	250
TOTAL CLAIMS (37 CFR 1.16(i))	27 minus 20 =	* 7			OR	x 60 =	420
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*				x 250 =	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).						620
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	2290

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	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
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 NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/371,363	02/10/2012	Rick L. Orsini	104093-0002-105	7984

1473 7590 04/18/2012

ROPES & GRAY LLP
PATENT DOCKETING 39/361
1211 AVENUE OF THE AMERICAS
NEW YORK, NY 10036-8704

EXAMINER	
VU, KIM Y	

ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
04/18/2012	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):

USPatentMail@ropesgray.com
USPatentMail2@ropesgray.com

Doc Code: TRACK1.GRANT

Decision Granting Request for Prioritized Examination (Track I or After RCE)	Application No.:13/368363

1. THE REQUEST FILED 02/10/12 IS **GRANTED**.

The above-identified application has met the requirements for prioritized examination

A. ☒ for an original nonprovisional application (Track I).
B. ☐ for an application undergoing continued examination (RCE).

2. **The above-identified application will undergo prioritized examination.** The application will be accorded special status throughout its entire course of prosecution until one of the following occurs:

A. filing a **petition for extension of time** to extend the time period for filing a reply;
B. filing an **amendment to amend the application to contain more than four independent claims, more than thirty total claims**, or a multiple dependent claim;
C. filing a **request for continued examination**;
D. filing a notice of appeal;
E. filing a request for suspension of action;
F. mailing of a notice of allowance;
G. mailing of a final Office action;
H. completion of examination as defined in 37 CFR 41.102; or
I. abandonment of the application.

Telephone inquiries with regard to this decision should be directed to Tod Swann at 571-272-3612. In his absence, calls may be directed to Kim Vu, 571-272-3859.

/Tod Swann/
[*Signature*]

MQAS
(Title)

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. 7984

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/371,363	02/10/2012 RULE	726	2492	104093-0002-105

APPLICANTS

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

**** CONTINUING DATA ***************************

This application is a CON of 11/258,839 10/25/2005
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 ****

02/24/2012

Foreign Priority claimed	35 USC 119(a-d) conditions met	Verified and Acknowledged	Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
☐ Yes ☑ No	☐ Yes ☑ No	/MICHAEL W CHAO/ Examiner's Signature	☐ Initials	TX	36	27	3

ADDRESS

ROPES & GRAY LLP
PATENT DOCKETING 39/361
1211 AVENUE OF THE AMERICAS
NEW YORK, NY 10036-8704
UNITED STATES

TITLE

SECURE DATA PARSER METHOD AND SYSTEM

FILING FEE RECEIVED	FEES: Authority has been given in Paper	
2590	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
L2	1861	713/153.ccls.	US-PGPUB; USPAT; EPO; IBM_TDB	AND	OFF	2012/05/04 10:58
L4	3030	726/27.ccls.	US-PGPUB; USPAT; EPO; IBM_TDB	AND	OFF	2012/05/04 10:59
L5	36	(security adj first).asn.	US-PGPUB; USPAT; EPO; IBM_TDB	OR	OFF	2012/05/04 11:34
L6	92	(orsini and rick or hare and mark or davenport and rojer or winick and steven).in.	US-PGPUB; USPAT; EPO; IBM_TDB	OR	OFF	2012/05/04 11:48
S4	38	microsoft.asn. and erasure adj codes	US-PGPUB; USPAT	OR	OFF	2012/05/01 14:06
S8	442	(fountain OR erasure OR tornado OR LT OR raptor OR rateless) adj2 cod$3 encrypted key (hash OR fingerprint OR checksum)	US-PGPUB; USPAT; EPO; IBM_TDB	AND	OFF	2012/05/01 14:37
S9	132	(fountain OR erasure OR tornado OR raptor OR rateless) adj (coding or codes) encrypted key (hash OR fingerprint OR checksum)	US-PGPUB; USPAT; EPO; IBM_TDB	AND	OFF	2012/05/01 14:55
S16	994	(fountain OR erasure OR tornado OR LT OR raptor OR rateless) adj2 cod$3 and distribution	US-PGPUB; USPAT; EPO; IBM_TDB	AND	OFF	2012/05/02 14:10
S18	208	(fountain OR erasure OR tornado OR LT OR raptor OR rateless) adj cod$3 and distribution and (@ad<"20041025" or @rlad<"20041025")	US-PGPUB; USPAT; EPO; IBM_TDB	AND	OFF	2012/05/02 14:11

5/4/2012 12:27:05 PM
C:\Users\mchao\Documents\EAST\Workspaces\13371363.wsp

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13371363	ORSINI ET AL.
	Examiner	Art Unit
	MICHAEL CHAO	2492

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

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

CLAIM		DATE								
Final	Original	05/02/2012								
	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	✓								
	26	✓								
	27	✓								

Notice of References Cited	Application/Control No. 13/371,363	Applicant(s)/Patent Under Reexamination ORSINI ET AL.	
	Examiner Michael Chao	Art Unit 2492	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2006/0080454	04-2006	Li, Jin	709/231
*	B	US-7,596,570	09-2009	Emigh et al.	1/1
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Horne et al., Excrow 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.
	V	Hand et al., Spread Spectrum Storage with Mnemosyne, 2003, Retrieved from the Internet <URL: springerlink.com/content/9vdp5b40ep2pjvba/>, pp 1-5 as printed.
	W	Kubiatowicz et al., OceanStore: an architecture for global-scale persistent storage, 2000, Retrieved from the Internet <URL: dl.acm.org/citation.cfm?id=356989.357007>, pp 1-12 as printed.
	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.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/371,363	02/10/2012	Rick L. Orsini	104093-0002-105	7984

1473 7590 05/14/2012

ROPES & GRAY LLP
PATENT DOCKETING 39/361
1211 AVENUE OF THE AMERICAS
NEW YORK, NY 10036-8704

EXAMINER	
CHAO, MICHAEL W	
ART UNIT	**PAPER NUMBER**
2492	

NOTIFICATION DATE	DELIVERY MODE
05/14/2012	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):

USPatentMail@ropesgray.com
USPatentMail2@ropesgray.com

Office Action Summary	Application No.	Applicant(s)	
	13/371,363	ORSINI ET AL.	
	Examiner	Art Unit	
	Michael Chao	2492	

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

Period for Reply

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

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

Status

1)☒ Responsive to communication(s) filed on *08 March 2012*.

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

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

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

Disposition of Claims

5)☒ Claim(s) *1-27* is/are pending in the application.

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

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-27* is/are rejected.

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

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

Application Papers

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

11)☒ The drawing(s) filed on *08 March 2012* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

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

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

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

Priority under 35 U.S.C. § 119

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

a)☐ All b)☐ Some * c)☐ None of:

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

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

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

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

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *2/29/2012*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This action is in response to application 13/371,363 claiming priority to 10/25/2004. Claims 1-27 are pending and directed toward distributed data storage in an encrypted system.

Specification

The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

The present title is “Secure Data Parser Method and System". A parser is a program for analyzing components of data. In contrast the present claims appear directed to a system that securely distributes data for storage.

Claim Rejections - 35 USC § 112

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

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 4, 6, 13, 15, 22, 24 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claims 4, 13, 22 recite: causing a plurality of data units in each of the shares to be rearranged relative to one another after the separating step. No corresponding disclosure or description could be found in the specification.

Claims 6, 15, 24 recite: recite wherein the data indicative of the encryption key comprises data created using a Shamir algorithm. Shamir, as used in the art, is the name of a person. Shamir has authored several algorithms some of which are not directed toward keying. As such there does not appear to be support as to how to use all Shamir algorithms to create data indicative of the encryption key. Applicant's use of one Shamir algorithm (presumably RSA) does not disclose how to use other unrelated algorithms for the same purpose. In other words, Applicant's disclosure of the use of a species of Shamir algorithm does not enable the genus of all Shamir algorithms. See In In re Wright, 999 F.2d 1557, 27 USPQ2d 1510 (Fed. Cir. 1993), In In re Vaeck, 947 F.2d 488, 495, 20 USPQ2d 1438, 1444 (Fed. Cir. 1991). See also MPEP 2164.06(b).

As to the issue of written description for the originally filed claims: "However, as discussed in paragraph I., supra, the issue of a lack of adequate written description may arise even for an original claim when an aspect of the claimed invention has not been described with sufficient particularity such that one skilled in the art would recognize that the applicant had possession of the claimed invention." See MPEP 2163 (II).

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

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

Claims 6, 15, 24 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 6, 15, 24 recite wherein the data indicative of the encryption key comprises data created using a Shamir algorithm. Shamir, as used in the art, is the name of a person. It is unclear which Shamir algorithm is intended, for the purposes of examination the claims have been interpreted to require RSA encryption.

Claim Rejections - 35 USC § 103

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

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

Claims 1-3, 5, 7-12, 14, 16-21, 23, and 25-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Horne et al. (Escrow Services and Incentives in Peer-to-Peer Networks) in view of Li (US 2006/0080454) or in the alternative in view of Hand (Spread Spectrum Storage with Mnemosyne).

With respect to claims 1, 10, 19, Horne teaches: A method for securing a data set, the method steps implemented by a programmed computer system, the method steps comprising:

encrypting the data set based on an encryption key to produce an encrypted data set; ("In the protocol that we describe, S encrypts C with a key K and sends the encryption EK(C)to R." Horne 2.2 ¶ 3)

creating hash information based on a hash operation using the data set; ("In order to take part in the protocol ES requires the correct hash of the encrypted content, H(EK(C)), and the key K that decrypts the content. . . . we assume that S sent the pair K,H(EK(C))———————————— to ES in a preprocessing stage, together with a description of C." Horne 2.2 ¶ 3; see also Horne § 4.2)

generating data splitting information, ("A Straightforward Method Based on Error Correcting Codes" Horne § 4.1) [wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;]

separating the encrypted data set into the plurality of shares based on the data splitting information; ("Distributed file storage: In this model files are not stored at a single server. Instead, a file is divided into many blocks encoded with an error correcting code, and each block is stored at a different location (this is the storage method used by Mojonation.com). The use of error correcting codes ensures that the file can be restored even if part of the peers that store parts of the file are unavailable or corrupt. The directory service might be centralized or distributed. Our ES service can cooperate with this storage system, where the use of error correcting codes we suggest in Section 4 might use (or might not use) the same error correcting code as the storage method." Horne § 5 ¶ 4)

including in the plurality of shares data indicative of (a) the encryption key and (b) the hash information; and ("In order to obtain the key K, R computes the hash of the encrypted content H(EK(C)) and sends it to ES, together with a description of the content C it desires to obtain, and the identity of S. It also sends a payment for the content C, which will only be processed if the content is valid (step 2)." Horne § 2.2 ¶ 7; "After receiving this message R picks a small random set of of the encrypted encoded blocks (where is a parameter to be defined below). It sends to ES this set of encrypted blocks, together with their indexes and the encrypted message that is directed from S to ES." Horne § 4.1 ¶ 3; "In order to verify the encrypted content that it receives from S, R should forward this signature and randomly chosen encrypted blocks to ES." Horne § 4.2 ¶ 8)

causing the plurality of shares to be stored in respective separate storage locations; (Horne § 5 ¶ 4)

wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares. ("The scheme could either use error correction codes, or use more efficient erasure codes. We first examine the use of error correction codes. The codes have the property that given n blocks, such that at least t of them are correct (although the receiver does not know which ones these are), the receiver can reconstruct the original message." Horne § 4.1 ¶ 6).

Although Horne discloses that a distributed storage system may be used (Horne § 5 ¶ 4) it does not disclose how the data is distributed among the stores, as claimed:

wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;

Li discloses a similar system directed toward peer distribution (Li [0003]) using erasure/error coding (Li [0106]). Li further discloses a method for selecting the peers for storing data ("each peer node is assigned k keys in the coded message space of n, with each key being the row index of the generator matrix G. The key assignment may be carried out by the server. Further, if the number of peers caching the media is smaller than n/k, it is possible to assign each peer a unique set of keys. As a result, it can be guaranteed that each peer holds distinctive coded messages. While this strategy provides a number of benefits, it still requires a central coordination node (such as the server)." Li [0109]; alternatively "in another embodiment, the role of the central coordination node is eliminated by allowing each peer to choose k random keys." Li [0110]). Note that, as used in Li, keys are referring to the erasure coding blocks held by a peer and are not cryptographic keys. ("the availability vector will include the media erasure coding keys assigned to serving peer, and the number of erasure blocks held by the serving peer. In addition, if the serving peer uses erasure coding and the media is also embedded coded, the availability vector will include the assigned media erasure coding keys" Li [0065])

A person of ordinary skill in the art at the time of invention would have combined Horne with Li by using the concepts of Li to implement the distribution of erasure coded blocks in Horne (Horne § 5 ¶ 4). It would have been obvious to one of ordinary skill in the art at the time of invention to combine Horne with Li in order to implement necessary

but unspecified functionality of Horne using a solution disclosed in a similar system (Li [0109-10]).

In the alternative, Hand discloses a similar system directed to distributed (Hand § 27.1 ¶ 1) erasure coded fragments for data storage (Hand § 27.1 ¶ 2). Hand additionally discloses a method for distributing the data, as claimed: wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;

("Location: Mnemosyne achieves its security properties by storing encrypted data blocks in pseudo-random (and, to an adversary, unpredictable) locations in a large virtual network store, which is then mapped onto distributed physical storage devices. The locations of the encrypted blocks making up a data set are determined by a sequence of 256-bit values obtained by successively hashing an initial value which depends ultimately on the filename and the user's key K.

Distribution: The sequence of 256-bit location identifiers from the previous step is finally mapped onto physical storage using a peer-to-peer network of storage nodes, each of which holds a fixed-size physical block store." Hand § 27.2 ¶ 6-7).

A person of ordinary skill in the art at the time of invention would have combined Horne with Hand by using the concepts of Hand to implement the distribution of erasure coded blocks in Horne (Horne § 5 ¶ 4). It would have been obvious to one of ordinary skill in the art at the time of invention to combine Horne with Hand in order to implement

necessary but unspecified functionality of Horne using a solution disclosed in a similar system Hand § 27.2 ¶ 6-7).

With respect to claims 2, 11, 20, Horne in view of Li or Hand discloses: wherein the step of separating the encrypted data set comprises using a deterministic technique. (“each peer node is assigned k keys in the coded message space of n, with each key being the row index of the generator matrix G. The key assignment may be carried out by the server. Further, if the number of peers caching the media is smaller than n/k, it is possible to assign each peer a unique set of keys. As a result, it can be guaranteed that each peer holds distinctive coded messages. While this strategy provides a number of benefits, it still requires a central coordination node (such as the server).” Li [0109]) ("The locations of the encrypted blocks making up a data set are determined by a sequence of 256-bit values obtained by successively hashing an initial value which depends ultimately on the filename and the user's key K.” Hand § 27.2 ¶ 6-7).

With respect to claims 3, 12, 21, Horne in view of Li or Hand discloses: wherein the step of separating the encrypted data set comprises using a substantially random technique. (“in another embodiment, the role of the central coordination node is eliminated by allowing each peer to choose k random keys.” Li [0110]) (“Location: Mnemosyne achieves its security properties by storing encrypted data blocks in pseudo-random (and, to an adversary, unpredictable) locations in a large virtual network store, which is then mapped onto distributed physical storage devices.” Hand § 27.2 ¶ 6-7;

thus as disclosed by Hand, the process is 'random' despite being deterministic due to a consistent result given the same inputs)

With respect to claims 5, 14, 23, Horne in view of Li or Hand discloses: wherein the step of separating the encrypted data into the plurality of shares comprises causing the plurality of shares to have a substantially random distribution of the encrypted data set. ("in another embodiment, the role of the central coordination node is eliminated by allowing each peer to choose k random keys." Li [0110]) ("Location: Mnemosyne achieves its security properties by storing encrypted data blocks in pseudo-random (and, to an adversary, unpredictable) locations in a large virtual network store, which is then mapped onto distributed physical storage devices." Hand § 27.2 ¶ 6-7; thus as disclosed by Hand, the process is 'random' despite being deterministic due to a consistent result given the same inputs).

With respect to claims 7, 16, 25, Horne in view of Li or Hand discloses: wherein the step of including data indicative of the encryption key comprises:

Encrypting the encryption key with a second key; and. ("It then sends these blocks to R together with the key K encrypted with the public key of ES." Horne § 4.1 ¶ 2)

Including in the plurality of shares data indicative of the encrypted encryption key.("In order to obtain the key K, R computes the hash of the encrypted content H(EK(C)) and sends it to ES, together with a description of the content C it desires to

obtain, and the identity of S. It also sends a payment for the content C, which will only be processed if the content is valid (step 2)." Horne § 2.2 ¶ 7).

With respect to claims 8, 17, 26, Horne in view of Li or Hand discloses: further comprising the method step of storing the second key outside of the plurality of shares ("It then sends these blocks to R together with the key K encrypted with the public key of ES." Horne § 4.1 ¶ 2; ES is distinct from source S and receiver R), wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares, and the second key. ("The scheme could either use error correction codes, or use more efficient erasure codes. We first examine the use of error correction codes. The codes have the property that given n blocks, such that at least t of them are correct (although the receiver does not know which ones these are), the receiver can reconstruct the original message." Horne § 4.1 ¶ 6).

With respect to claims 9, 18, 27, Horne in view of Li or Hand discloses: wherein the step of storing the shares in respective separate storage locations comprises storing the shares on at least two separate storage devices. ("Distributed file storage: In this model files are not stored at a single server. Instead, a file is divided into many blocks encoded with an error correcting code, and each block is stored at a different location (this is the storage method used by Mojonation.com). The use of error correcting codes ensures that the file can be restored even if part of the peers that store parts of the file are unavailable or corrupt. The directory service might be centralized or distributed. Our

ES service can cooperate with this storage system, where the use of error correcting codes we suggest in Section 4 might use (or might not use) the same error correcting code as the storage method." Horne § 5 ¶ 4)

Claims 4, 13, 22, are rejected under 35 U.S.C. 103(a) as being unpatentable over Horne et al. (Escrow Services and Incentives in Peer-to-Peer Networks) in view of [Li (US 2006/0080454) or in the alternative Hand (Spread Spectrum Storage with Mnemosyne)] in view of Kubiatowicz (OceanStore).

With respect to claims 4, 13, and 22, Horne in view of Li or Hand does not disclose: further comprising causing a plurality of data units in each of the shares to be rearranged relative to one another after the separating step.

Kubiatowicz discloses a similar system based on distributed storage (Kubiatowicz § 2 figure 1) of erasure codes (Kubiatowicz § 4.5). Kubiatowicz further discloses a method of updating the data objects.

("Objects in the OceanStore are modified through updates. Updates contain information about what changes to make to an object and the assumed state of the object under which those changes were developed, much as in the Bayou system [13]. In principle, every update to an OceanStore object creates a new version2. Consistency based on versioning, while more expensive to implement than update-in-place consistency, provides for cleaner recovery in the face of system failures [49]. It also obviates the need for backup and supports "permanent" pointers to information." Kubiatowicz § 2 ¶ 4) ("For the user, we provide a naming syntax which explicitly

incorporates version numbers. Such names can be included in other documents as a form of permanent hyper-link. In addition, interfaces will exist to examine modification history and to set versioning policies [44]. Although in principle every version of every object is archived, clients can choose to produce versions less frequently. Archival copies are also produced when objects are idle for a long time or before objects become inactive. When generating archival fragments, the floating replicas of an object participate together: they each generate a disjoint subset of the fragments and disseminate them into the infrastructure." Kubiatowicz § 4.5 ¶4).

A person of ordinary skill in the art would have modified Horne in view of Li (or Hand) with Kubiatowicz by providing a method for versioning the files to be distributed as disclosed in Kubiatowicz. It would have been obvious to one of ordinary skill in the art at the time of invention to allow versioning of the files so that users could update the files thereby allowing for flexibility of the media storage.

Claims 6, 15, 24, are rejected under 35 U.S.C. 103(a) as being unpatentable over Horne et al. (Escrow Services and Incentives in Peer-to-Peer Networks) in view of [Li (US 2006/0080454) or in the alternative in view of Hand (Spread Spectrum Storage with Mnemosyne)] in view of official notice

With respect to claims 6, 15, and 24 Horne in view of Li or Hand discloses: wherein the data indicative of the encryption key comprises data created using a [Shamir algorithm]. ("The encryption can be done using public key cryptography" Horne § 2.1.2 ¶ 5) ("It then sends these blocks to R together with the key K encrypted with the

public key of ES." Horne § 4.1 ¶ 2). While Horne does disclose the use of a public key encryption, it does not disclose a Shamir Algorithm. Public key encryption commonly refers to the RSA algorithm by Rivest, Shamir and Adleman, Official notice is taken thereof. It would have been obvious to one of ordinary skill in the art to select RSA as the public key encryption method discussed in Horne. It would have been obvious to one of ordinary skill in the art at the time of invention to select RSA as the public key encryption in order to take advantage of a known secure algorithm that conforms to the design requirements of Horne.

Conclusion

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

Emigh et al. (US 7,596,570) discloses an erasure coding system that distributes encrypted segments across multiple storage locations.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Chao whose telephone number is (571)270-5657. The examiner can normally be reached on 8-4 Monday through Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Saleh Najjar can be reached on (571)272-4006. 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.

/M. C./
Examiner, Art Unit 2492

/saleh najjar/

Supervisory Patent Examiner, Art Unit 2492

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13371363	ORSINI ET AL.
	Examiner	Art Unit
	MICHAEL CHAO	2492

SEARCHED			
Class	Subclass	Date	Examiner
726	26	5/4/2012	mc

SEARCH NOTES		
Search Notes	Date	Examiner
Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	5/4/2012	mc
Inventor name search in EAST	5/4/2012	mc
Assignee name search in EAST	5/4/2012	mc
google scholar searched "fountain OR erasure OR tornado OR LT OR raptor OR rateless code encrypted key hash OR fingerprint OR checksum"	5/4/2012	mc

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 14

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2827
Examiner Name	Not Yet Assigned
Attorney Docket Number	104093-0002-105

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
		US-7,577,689	08-18-2009	Masinter et al.	
		US-7,546,427	06-09-2009	Gladwin et al.	
		US-7,203,871	04-10-2007	Turner et al.	
		US-7,187,771	03-06-2007	Dickinson et al.	
		US-7,003,531	02-21-2006	Holenstein et al.	
		US-6,852,988	02-08-2005	Li	
		US-6,687,375	02-03-2004	Matyas, Jr. et al.	
		US-6,453,416	09-17-2002	Epstein	
		US-6,446,204	09-03-2002	Pang et al.	
		US-6,411,716	06-25-2002	Brickell	
		US-6,385,318	05-07-2002	Oishi	
		US-6,307,940	10-23-2001	Yamamoto et al.	
		US-6,292,782	09-18-2001	Weideman	
		US-6,292,568	09-18-2001	Akins, III et al.	
		US-6,289,455	09-11-2001	Kocher et al.	
		US-6,266,413	07-24-2001	Shefi	
		US-6,260,125	07-10-2001	McDowell	
		US-6,256,737	07-03-2001	Bianco et al.	
		US-6,061,790	05-09-2000	Bodnar	

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]
	**	AU-2004248616	06-04-2009	Security First Corporation		
	**	EP-0485090-A2	05-13-1992	Visa Int Service Ass		
	**	EP-0821504	01-28-1998	Nippon Telegraph and Telephone Corporation		
	**	EP-0862301	09-02-1998	Fujitsu Limited		
	**	EP-1011222	06-21-2000	Fujitsu Limited		
	**	EP-1239384-A2	09-11-2002	Pkware Inc		

Examiner Signature	/Michael Chao/	Date Considered	05/02/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. ** CITE NO.: Those document(s) which are marked with an double asterisk (**) next to the Cite No. are not supplied because they were previously cited by or submitted to the Office in a prior application relied upon in this application for an earlier filing date under 35 U.S.C. 120. [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.

29678293_1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.C

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 14

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2827
Examiner Name	Not Yet Assigned
Attorney Docket Number	104093-0002-105

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
		US-5,995,630	11-30-1999	Borza	
		US-5,987,232	11-16-1999	Tabuki	
		US-5,917,913	06-29-1999	Wang	
		US-5,915,019	06-22-1999	Ginter et al.	
		US-5,163,096	11-10-1992	Clark et al.	
		US-5,150,407	09-22-1992	Chan	
		US-2011/0246817	10-06-2011	Orsini et al.	
		US-2011/0246766	10-06-2011	Orsini et al.	
		US-2011/0179287	07-21-2011	Orsini et al.	
		US-2011/0179271	07-21-2011	Orsini et al.	
		US-2010/0299313	11-25-2010	ORSINI et al.	
		US-20090254572	10-08-2009	Redlich et al.	
		US-20080147821	06-19-2008	Dietrich et al.	
		US-2008/281879	11-13-2008	KAWAMURA	
		US-2008/0183975	07-31-2008	Foster et al.	
		US-2004/0267832	12-30-2004	Wong et al.	
		US-4,453,074	06-05-1984	Weinstein	
		US-4,924,513	05-08-1990	Herbison et al.	
		US-4,932,057	06-05-1990	Kolbert	

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]
	**	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.		
	**	GB-2237670-A	05-08-1991	De La Rue Syst et al.		
	**	JP-04297157-A	10-21-1992	Mitsubishi Electric Corp		

Examiner Signature	/Michael Chao/	Date Considered	05/02/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. ** CITE NO.: Those document(s) which are marked with an double asterisk (**) next to the Cite No. are not supplied because they were previously cited by or submitted to the Office in a prior application relied upon in this application for an earlier filing date under 35 U.S.C. 120. [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.

29678293_1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.C

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 3 of 14

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2827
Examiner Name	Not Yet Assigned
Attorney Docket Number	104093-0002-105

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
		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-5,268,963	12-07-1993	Monroe et al.	
		US-5,375,244	12-20-1994	McNair	
		US-5,386,104	01-31-1995	Sime	
		US-5,485,474	01-16-1996	Rabin	
		US-5,524,073	06-04-1996	Stambler	
		US-5,615,269	03-25-1997	Micali	
		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-5,682,425	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-5,768,382	06-16-1998	Schneier et al.	
		US-5,768,519	06-16-1998	Swift et al.	

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]
	**	RU-2124814	01-10-1999	A.A. Moldovjan		
	**	WO-00/36786-A1	06-22-2000	Philips Electronics Na		
	**	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		

Examiner Signature	/Michael Chao/	Date Considered	05/02/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. ** CITE NO.: Those document(s) which are marked with an double asterisk (**) next to the Cite No. are not supplied because they were previously cited by or submitted to the Office in a prior application relied upon in this application for an earlier filing date under 35 U.S.C. 120. [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.

29678293_1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.C

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 4 of 14

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2827
Examiner Name	Not Yet Assigned
Attorney Docket Number	104093-0002-105

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
		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-5,940,507	08-1999	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-5,991,414	11-23-1999	Garay et al.	
		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-6,073,237	06-06-2000	Ellison	
		US-6,092,201	07-18-2000	Turnbull et al.	
		US-6,094,485	07-25-2000	Weinstein et al.	
		US-6,192,472	02-20-2001	Garay et al.	

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]
	**	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-02/21283-A1	03-14-2002	Sanctuary Systems Pty Ltd.		
	**	WO-02/21761-A2	03-14-2002	Widevine Technologies Inc		
	**	WO-02/21761-A2	03-14-2002	Widevine Technologies Inc		

Examiner Signature	/Michael Chao/	Date Considered	05/02/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. ** CITE NO.: Those document(s) which are marked with an double asterisk (**) next to the Cite No. are not supplied because they were previously cited by or submitted to the Office in a prior application relied upon in this application for an earlier filing date under 35 U.S.C. 120. [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.

29678293_1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.C

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 5 of 14

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2827
Examiner Name	Not Yet Assigned
Attorney Docket Number	104093-0002-105

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
		US-6,134,550	10-17-2000	Van Oorschot 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-6,289,509	09-11-2001	Kryloff	
		US-6,301,659	10-09-2001	Micali	
		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-6,356,941	03-12-2002	Cohen	
		US-6,363,425	03-26-2002	Hook et al.	
		US-6,386,451	05-14-2002	Sehr	
		US-6,424,718	07-23-2002	Holloway	
		US-6,438,690	08-20-2002	Patel et al.	
		US-6,449,730	09-10-2002	Mann et al.	
		US-6,483,921	11-19-2002	Harkins	
		US-6,553,493	04-22-2003	Okumura et al.	

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]
	**	WO-04/111791-A2	12-23-2004	Security First Corp.		
	**	WO-06/047694-A1	05-04-2006	Orsini Rick L et al.		
	**	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	Surfcontrol On Demand Ltd.		

Examiner Signature	/Michael Chao/	Date Considered	05/02/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. ** CITE NO.: Those document(s) which are marked with an double asterisk (**) next to the Cite No. are not supplied because they were previously cited by or submitted to the Office in a prior application relied upon in this application for an earlier filing date under 35 U.S.C. 120. [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.

29678293_1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.C

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 6 of 14

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2827
Examiner Name	Not Yet Assigned
Attorney Docket Number	104093-0002-105

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
		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-6,789,198	09-07-2004	Chan	
		US-6,856,383	02-15-2005	Vachris et al.	
		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-7,050,580	05-23-2006	Ferre Herrero	
		US-7,050,583	05-23-2006	Montgomery	
		US-7,069,451	06-27-2006	Ginter et al.	
		US-7,096,494	08-22-2006	Chen	
		US-7,117,365	10-03-2006	Rump et al.	
		US-7,133,845	11-07-2006	Ginter et al.	
		US-7,218,736	05-15-2007	Nishimura et al.	
		US-7,225,158	05-29-2007	Toshikage et al.	
		US-7,337,320	02-26-2008	Tada et al.	

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]
	**	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-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.		

Examiner Signature	/Michael Chao/	Date Considered	05/02/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. ** CITE NO.: Those document(s) which are marked with an double asterisk (**) next to the Cite No. are not supplied because they were previously cited by or submitted to the Office in a prior application relied upon in this application for an earlier filing date under 35 U.S.C. 120. [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.

29678293_1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.C

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 7 of 14

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2827
Examiner Name	Not Yet Assigned
Attorney Docket Number	104093-0002-105

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
		US-7,349,539	03-25-2008	Wee et al.	
		US-7,391,865	06-24-2008	Orsini et al.	
		US-7,627,125	12-01-2009	Lumsden et al.	
		US-7,649,992	01-19-2010	Raju et al.	
		US-7,869,597	01-11-2011	Nakai et al.	
		US-2001/0001876	05-24-2001	Morgan et al.	
		US-2001/0051902	12-13-2001	Messner	
		US-20020010679	01-24-2002	Felsher	
		US-2002/0032663	03-14-2002	Messner	
		US-2002/0046359	04-18-2002	Boden	
		US-2002/0071566	06-13-2002	Kurn	
		US-2002/0091640	07-11-2002	Gupta	
		US-2002/0129235	09-12-2002	Okamoto et al.	
		US-2002/0162047	10-31-2002	Peters et al.	
		US-2002/0172358	11-21-2002	Hurich	
		US-2003/0051054	03-13-2003	Redlich et al.	
		US-2003/0058274	03-27-2003	Hill et al.	
		US-2003/0070077	04-10-2003	Redlich et al.	
		US-2003/0167408	09-04-2003	Fitzpatrick et al.	

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]
	**	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		

Examiner Signature	/Michael Chao/	Date Considered	05/02/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. ** CITE NO.: Those document(s) which are marked with an double asterisk (**) next to the Cite No. are not supplied because they were previously cited by or submitted to the Office in a prior application relied upon in this application for an earlier filing date under 35 U.S.C. 120. [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.

29678293_1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.C

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 8 of 14

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2827
Examiner Name	Not Yet Assigned
Attorney Docket Number	104093-0002-105

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
		US-2003/0051159	03-13-2003	McCown et al.	
		US-7,391,865	06-24-2008	Orsini et al.	
		US-20040111608	06-10-2004	Oom Temudo de Castro et al.	
		US-2004/0122863	06-24-2004	Sidman	
		US-2006/0177061	08-10-2006	Orsini et al.	
		US-2006/0184764	08-17-2006	Osaki	
		US-2006/0282681	12-14-2006	Scheidt et al.	
		US-2006/0294378	12-28-2006	Lumsden et al.	
		US-20070192586	08-16-2007	McNeely	
		US-8,009,830	08-30-2011	Orsini et al.	
		US-2008/0137857	06-12-2008	Bellare et al.	
		US-2008/0170693	07-17-2008	Spies et al.	
		US-2008/0183992	07-31-2008	Martin et al.	
		US-20080199003	08-21-2008	Hennessey et al.	
		US-20080244277	10-02-2008	Orsini et al.	
		US-20090077379	03-19-2009	Geyzel et al.	
		US-2009/0097661	04-16-2009	Orsini et al.	
		US-2009/0177894	07-09-2009	Orsini et al.	
		US-2009/0254750	10-08-2009	Bono et al.	

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]

Examiner Signature	/Michael Chao/	Date Considered	05/02/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. ** CITE NO.: Those document(s) which are marked with an double asterisk (**) next to the Cite No. are not supplied because they were previously cited by or submitted to the Office in a prior application relied upon in this application for an earlier filing date under 35 U.S.C. 120. [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.

29678293_1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.C

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 9 of 14

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2827
Examiner Name	Not Yet Assigned
Attorney Docket Number	104093-0002-105

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
		US-2010/0150341	06-17-2010	Dodgson et al.	
		US-2010/0153670	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-2011/0202763	08-18-2011	Martin et al.	
		US-2011/0202755	08-18-2011	ORSINI et al.	

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]

Examiner Signature	/Michael Chac/	Date Considered	05/02/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. ** CITE NO.: Those document(s) which are marked with an double asterisk (**) next to the Cite No. are not supplied because they were previously cited by or submitted to the Office in a prior application relied upon in this application for an earlier filing date under 35 U.S.C. 120. [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.

29678293_1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.C

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 10 of 14

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2827
Examiner Name	Not Yet Assigned
Attorney Docket Number	104093-0002-105

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	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[2]
	**	"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.	
	**	"Lancope Announces Stealthwatch 3.0 for Enhanced Enterprise-Wide Security and Improved Manageability", Business Wire (Newswire Association, Inc.), 14 April 2003.	
	**	"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.	
	**	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.	
	**	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.	

Examiner Signature	/Michael Chao/	Date Considered	05/02/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ** CITE NO.: Those document(s) which are marked with an double asterisk (**) next to the Cite No. are not supplied because they were previously cited by or submitted to the Office in a prior application relied upon in this application for an earlier filing date under 35 U.S.C. 120.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

29678293_1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.C

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 11 of 14

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2827
Examiner Name	Not Yet Assigned
Attorney Docket Number	104093-0002-105

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	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[2]
	**	Damgard et. al., "Non-interactive and Reusable Non-malleable Commitment Schemes," ACM STOC '03; pgs. 427-428; June 9-11, 2003.	
	**	Decleene et al., "Secure group communications for wireless networks," MILCOM 2001 Proceedings, Communications for Network-Centric Operations: Creating the Information Force; IEEE, US, vol. 1, 28 October 2001, pages 113-117	
	**	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	
	**	Gibson, "Opinion", eWeek - Enterprise News & Reviews, 14 April 2003.	
	**	Grant et. al., "Secret Sharing and Splitting", (White Paper) Notre Dame, Indiana, 16 December 2002.	

Examiner Signature	/Michael Chao/	Date Considered	05/02/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ** CITE NO.: Those document(s) which are marked with an double asterisk (**) next to the Cite No. are not supplied because they were previously cited by or submitted to the Office in a prior application relied upon in this application for an earlier filing date under 35 U.S.C. 120.

[1]Applicant's unique citation designation number (optional). [2]Applicant is to place a check mark here if English language Translation is attached.

29678293_1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.C

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 12 of 14

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2827
Examiner Name	Not Yet Assigned
Attorney Docket Number	104093-0002-105

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	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[2]
	**	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.	
	**	International Search Report - International Application No. PCT/US/06/45066, dated July 17, 2008	
	**	International Search Report and Written Opinion dated December 14, 2010 in International Application No. PCT/US2010/035377	
	**	International Search Report and Written Opinion dated September 8, 2009 in International Application No. PCT/US2009/001158	
	**	International Search Report dated December 16, 2008, International Application No. PCT/US07/023626	
	**	International Search Report dated March 10, 2009, International Application No. PCT/US09/000083	
	**	International Search Report dated November 21, 2008, International Application No. PCT/US08/010677	
	**	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]	

Examiner Signature	/Michael Chao/	Date Considered	05/02/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ** CITE NO.: Those document(s) which are marked with an double asterisk (**) next to the Cite No. are not supplied because they were previously cited by or submitted to the Office in a prior application relied upon in this application for an earlier filing date under 35 U.S.C. 120.

[1]Applicant's unique citation designation number (optional). [2]Applicant is to place a check mark here if English language Translation is attached.

29678293_1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.C

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 13 of 14

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2827
Examiner Name	Not Yet Assigned
Attorney Docket Number	104093-0002-105

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	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[2]
	**	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" 1997, 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	
	**	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	
	**	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	
	**	Savage, "RSA Unveils Nightingale Technology", CRN.com, 14 April 2003.	

Examiner Signature	/Michael Chao/	Date Considered	05/02/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ** CITE NO.: Those document(s) which are marked with an double asterisk (**) next to the Cite No. are not supplied because they were previously cited by or submitted to the Office in a prior application relied upon in this application for an earlier filing date under 35 U.S.C. 120.

[1]Applicant's unique citation designation number (optional). [2]Applicant is to place a check mark here if English language Translation is attached.

29678293_1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.C

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 14 of 14

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2827
Examiner Name	Not Yet Assigned
Attorney Docket Number	104093-0002-105

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	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[2]
	**	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.	
	**	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.	

Examiner Signature	/Michael Chao/	Date Considered	05/02/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ** CITE NO.: Those document(s) which are marked with an double asterisk (**) next to the Cite No. are not supplied because they were previously cited by or submitted to the Office in a prior application relied upon in this application for an earlier filing date under 35 U.S.C. 120.

[1]Applicant's unique citation designation number (optional). [2]Applicant is to place a check mark here if English language Translation is attached.

29678293_1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.C

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/371,363	02/10/2012	Rick L. Orsini	104093-0002-105

CONFIRMATION NO. 7984

1473
ROPES & GRAY LLP
PATENT DOCKETING 39/361
1211 AVENUE OF THE AMERICAS
NEW YORK, NY 10036-8704

PUBLICATION NOTICE



Title:SECURE DATA PARSER METHOD AND SYSTEM

Publication No.US-2012-0166815-A1
Publication Date:06/28/2012

NOTICE OF PUBLICATION OF APPLICATION

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

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

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 May 2010 (20.05.2010)

PCT

(10) International Publication Number
WO 2010/057181 A2

(51) International Patent Classification:
G06F 12/14 (2006.01) *G06F 12/08* (2006.01)
H04L 9/08 (2006.01)

(21) International Application Number:
PCT/US2009/064786

(22) International Filing Date:
17 November 2009 (17.11.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

12/272,012	17 November 2008 (17.11.2008)	US
12/336,562	17 December 2008 (17.12.2008)	US
12/336,564	17 December 2008 (17.12.2008)	US
12/336,559	17 December 2008 (17.12.2008)	US
12/336,568	17 December 2008 (17.12.2008)	US
12/336,558	17 December 2008 (17.12.2008)	US
12/342,464	23 December 2008 (23.12.2008)	US
12/342,500	23 December 2008 (23.12.2008)	US
12/342,575	23 December 2008 (23.12.2008)	US
12/342,523	23 December 2008 (23.12.2008)	US
12/342,414	23 December 2008 (23.12.2008)	US
12/342,438	23 December 2008 (23.12.2008)	US
12/342,610	23 December 2008 (23.12.2008)	US
12/342,636	23 December 2008 (23.12.2008)	US
12/342,547	23 December 2008 (23.12.2008)	US
12/342,379	23 December 2008 (23.12.2008)	US
12/346,561	30 December 2008 (30.12.2008)	US
12/346,578	30 December 2008 (30.12.2008)	US

(71) Applicant *(for all designated States except US)*: **UNISYS CORPORATION** [US/US]; Unisys Way, MS/S1-108, Blue Bell, PA 19424-0001 (US).

(72) Inventors: **SUMMERS, Scott**; 14 Sugarpine Lane, Collegeville, PA 19426 (US). **FRENCH, Albert**; 355 Grubb Road, Schwenksville, PA 19473 (US).

(74) Agent: **GREGSON, Richard, J.**; Unisys Corporation, Unisys Way, MS/S1-108, Blue Bell, PA 19424-0001 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

WO 2010/057181 A2

(54) Title: SIMULTANEOUS STATE-BASED CRYPTOGRAPHIC SPLITTING IN A SECURE STORAGE APPLIANCE

(57) Abstract: Methods and systems for managing data blocks and I/O requests are provided. One method is a method of managing data blocks in a secure storage appliance. The method includes receiving a block of data associated with a volume, the volume associated with a plurality of shares stored on a plurality of physical storage devices, and storing the block of data in a buffer. The method also includes associating the block of data with a state from among a plurality of states, each of the states corresponding to a status of the block of data. The method further includes processing the block of data by performing at least one cryptographic operation on the block of data, and upon completion of processing the block of data, updating the state of the block of data.

SIMULTANEOUS STATE-BASED CRYPTOGRAPHIC SPLITTING IN A SECURE STORAGE APPLIANCE

Technical Field

The present disclosure relates to data storage systems, and security for such systems. In particular, the present disclosure relates to simultaneous state-based cryptographic splitting in a secure storage appliance.

Background

Modern organizations generate and store large quantities of data. In many instances, organizations store much of their important data at a centralized data storage system. It is frequently important that such organizations be able to quickly access the data stored at the data storage system. In addition, it is frequently important that data stored at the data storage system be recoverable if the data is written to the data storage system incorrectly or if portions of the data stored at the repository is corrupted. Furthermore, it is important that data be able to be backed up to provide security in the event of device failure or other catastrophic event.

The large scale data centers managed by such organizations typically require mass data storage structures and storage area networks that are capable of providing both long-term mass data storage and access capabilities for application servers using that data. Some data security measures are usually implemented in such large data storage networks, and are intended to ensure proper data privacy and prevent data corruption. Typically, data security is accomplished via encryption of data and/or access control to a network within which the data is stored. Data can be

stored in one or more locations, e.g. using a redundant array of inexpensive disks (RAID) or other techniques.

One example of an existing mass data storage system 10 is illustrated in Figure 1. As shown, an application server 12 (e.g. a database or file system provider) connects to a number of storage devices 14_1-14_N providing mass storage of data to be maintained accessible to the application server via direct connection 15, an IP-based network 16, and a Storage Area Network 18. Each of the storage devices 14 can host disks 20 of various types and configurations useable to store this data.

The physical disks 20 are made visible/accessible to the application server 12 by mapping those disks to addressable ports using, for example, logical unit numbering (LUN), internet SCSI (iSCSI), or common internet file system (CIFS) connection schemes. In the configuration shown, five disks are made available to the application server 12, bearing assigned letters I-M. Each of the assigned drive letters corresponds to a different physical disk 20 (or at least a different portion of a physical disk) connected to a storage device 14, and has a dedicated addressable port through which that disk 20 is accessible for storage and retrieval of data. Therefore, the application server 12 directly addresses data stored on the physical disks 20.

A second typical data storage arrangement 30 is shown in Figure 2. The arrangement 30 illustrates a typical data backup configuration useable to tape-backup files stored in a data network. The network 30 includes an application server 32, which makes a snapshot of data 34 to send to a backup server 36. The backup server 36 stores the snapshot, and operates a tape management system 38 to record that snapshot to a magnetic tape 40 or other long-term storage device.

These data storage arrangements have a number of disadvantages. For example, in the network 10, a number of data access vulnerabilities exist. An unauthorized user can steal a physical disk 20, and thereby obtain access to sensitive files stored on that disk. Or, the unauthorized user can exploit network vulnerabilities to observe data stored on disks 20 by monitoring the data passing in any of the networks 15, 16, 18 between an authorized application server 12 or other authorized user and the physical disk 20. The network 10 also has inherent data loss risks. In the network 30, physical data storage can be time consuming, and physical backup tapes can be subject to failure, damage, or theft.

To overcome some of these disadvantages, systems have been introduced which duplicate and/or separate files and directories for storage across one or more physical disks. The files and directories are typically stored or backed up as a monolith, meaning that the files are logically grouped with other like data before being secured. Although this provides a convenient arrangement for retrieval, in that a common security construct (e.g. an encryption key or password) is related to all of the data, it also provides additional risk exposure if the data is compromised.

For these and other reasons, improvements are desirable.

Summary

In accordance with the following disclosure, the above and other problems are solved by the following:

In a first aspect, a method of managing data blocks in a secure storage appliance is disclosed. The method includes receiving a block of data associated with a volume, the volume associated with a plurality of shares stored on

a plurality of physical storage devices, and storing the block of data in a buffer. The method also includes associating the block of data with a state from among a plurality of states, each of the states corresponding to a status of the block of data. The method further includes processing the block of data by performing at least one cryptographic operation on the block of data, and upon completion of processing the block of data, updating the state of the block of data.

In a second aspect, a method of managing I/O requests in a secure storage appliance is disclosed. The method includes receiving an I/O request at the secure storage appliance, the I/O request associated with a volume, the volume associated with a plurality of shares stored on a plurality of physical storage devices. The method further includes determining whether a block of data referenced by the I/O request is present in a buffer. The method also includes transferring the block of data to a buffer and associating the block of data with a transfer state, determining whether the block of data in the buffer is updated, and processing the block of data.

In a third aspect, a secure storage appliance is disclosed. The secure storage appliance includes a plurality of buffers, each buffer capable of holding a block of data having a state from among a plurality of states. The secure storage appliance also includes a programmable circuit capable of accessing the plurality of buffers. The programmable circuit is configured to execute program instructions to receive an I/O request, the I/O request associated with a volume, the volume associated with a plurality of shares stored on a plurality of physical storage devices communicatively connected to the secure storage appliance. The programmable circuit is further configured to execute program instructions to determine whether a block of data referenced by the I/O request is present in a buffer, transfer the block

of data to a buffer among the plurality of buffers, determine whether the block of data in the buffer is updated, and process the block of data.

In a fourth aspect, a secure storage appliance is disclosed. The secure storage appliance includes a plurality of buffers, each buffer capable of holding a block of data having a state selected from among a plurality of states. The secure storage appliance further includes a programmable circuit capable of accessing the plurality of buffers. The programmable circuit is configured to execute program instructions to receive a block of data associated with a volume, the volume associated with a plurality of shares stored on a plurality of physical storage devices. The programmable circuit is also configured to execute program instructions to store the block of data in a buffer from among the plurality of buffers and associate the buffer with a state corresponding to a status of the block of data. The programmable circuit is further configured to execute program instructions to process the block of data by performing at least one cryptographic operation on the block of data and update the state of the buffer upon completion of processing the block of data.

Brief Description of the Drawings

Figure 1 illustrates an example prior art network providing data storage;

Figure 2 illustrates an example prior art network providing data backup capabilities;

Figure 3 illustrates a data storage system according to a possible embodiment of the present disclosure;

Figure 4 illustrates a data storage system according to a further possible embodiment of the present disclosure;

Figure 5 illustrates a portion of a data storage system including a secure storage appliance, according to a possible embodiment of the present disclosure;

Figure 6 illustrates a block diagram of logical components of a secure storage appliance, according to a possible embodiment of the present disclosure.

Figure 7 illustrates a portion of a data storage system including a secure storage appliance, according to a further possible embodiment of the present disclosure;

Figure 8 illustrates dataflow of a write operation according to a possible embodiment of the present disclosure;

Figure 9 illustrates dataflow of a read operation according to a possible embodiment of the present disclosure;

Figure 10 illustrates a further possible embodiment of a data storage network including redundant secure storage appliances, according to a possible embodiment of the present disclosure;

Figure 11 illustrates incorporation of secure storage appliances in a portion of a data storage network, according to a possible embodiment of the present disclosure;

Figure 12 illustrates an arrangement of a data storage network according to a possible embodiment of the present disclosure;

Figure 13 illustrates a physical block structure of data to be written onto a physical storage device, according to aspects of the present disclosure;

Figure 14 shows a flowchart of systems and methods for providing access to secure storage in a storage area network according to a possible embodiment of the present disclosure;

Figure 15 shows a flowchart of systems and methods for reading block-level secured data according to a possible embodiment of the present disclosure;

Figure 16 shows a flowchart of systems and methods for writing block-level secured data according to a possible embodiment of the present disclosure;

Figure 17 shows a possible arrangement for providing secure storage data backup, according to a possible embodiment of the present disclosure;

Figure 18 shows a possible arrangement for providing secure storage for a thin client computing network, according to a possible embodiment of the present disclosure;

Figure 19 shows a state diagram for simultaneous state-based cryptographic splitting in a secure storage appliance, according to aspects of the present disclosure;

Figure 20 shows a flowchart of methods and systems for simultaneous state-based cryptographic splitting in a secure storage appliance, according to aspects of the present disclosure;

Figure 21 shows a flowchart of methods and systems for reconstituting data in a secure storage appliance, according to a possible aspect of the present disclosure;

Figure 22 shows a flowchart of methods and systems for cryptographically splitting data in a secure storage appliance, according to a possible aspect of the present disclosure;

Figure 23 shows a flowchart of methods and systems for managing data blocks in a secure storage appliance, according to a possible embodiment of the present disclosure; and

Figure 24 shows a flowchart of methods and systems for managing I/O requests in a secure storage appliance, according to a possible embodiment of the present disclosure.

Detailed Description

Various embodiments of the present invention will be described in detail with reference to the drawings, wherein like reference numerals represent like parts and assemblies throughout the several views. Reference to various embodiments does not limit the scope of the invention, which is limited only by the scope of the claims attached hereto. Additionally, any examples set forth in this specification are not intended to be limiting and merely set forth some of the many possible embodiments for the claimed invention.

The logical operations of the various embodiments of the disclosure described herein are implemented as: (1) a sequence of computer implemented steps, operations, or procedures running on a programmable circuit within a computer, and/or (2) a sequence of computer implemented steps, operations, or procedures running on a programmable circuit within a directory system, database, or compiler.

In general the present disclosure relates to a block-level data storage security system. By block-level, it is intended that the data storage and security performed according to the present disclosure is not performed based on the size or arrangement of logical files (e.g. on a per-file or per-directory level), but rather that the data security is based on individual read and write operations related to physical

blocks of data. In various embodiments of the present disclosure, the data managed by the read and write operations are split or grouped on a bitwise or other physical storage level. These physical storage portions of files can be stored in a number of separated components and encrypted. The split, encrypted data improves data security for the data "at rest" on the physical disks, regardless of the access vulnerabilities of physical disks storing the data. This is at least in part because the data cannot be recognizably reconstituted without having appropriate access and decryption rights to multiple, distributed disks. The access rights limitations provided by such a system also makes deletion of data simple, in that deletion of access rights (e.g. encryption keys) provides for effective deletion of all data related to those rights.

The various embodiments of the present disclosure are applicable across a number of possible networks and network configurations; in certain embodiments, the block-level data storage security system can be implemented within a storage area network (SAN) or Network-Attached Storage (NAS) system. Other possible networks in which such systems can be implemented exist as well.

In certain aspects of the present disclosure, simultaneous state-based processing of cryptographic splitting and reconstituting operations are provided in a secure storage appliance. This state-based, pipelined processing allows the secure storage appliance to perform sub-tasks as resources of the secure storage appliance become available for use. The secure storage appliance can therefore improve throughput of processed data and I/O requests related to that data, based on these operations.

Referring now to Figure 3, a block diagram illustrating an example data storage system 100 is shown, according to the principles of the present

disclosure. In the example of Figure 3, system 100 includes a set of client devices 105A through 105N (collectively, "client devices 105"). Client devices 105 can be a wide variety of different types of devices. For example, client devices 105 can be personal computers, laptop computers, network telephones, mobile telephones, television set top boxes, network televisions, video gaming consoles, web kiosks, devices integrated into vehicles, mainframe computers, personal media players, intermediate network devices, network appliances, and other types of computing devices. Client devices 105 may or may not be used directly by human users.

Client devices 105 are connected to a network 110. Network 110 facilitates communication among electronic devices connected to network 110. Network 110 can be a wide variety of electronic communication networks. For example, network 110 can be a local-area network, a wide-area network (e.g., the Internet), an extranet, or another type of communication network. Network 110 can include a variety of connections, including wired and wireless connections. A variety of communications protocols can be used on network 110 including Ethernet, WiFi, WiMax, Transfer Control Protocol, and many other communications protocols.

In addition, system 100 includes an application server 115. Application server 115 is connected to the network 110, which is able to facilitate communication between the client devices 105 and the application server 115. The application server 115 provides a service to the client devices 105 via network 110. For example, the application server 115 can provide a web application to the client devices 105. In another example, the application server 115 can provide a network-attached storage server to the client devices 105. In another example, the application

server 115 can provide a database access service to the client devices 105. Other possibilities exist as well.

The application server 115 can be implemented in several ways. For example, the application server 115 can be implemented as a standalone server device, as a server blade, as an intermediate network device, as a mainframe computing device, as a network appliance, or as another type of computing device. Furthermore, it should be appreciated that the application server 115 can include a plurality of separate computing devices that operate like one computing device. For instance, the application server 115 can include an array of server blades, a network data center, or another set of separate computing devices that operate as if one computing device. In certain instances, the application server can be a virtualized application server associated with a particular group of users, as described in greater detail below in Figure 18.

The application server 115 is communicatively connected to a secure storage appliance 120 that is integrated in a storage area network (SAN) 125. Further, the secure storage appliance 120 is communicatively connected to a plurality of storage devices 130A through 130N (collectively, "storage devices 130"). Similar to the secure storage appliance 120, the storage devices 130 can be integrated with the SAN 125.

The secure storage appliance 120 can be implemented in several ways. For example, the secure storage appliance 120 can be implemented as a standalone server device, as a server blade, as an intermediate network device, as a mainframe computing device, as a network appliance, or as another type of computing device. Furthermore, it should be appreciated that, like the application server 115, the secure storage appliance 120 can include a plurality of separate

computing devices that operate like one computing device. In certain embodiments, SAN 125 may include a plurality of secure storage appliances. Each of secure storage appliances 214 is communicatively connected to a plurality of the storage devices 130. In addition, it should be appreciated that the secure storage appliance 120 can be implemented on the same physical computing device as the application server 115.

The application server 115 can be communicatively connected to the secure storage appliance 120 in a variety of ways. For example, the application server 115 can be communicatively connected to the secure storage appliance 120 such that the application server 115 explicitly sends I/O commands to secure storage appliance 120. In another example, the application server 115 can be communicatively connected to secure storage appliance 120 such that the secure storage appliance 120 transparently intercepts I/O commands sent by the application server 115. On a physical level, the application server 115 and the secure storage appliance 120 can be connected via most physical interfaces that support a SCSI command set. Examples of such interfaces include Fibre Channel and iSCSI interfaces.

The storage devices 130 can be implemented in a variety of different ways as well. For example, one or more of the storage devices 130 can be implemented as disk arrays, tape drives, JBODs ("just a bunch of disks"), or other types of electronic data storage devices.

In various embodiments, the SAN 125 is implemented in a variety of ways. For example, the SAN 125 can be a local-area network, a wide-area network (e.g., the Internet), an extranet, or another type of electronic communication network. The SAN 125 can include a variety of connections, including wired and

wireless connections. A variety of communications protocols can be used on the SAN 125 including Ethernet, WiFi, WiMax, Transfer Control Protocol, and many other communications protocols. In certain embodiments, the SAN 125 is a high-bandwidth data network provided using, at least in part, an optical communication network employing Fibre Channel connections and Fibre Channel Protocol (FCP) data communications protocol between ports of data storage computing systems.

The SAN 125 additionally includes an administrator device 135. The administrator device 135 is communicatively connected to the secure storage appliance 120 and optionally to the storage devices 130. The administrator device 135 facilitates administrative management of the secure storage appliance 120 and to storage devices. For example, the administrator device 135 can provide an application that can transfer configuration information to the secure storage appliance 120 and the storage devices 130. In another example, the administrator device 135 can provide a directory service used to store information about the SAN 125 resources and also centralize the SAN 125.

In various embodiments, the administrator device 135 can be implemented in several ways. For example, the administrator device 135 can be implemented as a standalone computing device such as a PC or a laptop, or as another type of computing device. Furthermore, it should be appreciated that, like the secure storage appliance 120, the administrator device 135 can include a plurality of separate computing devices that operate as one computing device.

Now referring to Figure 4, a data storage system 200 is shown according to a possible embodiment of the present disclosure. The data storage system 200 provides additional security by way of introduction of a secure storage

appliance and related infrastructure/functionality into the data storage system 200, as described in the generalized example of Figure 3.

In the embodiment shown, the data storage system 200 includes an application server 202, upon which a number of files and databases are stored. The application server 202 is generally one or more computing devices capable of connecting to a communication network and providing data and/or application services to one or more users (e.g. in a client-server, thin client, or local account model). The application server 202 is connected to a plurality of storage systems 204. In the embodiment shown, storage systems 204_{1-5} are shown, and are illustrated as a variety of types of systems including direct local storage, as well as hosted remote storage. Each of storage systems 204 manages storage on one or more physical storage devices 206. The physical storage devices 206 generally correspond to hard disks or other long-term data storage devices. In the specific embodiment shown, the JBOD storage system 204_1 connects to physical storage devices 206_1, the NAS storage system 204_2 connects to physical storage device 206_2, the JBOD storage system 204_3 connects to physical storage devices 206_{3-7}, the storage system 204_4 connects to physical storage devices 206_{8-12}, and the JBOD storage system 204_5 connects to physical storage device 206_{13}. Other arrangements are possible as well, and are in general a matter of design choice.

In the embodiment shown, a plurality of different networks and communicative connections reside between the application server 202 and the storage systems 204. For example, the application server 202 is directly connected to JBOD storage system 204_1 via a plurality of physical storage devices 208 (JBOD connection), e.g. for local storage. The application server 202 is also communicatively connected to storage systems 204_{2-3} via network 210, which uses

any of a number of IP-based protocols such as Ethernet, WiFi, WiMax, Transfer Control Protocol, or any other of a number of communications protocols. The application server 202 also connects to storage systems 204_{4-5} via a storage area network (SAN) 212, which can be any of a number of types of SAN networks described in conjunction with SAN 125, above.

A secure storage appliance 120 is connected between the application server 202 and a plurality of the storage systems 204. The secure storage appliance 120 can connect to dedicated storage systems (e.g. the JBOD storage system 204_5 in Figure 4), or to storage systems connected both directly through the SAN 212, and via the secure storage appliance 120 (e.g. the JBOD storage system 204_3 and storage system 204_4). Additionally, the secure storage appliance 120 can connect to systems connected via the network 210 (e.g. the JBOD storage system 204_3). Other arrangements are possible as well. In instances where the secure storage appliance 120 is connected to one of storage systems 204, one or more of the physical storage devices 206 managed by the corresponding system is secured by way of data processing by the secure storage appliance. In the embodiment shown, the physical storage devices 206_{3-7}, 206_{10-13} are secured physical storage devices, meaning that these devices contain data managed by the secure storage appliance 120, as explained in further detail below.

Generally, inclusion of the secure storage appliance 120 within the data storage system 200 may provide improved data security for data stored on the physical storage devices. As is explained below, this can be accomplished, for example, by cryptographically splitting the data to be stored on the physical devices, such that generally each device contains only a portion of the data required to

reconstruct the originally stored data, and that portion of the data is a block-level portion of the data encrypted to prevent reconstitution by unauthorized users.

Through use of the secure storage appliance 120 within the data storage system 200, a plurality of physical storage devices 208 can be mapped to a single volume, and that volume can be presented as a virtual disk for use by one or more groups of users. In comparing the example data storage system 200 to the prior art system shown in Figure 1, it can be seen that the secure storage appliance 120 allows a user to have an arrangement other than one-to-one correspondence between drive volume letters (in Figure 1, drive letters I-M) and physical storage devices. In the embodiment shown, two additional volumes are exposed to the application server 202, virtual disk drives T and U, in which secure copies of data can be stored. Virtual disk having volume label T is illustrated as containing secured volumes F3 and F7 (i.e. the drives mapped to the iSCSI2 port of the application server 202, as well as a new drive), thereby providing a secured copy of information on either of those drives for access by a group of users. Virtual disk having volume label U provides a secured copy of the data held in DB1 (i.e. the drive mapped to LUN03). By distributing volumes across multiple disks, security is enhanced because copying or stealing data from a single physical disk will generally be insufficient to access that data (i.e. multiple disks of data, as well as separately-held encryption keys, must be acquired)

Referring now to Figure 5, a portion of the data storage system 200 is shown, including details of the secure storage appliance 120. In the embodiment shown, the secure storage appliance 120 includes a number of functional modules that generally allow the secure storage appliance to map a number of physical disks to one or more separate, accessible volumes that can be made available to a client,

and presenting a virtual disk to clients based on those defined volumes. Transparently to the user, the secure storage appliance applies a number of techniques to stored and retrieved data to provide data security.

In the embodiment shown, the secure storage appliance 120 includes a core functional unit 216, a LUN mapping unit 218, and a storage subsystem interface 220. The core functional unit 216 includes a data conversion module 222 that operates on data written to physical storage devices 206 and retrieved from the physical storage devices 206. In general, when the data conversion module 222 receives a logical unit of data (e.g. a file or directory) to be written to physical storage devices 206, it splits that primary data block at a physical level (i.e. a "block level") and encrypts the secondary data blocks using a number of encryption keys.

The manner of splitting the primary data block, and the number of physical blocks produced, is dictated by additional control logic within the core functional unit 216. As described in further detail below, during a write operation that writes a primary data block to physical storage (e.g. from an application server 202), the core functional unit 216 directs the data conversion module 222 to split the primary data block received from the application server 202 into N separate secondary data blocks. Each of the N secondary data blocks is intended to be written to a different one of physical storage devices 206 within the data storage system 200. The core functional unit 216 also dictates to the data conversion module 222 the number of shares (for example, denoted as M of the N total shares) that are required to reconstitute the primary data block when requested by the application server 202.

The secure storage appliance 120 connects to a metadata store 224, which is configured to hold metadata information about the locations, redundancy,

and encryption of the data stored on the physical storage devices 206. The metadata store 224 is generally held locally or in proximity to the secure storage appliance 120, to ensure fast access of metadata regarding the shares. The metadata store 224 can be, in various embodiments, a database or file system storage of data describing the data connections, locations, and shares used by the secure storage appliance. Additional details regarding the specific metadata stored in the metadata store 224 are described below.

The LUN mapping unit 218 generally provides a mapping of one or more physical storage devices 206 to a volume. Each volume corresponds to a specific collection of physical storage devices 206 upon which the data received from client devices is stored. In contrast, typical prior art systems assign a LUN (logical unit number) or other identifier to each physical storage device or connection port to such a device, such that data read operations and data write operations directed to one of storage systems 204 can be performed specific to a device associated with the system. In the embodiment shown, the LUNs correspond to target addressable locations on the secure storage appliance 120, of which one or more is exposed to a client device, such as an application server 202. Based on the mapping of LUNs to a volume, the virtual disk related to that volume appears as a directly-addressable component of the data storage system 200, having its own LUN. From the perspective of the application server 202, this obscures the fact that primary data blocks written to a volume can in fact be split, encrypted, and written to a plurality of physical storage devices across one or more storage systems 204.

The storage subsystem interface 220 routes data from the core functional unit 216 to the storage systems 204 communicatively connected to the secure storage appliance 120. The storage subsystem interface 220 allows

addressing various types of storage systems 204. Other functionality can be included as well.

In the embodiment shown, a plurality of LUNs are made available by the LUN mapping unit 218, for addressing by client devices. As shown by way of example, LUNs LUN04-LUNnn are illustrated as being addressable by client devices. Within the core functional unit 216, the data conversion module 222 associates data written to each LUN with a share of that data, split into N shares and encrypted. In the embodiment shown in the example of Fig. 5, a block read operation or block write operation to LUN04 is illustrated as being associated with a four-way write, in which secondary data blocks L04.a through L04.d are created, and mapped to various devices connected to output ports, shown in Figure 5 as network interface cards (NICs), a Fibre Channel interface, and a serial ATA interface. An analogous operation is also shown with respect to LUN05, but written to a different combination of shares and corresponding physical disks.

The core functional unit 216, LUN mapping unit 218, and storage subsystem interface 220 can include additional functionality as well, for managing timing and efficiency of data read and write operations. Additional details regarding this functionality are described in another embodiment, detailed below in conjunction with the secure storage appliance functionality described in Figure 6.

The secure storage appliance 120 includes an administration interface 226 that allows an administrator to set up components of the secure storage appliance 120 and to otherwise manage data encryption, splitting, and redundancy. The administration interface 226 handles initialization and discovery on the secure storage appliance, as well as creation, modifying, and deletion of individual volumes and virtual disks; event handling; data base administration; and other system

services (such as logging). Additional details regarding usage of the administration interface 226 are described below in conjunction with Figure 14.

In the embodiment shown of the secure storage appliance 120, the secure storage appliance 120 connects to an optional enterprise directory 228 and a key manager 230 via the administration interface 226. The enterprise directory 228 is generally a central repository for information about the state of the secure storage appliance 120, and can be used to help coordinate use of multiple secure storage appliances in a network, as illustrated in the configuration shown in Figure 10, below. The enterprise directory 228 can store, in various embodiments, information including a remote user table, a virtual disk table, a metadata table, a device table, log and audit files, administrator accounts, and other secure storage appliance status information.

In embodiments lacking the enterprise directory 228, redundant secure storage appliances 214 can manage and prevent failures by storing status information of other secure storage appliances, to ensure that each appliance is aware of the current state of the other appliances.

The key manager 230 stores and manages certain keys used by the data storage system 200 for encrypting data specific to various physical storage locations and various individuals and groups accessing those devices. In certain embodiments, the key manager 230 stores workgroup keys. Each workgroup key relates to a specific community of individuals (i.e. a "community of interest") and a specific volume, thereby defining a virtual disk for that community. The key manager 230 can also store local copies of session keys for access by the secure storage appliance 120. Secure storage appliance 120 uses each of the session keys to locally encrypt data on different ones of physical storage devices 206. Passwords

can be stored at the key manager 230 as well. In certain embodiments, the key manager 230 is operable on a computing system configured to execute any of a number of key management software packages, such as the Key Management Service provided for a Windows Server environment, manufactured by Microsoft Corp. of Redmond, Washington.

Although the present disclosure provides for encryption keys including session keys and workgroup keys, additional keys may be used as well, such as a disk signature key, security group key, client key, or other types of keys. Each of these keys can be stored on one or more of physical storage devices 206, at the secure storage appliance 120, or in the key manager 230.

Although Figures 4-5 illustrate a particular arrangement of a data storage system 200 for secure storage of data, additional arrangements are possible as well that can operate consistently with the concepts of the present disclosure. For example, in certain embodiments, the system can include a different number or type of storage systems or physical storage devices, and can include one or more different types of client systems in place of or in addition to the application server 202. Furthermore, the secure storage appliance 120 can be placed in any of a number of different types of networks, but does not require the presence of multiple types of networks as illustrated in the example of Figure 4.

Figure 6 is a block diagram that illustrates example logical components of the secure storage appliance 120. Figure 6 represents only one example of the logical components of the secure storage appliance 120, for performing the operations described herein. The operations of the secure storage appliance 120 can be conceptualized and implemented in many different ways.

As illustrated in the example of Figure 6, the secure storage appliance 120 comprises a primary interface 300 and a secondary interface 302. The primary interface 300 enables secure storage appliance 120 to receive primary I/O requests and to send primary I/O responses. For instance, the primary interface 300 can enable secure storage appliance 120 to receive primary I/O requests (e.g. read and write requests) from the application server device 202 and to send primary I/O responses to the application server 202. Secondary interface enables the secure storage appliance 120 to send secondary I/O requests to the storage systems 204, and to receive secondary I/O responses from those storage systems 204.

In addition, the secure storage appliance 120 comprises a parser driver 304. The parser driver 304 generally corresponds to the data conversion module 222 of Figure 5, in that it processes primary I/O requests to generate secondary I/O requests and processes secondary I/O responses to generate primary I/O responses. To accomplish this, the parser driver 304 comprises a read module 305 that processes primary read requests to generate secondary read requests and processes secondary read responses to generate primary read responses. In addition, the parser driver 304 comprises a decryption module 308 that enables the read module 305 to reconstruct a primary data block using secondary blocks contained in secondary read responses. Example operations performed by the read module 305 are described below with reference to Figs. 15, 22, and 24. Furthermore, the parser driver 304 comprises a write module 306 that processes primary write requests to generate secondary write requests and processes secondary write responses to generate primary write responses. The parser driver 304 also comprises an encryption module 310 that enables the write module 306 to cryptographically split primary data blocks in primary write requests into secondary data blocks to put in

secondary write requests. An example operation performed by the write module 306 is described below as well with reference to Figs. 16, 23, and 25.

In the example of Figure 6, the secure storage appliance 120 also comprises a cache driver 315. When enabled, the cache driver 315 receives primary I/O requests received by the primary interface 300 before the primary I/O requests are received by parser driver 304. When the cache driver 315 receives a primary read request to read data at a primary storage location of a virtual disk, the cache driver 315 determines whether a write-through cache 316 at the secure storage appliance 120 contains a primary write request to write a primary data block to the primary storage location of the virtual disk. If the cache driver 315 determines that the write-through cache 316 contains a primary write request to write a primary data block to the primary storage location of the virtual disk, the cache driver 315 outputs a primary read response that contains the primary data block. When the parser driver 304 receives a primary write request to write a primary data block to a primary storage location of a virtual disk, the cache driver 315 caches the primary write request in the write-through cache 316. A write-through module 318 performs write operations to memory from the write-through cache 316.

The secure storage appliance 120 also includes an outstanding write list (OWL) module 326. When enabled, the OWL module 326 receives primary I/O requests from the primary interface 300 before the primary I/O requests are received by the parser driver 304. The OWL module 326 uses an outstanding write list 320 to process the primary I/O requests.

In addition, the secure storage appliance 120 comprises a backup module 324. The backup module 324 performs an operation that backs up data at

the storage systems 204 to backup devices, as described below in conjunction with Figures 17-18.

The secure storage appliance 120 also comprises a configuration change module 312. The configuration change module 312 performs an operation that creates or destroys a volume, and sets its redundancy configuration. Example redundancy configurations (i.e. "M of N" configurations) are described throughout the present disclosure, and refer to the number of shares formed from a block of data, and the number of those shares required to reconstitute the block of data. Further discussion is provided with respect to possible redundancy configurations below, in conjunction with Figures 8-9.

It should be appreciated that many alternate implementations of the secure storage appliance 120 are possible. For example, a first alternate implementation of the secure storage appliance 120 can include the OWL module 326, but not the cache driver 315, or vice versa. In other examples, the secure storage appliance 120 might not include the backup module 324 or the configuration change module 312. Furthermore, there can be many alternate operations performed by the various modules of the secure storage appliance 120.

Figure 7 illustrates further details regarding connections to and operational hardware and software included in secure storage appliance 120, according to a possible embodiment of the present disclosure. The secure storage appliance 120 illustrates the various operational hardware modules available in the secure storage appliance to accomplish the data flow and software module operations described in Figures 4-6, above. In the embodiment shown, the secure storage appliance 120 is communicatively connected to a client device 402, an

administrative console 404, a key management server 406, a plurality of storage devices 408, and an additional secure storage appliance 120'.

In the embodiment shown, the secure storage appliance 120 connects to the client device 402 via both an IP network connection 401 and a SAN network connection 403. The secure storage appliance 120 connects to the administrative console 404 by one or more IP connections 405 as well. The key management server 406 is also connected to the secure storage appliance 120 by an IP network connection 407. The storage devices 408 are connected to the secure storage appliance 120 by the SAN network connection 403, such as a Fibre Channel or other high-bandwidth data connection. Finally, in the embodiment shown, secure storage appliances 120 and 120' are connected via any of a number of types of communicative connections 411, such as an IP or other connection, for communicating heartbeat messages and status information for coordinating actions of the secure storage appliance 120 and the secure storage appliance 120'. Although in the embodiment shown, these specific connections and systems are included, the arrangement of devices connected to the secure storage appliance 120, as well as the types and numbers of devices connected to the appliance may be different in other embodiments.

The secure storage appliance 120 includes a number of software-based components, including a management service 410 and a system management module 412. The management service 410 and the system management module 412 each connect to the administrative console 404 or otherwise provide system management functionality for the secure storage appliance 120. The management service 410 and system management module 412 are generally used to set various settings in the secure storage appliance 120, view logs 414 stored on the appliance,

and configure other aspects of a network including the secure storage appliance 120. Additionally, the management service 410 connects to the key management server 406, and can request and receive keys from the key management server 406 as needed.

A cluster service 416 provides synchronization of state information between the secure storage appliance 120 and secure storage appliance 120'. In certain embodiments, the cluster service 416 manages a heartbeat message and status information exchanged between the secure storage appliance 120 and the secure storage appliance 120'. Secure storage appliance 120 and secure storage appliance 120' periodically exchange heartbeat messages to ensure that secure storage appliance 120 and secure storage appliance 120' maintain contact. Secure storage appliance 120 and secure storage appliance 120' maintain contact to ensure that the state information received by each secure storage appliance indicating the state of the other secure storage appliance is up to date. An active directory services 418 stores the status information, and provides status information periodically to other secure storage appliances via the communicative connections 411.

Additional hardware and/or software components provide datapath functionality to the secure storage appliance 120 to allow receipt of data and storage of data at the storage devices 408. In the embodiment shown, the secure storage appliance 120 includes a SNMP connection module 420 that enables secure storage appliance 120 to communicate with client devices via the IP network connection 401, as well as one or more high-bandwidth data connection modules, such as a Fibre Channel input module 422 or SCSI input module 424 for receiving data from the client device 402 or storage devices 408. Analogous data output modules including a Fibre Channel connection module 421 or SCSI connection module 423

can connect to the storage devices 408 or client device 402 via the SAN network connection 403 for output of data.

Additional functional systems within the secure storage appliance 120 assist in datapath operations. A SCSI command module 425 parses and forms commands to be sent out or received from the client device 402 and storage devices 408. A multipath communications module 426 provides a generalized communications interface for the secure storage appliance 120, and a disk volume 428, disk 429, and cache 316 provide local data storage for the secure storage appliance 120.

Additional functional components can be included in the secure storage appliance 120 as well. In the embodiment shown, a parser driver 304 provides data splitting and encryption capabilities for the secure storage appliance 120, as previously explained. A provider 434 includes volume management information, for creation and destruction of volumes. An events module 436 generates and handles events based on observed occurrences at the secure storage appliance (e.g. data errors or communications errors with other systems).

Figures 8-9 provide a top level sense of a dataflow occurring during write and read operations, respectively, passing through a secure storage appliance, such as the secure storage appliance described above in conjunction with Figures 3-7. Figure 8 illustrates a dataflow of a write operation according to a possible embodiment of the present disclosure, while Figure 9 illustrates dataflow of a read operation. In the write operation of Figure 8, a primary data block 450 is transmitted to a secure storage appliance (e.g. from a client device such as an application server). The secure storage appliance can include a functional block 460 to separate the primary data block into N secondary data blocks 470, shown as S-1 through S-N.

In certain embodiments, the functional block 460 is included in a parser driver, such as parser driver 304, above. The specific number of secondary data blocks can vary in different networks, and can be defined by an administrative user having access to control settings relevant to the secure storage appliance. Each of the secondary data blocks 470 can be written to separate physical storage devices. In the read operation of Figure 9, M secondary data blocks are accessed from physical storage devices, and provided to the functional block 460 (e.g. parser driver 304). The functional block 460 then performs an operation inverse to that illustrated in Figure 8, thereby reconstituting the primary data block 450. The primary data block can then be provided to the requesting device (e.g. a client device).

In each of Figures 8-9, the N secondary data blocks 470 each represent a cryptographically split portion of the primary data block 450, such that the functional block 460 requires only M of the N secondary data blocks (where M <= N) to reconstitute the primary data block 450. The cryptographic splitting and data reconstitution of Figures 8-9 can be performed according to any of a number of techniques. In one embodiment, the parser driver 304 executes SecureParser software provided by Security First Corporation of Rancho Santa Margarita, California.

Although, in the embodiment shown in Figure 9, the parser driver 304 uses the N secondary data blocks 470 to reconstitute the primary data block 450, it is understood that in certain applications, fewer than all of the N secondary data blocks 470 are required. For example, when the parser driver 304 generates N secondary data blocks during a write operation such that only M secondary data blocks are required to reconstitute the primary data block (where M < N), then data

conversion module 60 only needs to read that subset of secondary data block from physical storage devices to reconstitute the primary data block 450.

For example, during operation of the parser driver 304 a data conversion routine may generate four secondary data blocks 470, of which two are needed to reconstitute a primary data block (i.e. M = 2, N = 4). In such an instance, two of the secondary data blocks 470 may be stored locally, and two of the secondary data blocks 470 may be stored remotely to ensure that, upon failure of a device or catastrophic event at one location, the primary data block 450 can be recovered by accessing one or both of the secondary data blocks 470 stored remotely. Other arrangements are possible as well, such as one in which four secondary data blocks 470 are stored locally and all are required to reconstitute the primary data block 450 (i.e. M = 4, N = 4). At its simplest, a single share could be created (M = N = 1).

Figure 10 illustrates a further possible embodiment of a data storage system 250, according to a possible embodiment of the present disclosure. The data storage system 250 generally corresponds to the data storage system 200 of Figure 4, above, but further includes redundant secure storage appliances 214. Each of secure storage appliances 214 may be an instance of secure storage appliance 120. Inclusion of redundant secure storage appliances 214 allows for load balancing of read and write requests in the data storage system 250, such that a single secure storage appliance is not required to process every secure primary read command or primary write command passed from the application server 202 to one of the secure storage appliances 214. Use of redundant secure storage appliances also allows for failsafe operation of the data storage system 250, by ensuring that requests made of a failed secure storage appliance are rerouted to alternative secure storage appliances.

In the embodiment of the data storage system 250 shown, two secure storage appliances 214 are shown. Each of the secure storage appliances 214 can be connected to any of a number of clients (e.g. the application server 202), as well as secured storage systems 204, the metadata store 224, and a remote server 252. In various embodiments, the remote server 252 could be, for example, an enterprise directory 228 and/or a key manager 230.

The secure storage appliances 214 are also typically connected to each other via a network connection. In the embodiment shown in the example of Fig. 10, the secure storage appliances 214 reside within a network 254. In various embodiments, network 254 can be, for example, an IP-based network, SAN as previously described in conjunction with Figures 4-5, or another type of network. In certain embodiments, the network 254 can include aspects of one or both types of networks. An example of a particular configuration of such a network is described below in conjunction with Figures 11-12.

The secure storage appliances 214 in the data storage system 250 are connected to each other across a TCP/IP portion of the network 254. This allows for the sharing of configuration data, and the monitoring of state, between the secure storage appliances 214. In certain embodiments there can be two IP-based networks, one for sharing of heartbeat information for resiliency, and a second for configuration and administrative use. The secure storage appliance 120 can also potentially be able to access the storage systems 204, including remote storage systems, across an IP network using a data interface.

In operation, sharing of configuration data, state data, and heartbeat information between the secure storage appliances 214 allows the secure storage appliances 214 to monitor and determine whether other secure storage appliances are

present within the data storage system 250. Each of the secure storage appliances 214 can be assigned specific addresses of read operations and write operations to process. Secure storage appliances 214 can reroute received I/O commands to the appropriate one of the secure storage appliances 214 assigned that operation based upon the availability of that secure storage appliance and the resources available to the appliance. Furthermore, the secure storage appliances 214 can avoid addressing a common storage device 204 or application server 202 port at the same time, thereby avoiding conflicts. The secure storage appliances 214 also avoid reading from and writing to the same share concurrently to prevent the possibility of reading stale data.

When one of the secure storage appliances 214 fails, a second secure storage appliance can determine the state of the failed secure storage appliance based upon tracked configuration data (e.g. data tracked locally or stored at the remote server 252). The remaining operational one of the secure storage appliances 214 can also access information in the metadata store 224, including share and key information defining volumes, virtual disks and client access rights, to either process or reroute requests assigned to the failed device.

As previously described, the data storage system 250 is intended to be exemplary of a possible network in which aspects of the present disclosure can be implemented; other arrangements are possible as well, using different types of networks, systems, storage devices, and other components.

Referring now to Figure 11, one possibility of a methodology of incorporating secure storage appliances into a data storage network, such as a SAN, is shown according to a possible embodiment of the present disclosure. In the embodiment shown, a secure storage network 500 provides for fully redundant

storage, in that each of the storage systems connected at a client side of the network is replicated in mass storage, and each component of the network (switches, secure storage appliances) is located in a redundant array of systems, thereby providing a failsafe in case of component failure. In alternative embodiments, the secure storage network 500 can be simplified by including only a single switch and/or single secure storage appliance, thereby reducing the cost and complexity of the network (while coincidentally reducing the protection from component failure).

In the embodiment shown, an overall secure storage network 500 includes a plurality of data lines 502a-d interconnected by switches 504a-b. Data lines 502a-b connect to storage systems 506a-c, which connect to physical storage disks 508a-f. The storage systems 506a-c correspond generally to smaller-scale storage servers, such as an application server, client device, or other system as previously described. In the embodiment shown in the example of Fig. 11, storage system 506a connects to physical storage disks 508a-b, storage system 506b connects to physical storage disks 508c-d, and storage system 506c connects to physical storage disks 508e-f. The secure storage network 500 can be implemented in a number of different ways, such as through use of Fibre Channel or iSCSI communications as the data lines 502a-d, ports, and other data communications channels. Other high bandwidth communicative connections can be used as well.

The switches 504a-b connect to a large-scale storage system, such as the mass storage 510 via the data lines 502c-d. The mass storage 510 includes, in the embodiment shown, two data directors 512a-b, which respectively direct data storage and requests for data to one or more of the back end physical storage devices 514a-d. In the embodiment shown, the physical storage devices 514a-c are

unsecured (i.e. not cryptographically split and encrypted), while the physical storage device 514d stores secure data (i.e. password secured or other arrangement).

The secure storage appliances 516a-b also connect to the data lines 502a-d, and each connect to the secure physical storage devices 518a-e. Additionally, the secure storage appliances 516a-b connect to the physical storage devices 520a-c, which can reside at a remote storage location (e.g. the location of the large-scale storage system mass storage 510).

In certain embodiments providing redundant storage locations, the secure storage network 500 allows a user to configure the secure storage appliances 516a-b such that, using the M of N cryptographic splitting enabled in each of the secure storage appliances 516a-b, M shares of data can be stored on physical storage devices at a local location to provide fast retrieval of data, while another M shares of data can be stored on remote physical storage devices at a remote location. Therefore, failure of one or more physical disks or secure storage appliances does not render data unrecoverable, because a sufficient number of shares of data remain accessible to at least one secure storage appliance capable of reconstituting requested data.

Figure 12 illustrates a particular cluster-based arrangement of a data storage network 600 according to a possible embodiment of the present disclosure. The data storage network 600 is generally arranged such that clustered secure storage appliances access and store shares on clustered physical storage devices, thereby ensuring fast local storage and access to the cryptographically split data. The data storage network 600 is therefore a particular arrangement of the networks and systems described above in Figures 1-11, in that it represents an arrangement in which physical proximity of devices is accounted for.

In the embodiment shown, the data storage network 600 includes two clusters, 602a-b. Each of the clusters 602a-b includes a pair of secure storage appliances 604a-b, respectively. In the embodiment shown, the clusters 602a-b are labeled as clusters A and B, respectively, with each cluster including two secure storage appliances 604a-b (shown as appliances A1 and A2 in cluster 602a, and appliances B1 and B2 in cluster 602b, respectively). The secure storage appliances 604a-b within each of the clusters 602a-b are connected via a data network 605 (e.g. via switches or other data connections in an iSCSI, Fibre Channel, or other data network, as described above and indicated via the nodes and connecting lines shown within the data network 605) to a plurality of physical storage devices 610. Additionally, the secure storage appliances 604a-b are connected to client devices 612, shown as client devices C1-C3, via the data network 605. The client devices 612 can be any of a number of types of devices, such as application servers, database servers, or other types of data-storing and managing client devices.

In the embodiment shown, the client devices 612 are connected to the secure storage appliances 604a-b such that each of client devices 612 can send I/O operations (e.g. a read request or a write request) to two or more of the secure storage appliances 604a-b, to ensure a backup datapath in case of a connection failure to one of secure storage appliances 604a-b. Likewise, the secure storage appliances 604a-b of each of clusters 602a-b are both connected to a common set of physical storage devices 610. Although not shown in the example of Fig. 12, the physical storage devices 610 can be, in certain embodiments, managed by separate storage systems, as described above. Such storage systems are removed from the illustration of the data storage network 600 for simplicity, but can be present in practice.

An administrative system 614 connects to a maintenance console 616 via a local area network 618. Maintenance console 616 has access to a secured domain 620 of an IP-based network 622. The maintenance console 616 uses the secured domain 620 to access and configure the secure storage appliances 604a-b. One method of configuring the secure storage appliances is described below in conjunction with Figure 14.

The maintenance console 616 is also connected to both the client devices 612 and the physical storage devices 610 via the IP-based network 622. The maintenance console 616 can determine the status of each of these devices to determine whether connectivity issues exist, or whether the device itself has become non-responsive.

Referring now to Figure 13, an example physical block structure of data written onto one or more physical storage devices is shown, according to aspects of the present disclosure. The example of Fig. 13 illustrates three strips 700A, 700B, and 700C (collectively, "shares"). Each of strips 700 is a share of a physical storage device devoted to storing data associated with a common volume. For example, in a system in which a write operation splits a primary data block into three secondary data blocks (i.e. N = 3), the strips 700 (shares) would be appropriately used to store each of the secondary data blocks. As used in this disclosure, a volume is grouped storage that is presented by a secure storage appliance to clients of secure storage appliance (e.g. secure storage appliance 120 or one of secure storage appliances 214 as previously described), such that the storage appears as a contiguous, unitary storage location. Secondary data blocks of a volume are distributed among strips 700. In systems implementing a different number of shares (e.g. N = 2, 4, 6, etc.), a different, corresponding number of shares

would be used. As basic as a 1 of 1 configuration (M = 1, N = 1) configuration could be used.

Each of the strips 700 corresponds to a reserved portion of memory of a different one of physical storage devices (e.g. physical storage devices 206 previously described), and relates to a particular I/O operation from storage or reading of data to/from the physical storage device. Typically, each of the strips 700 resides on a different one of physical storage devices. Furthermore, although three different strips are shown in the illustrative embodiment shown, more or fewer strips can be used as well. In certain embodiments, each of the strips 700 begins on a sector boundary. In other arrangements, the each of the strips 700 can begin at any other memory location convenient for management within the share.

Each of strips 700 includes a share label 704, a signature 706, header information 708, virtual disk information 710, and data blocks 712. The share label 704 is written on each of strips 700 in plain text, and identifies the volume and individual share. The share label 704 can also, in certain embodiments, contain information describing other header information for the strips 700, as well as the origin of the data written to the strip (e.g. the originating cluster).

The signature 706 contain information required to construct the volume, and is encrypted by a workgroup key. The signatures 706 contain information that can be used to identify the physical device upon which data (i.e. the share) is stored. The workgroup key corresponds to a key associated with a group of one or more users having a common set of usage rights with respect to data (i.e. all users within the group can have access to common data.) In various embodiments, the workgroup key can be assigned to a corporate department using common data, a

common group of one or more users, or some other community of interest for whom common access rights are desired.

The header information 708 contains session keys used to encrypt and decrypt the volume information included in the virtual disk information 710, described below. The header information 708 is also encrypted by the workgroup key. In certain embodiments, the header information 708 includes headers per section of data. For example, the header information 708 may include one header for each 64 GB of data. In such embodiments, it may be advantageous to include at least one empty header location to allow re-keying of the data encrypted with a preexisting session key, using a new session key.

The virtual disk information 710 includes metadata that describes a virtual disk, as it is presented by a secure storage appliance. The virtual disk information 710, in certain embodiments, includes names to present the virtual disk, a volume security descriptor, and security group information. The virtual disk information 710 can be, in certain embodiments, encrypted by a session key associated with the physical storage device upon which the strips 700 are stored, respectively.

The secondary data blocks 712 correspond to a series of memory locations used to contain the cryptographically split and encrypted data. Each of the secondary data blocks 712 contains data created at a secure storage appliance, followed by metadata created by the secure storage appliance as well. The N secondary data blocks created from a primary data block are combined to form a stripe 714 of data. The metadata stored alongside each of the secondary data blocks 712 contains an indicator of the header used for encrypting the data. In one example implementation, each of the secondary data blocks 712 includes metadata that

specifies a number of times that the secondary data block has been written. A volume identifier and stripe location of an primary data block an be stored as well.

It is noted that, although a session key is associated with a volume, multiple session keys can be used per volume. For example, a volume may include one session key per 64 GB block of data. In this example, each 64 GB block of data contains an identifier of the session key to use in decrypting that 64 GB block of data. The session keys used to encrypt data in each of strips 700 can be of any of a number of forms. In certain embodiments, the session keys use an AES-256 Counter with Bit Splitting. In other embodiments, it may be possible to perform bit splitting without encryption. Therefore, alongside each secondary data block 712, an indicator of the session key used to encrypt the data block may be provided.

A variety of access request prioritization algorithms can be included for use with the volume, to allow access of only quickest-responding physical storage devices associated with the volume. Status information can be stored in association with a volume and/or share as well, with changes in status logged based on detection of event occurrences. The status log can be located in a reserved, dedication portion of memory of a volume. Other arrangements are possible as well.

It is noted that, based on the encryption of session keys with workgroup keys and the encryption of the secondary data blocks 712 in each of strips 700 with session keys, it is possible to effectively delete all of the data on a disk or volume (i.e. render the data useless) by deleting all workgroup keys that could decrypt a session key for that disk or volume.

Referring now to Figures 14-16, basic example flowcharts of setup and use of the networks and systems disclosed herein are described. Although these flowcharts are intended as example methods for administrative and I/O operations,

such operations can include additional steps/modules, can be performed in a different order, and can be associated with different number and operation of modules. In certain embodiments, the various modules can be executed concurrently.

Figure 14 shows a flowchart of systems and methods 800 for providing access to secure storage in a storage area network according to a possible embodiment of the present disclosure. The systems and methods 800 correspond to a setup arrangement for a network including a secure data storage system such as those described herein, including one or more secure storage appliances. The embodiments of the systems and methods described herein can be performed by an administrative user or administrative software associated with a secure storage appliance, as described herein.

Operational flow is instantiated at a start operation 802, which corresponds to initial introduction of a secure storage appliance into a network by an administrator or other individuals of such a network in a SAN, NAS, or other type of networked data storage environment. Operational flow proceeds to a client definition module 804 that defines connections to client devices (i.e. application servers or other front-end servers, clients, or other devices) from the secure storage appliance. For example, the client definition module 804 can correspond to mapping connections in a SAN or other network between a client such as application server 202 and a secure storage appliance 120 of Figure 4.

Operational flow proceeds to a storage definition module 806. The storage definition module 806 allows an administrator to define connections to storage systems and related physical storage devices. For example, the storage

definition module 806 can correspond to discovering ports and routes to storage systems 204 within the system 200 of Figure 4, above.

Operational flow proceeds to a volume definition module 808. The volume definition module 808 defines available volumes by grouping physical storage into logical arrangements for storage of shares of data. For example, an administrator can create a volume, and assign a number of attributes to that volume. A storage volume consists of multiple shares or segments of storage from the same or different locations. The administrator can determine a number of shares into which data is cryptographically split, and the number of shares required to reconstitute that data. The administrator can then assign specific physical storage devices to the volume, such that each of the N shares is stored on particular devices. The volume definition module 808 can generate session keys for storing data on each of the physical storage devices, and store that information in a key server and/or on the physical storage devices. In certain embodiments, the session keys generated in the volume definition module 808 are stored both on a key server connected to the secure storage appliance and on the associated physical storage device (e.g. after being encrypted with an appropriate workgroup key generated by the communities of interest module 810, below). Optionally, the volume definition module 808 includes a capability of configuring preferences for which shares are first accessed upon receipt of a request to read data from those shares.

Operational flow proceeds to a communities of interest module 810. The communities of interest module 810 corresponds to creation of one or more groups of individuals having interest in data to be stored on a particular volume. The communities of interest module 810 module further corresponds to assigning of access rights and visibility to volumes to one or more of those groups.

In creating the groups via the communities of interest module 810, one or more workgroup keys may be created, with each community of interest being associated with one or more workgroup keys. The workgroup keys are used to encrypt access information (e.g. the session keys stored on volumes created during operation of the volume definition module 808) related to shares, to ensure that only individuals and devices from within the community of interest can view and access data associated with that group. Once the community of interest is created and associated with a volume, client devices identified as part of the community of interest can be provided with a virtual disk, which is presented to the client device as if it is a single, unitary volume upon which files can be stored.

In use, the virtual disks appear as physical disks to the client and support SCSI or other data storage commands. Each virtual disk is associated on a many-to-one basis with a volume, thereby allowing multiple communities of interest to view common data on a volume (e.g. by replicating the relevant session keys and encrypting those keys with relevant workgroup keys of the various communities of interest). A write command will cause the data to be encrypted and split among multiple shares of the volume before writing, while a read command will cause the data to be retrieved from the shares, combined, and decrypted.

Operational flow terminates at end operation 812, which corresponds to completion of the basic required setup tasks to allow usage of a secure data storage system.

Figure 15 shows a flowchart of systems and methods 820 for reading block-level secured data according to a possible embodiment of the present disclosure. The systems and methods 820 correspond to a read or input command related to data stored via a secure storage appliance, such as those described herein.

Operational flow in the system and methods 820 begins at a start operation 822. Operational flow proceeds to a receive read request module 824, which corresponds to receipt of a primary read request at a secure storage appliance from a client device (e.g. an application server or other client device, as illustrated in Figures 3-4). The read request generally includes an identifier of a virtual disk from which data is to be read, as well as an identifier of the requested data.

Operational flow proceeds to an identity determination module 826, which corresponds to a determination of the identity of the client from which the read request is received. The client's identity generally corresponds with a specific community of interest. This assumes that the client's identity for which the secure storage appliance will access a workgroup key associated with the virtual disk that is associated with the client.

Operational flow proceeds to a share determination module 828. The share determination module 828 determines which shares correspond with a volume that is accessed by way of the virtual disk presented to the user and with which the read request is associated. The shares correspond to at least a minimum number of shares needed to reconstitute the primary data block (i.e. at least M of the N shares). In operation, a read module 830 issues secondary read requests to the M shares, and receives in return the secondary data blocks stored on the associated physical storage devices.

A success operation 832 determines whether the read module 830 successfully read the secondary data blocks. The success operation may detect for example, that data has been corrupted, or that a physical storage device holding one of the M requested shares has failed, or other errors. If the read is successful, operational flow branches "yes" to a reconstitute data module 834. The reconstitute

data module 834 decrypts a session key associated with each share with the workgroup key accessed by the identity determination module 826. The reconstitute data module 834 provides the session key and the encrypted and cryptographically split data to a data processing system within the secure storage appliance, which reconstitutes the requested data in the form of an unencrypted block of data physical disk locations in accordance with the principles described above in Figures 8-9 and 13. A provide data module 836 sends the reconstituted block of data to the requesting client device. A metadata update module 838 updates metadata associated with the shares, including, for example, access information related to the shares. From the metadata update module 838, operational flow proceeds to an end operation 840, signifying completion of the read request.

If the success operation 832 determines that not all of the M shares are successfully read, operational flow proceeds to a supplemental read operation 842, which determines whether an additional share exists from which to read data. If such a share exists (e.g. $M < N$), then the supplemental read operation reads that data, and operational flow returns to the success operation 832 to determine whether the system has now successfully read at least M shares and can reconstitute the primary data block as requested. If the supplemental read operation 842 determines that no further blocks of data are available to be read (e.g. $M = N$ or M + failed reads $> N$), operational flow proceeds to a fail module 844, which returns a failed read response to the requesting client device. Operational flow proceeds to the metadata update module 838 and end operation 840, respectively, signifying completion of the read request.

Optionally, the fail module 844 can correspond to a failover event in which a backup copy of the data (e.g. a second N shares of data stored remotely

from the first N shares) are accessed. In such an instance, once those shares are tested and failed, a fail message is sent to a client device.

In certain embodiments, commands and data blocks transmitted to the client device can be protected or encrypted, such as by using a public/private key or symmetric key encryption techniques, or by isolating the data channel between the secure storage appliance and client. Other possibilities exist for protecting data passing between the client and secure storage appliance as well.

Furthermore, although the system and methods 820 of Figure 15 illustrates a basic read operation, it is understood that certain additional cases related to read errors, communications errors, or other anomalies may occur which can alter the flow of processing a read operation. For example, additional considerations may apply regarding which M of the N shares to read from upon initially accessing physical storage devices 206. Similar considerations apply with respect to subsequent secondary read requests to the physical storage devices in case those read requests fail as well.

Figure 16 shows a flowchart of systems and methods 850 for writing block-level secured data according to a possible embodiment of the present disclosure. The systems and methods 850 as disclosed provide a basic example of a write operation, and similarly to the read operation of Figure 15 additional cases and different operational flow may be used.

In the example systems and methods 850 disclosed, operational flow is instantiated at a start operation 852. Operational flow proceeds to a write request receipt module 854, which corresponds to receiving a primary write request from a client device (e.g. an application server as shown in Figures 3-4) at a secure storage

appliance. The primary write request generally addresses a virtual disk, and includes a block of data to be written to the virtual disk.

Operational flow proceeds to an identity determination module 856, which determines the identity of the client device from which the primary write request is received. After determining the identity of the client device, the identity determination module 856 accesses a workgroup key based upon the identity of the client device and accesses the virtual disk at which the primary write request is targeted. Operational flow proceeds to a share determination module 858, which determines the number of secondary data blocks that will be created, and the specific physical disks on which those shares will be stored. The share determination module 858 obtains the session keys for each of the shares that are encrypted with the workgroup key obtained in the identity determination module 856 (e.g. locally, from a key manager, or from the physical disks themselves). These session keys for each share are decrypted using the workgroup key.

Operational flow proceeds to a data processing module 860, which provides to the parser driver 304 the share information, session keys, and the primary data block. The parser driver 304 operates to cryptographically split and encrypt the primary data block, thereby generating N secondary data blocks to be written to N shares in accordance with the principles described above in the examples of Figures 8-9 and 13. Operational flow proceeds to a secondary write module 862 which transmits the share information to the physical storage devices for storage.

Operational flow proceeds to a metadata storage module 864, which updates a metadata repository by logging the data written, allowing the secure storage appliance to track the physical disks upon which data has been written, and

with what session and workgroup keys the data can be accessed. Operational flow terminates at an end operation 866, which signifies completion of the write request.

As previously mentioned, in certain instances additional operations can be included in the system and methods 850 for writing data using the secure storage appliance. For example, confirmation messages can be returned to the secure storage appliance confirming successful storage of data on the physical disks. Other operations are possible as well.

Now referring to Figures 17-18 of the present disclosure, certain applications of the present disclosure are discussed in the context of (1) data backup systems and (2) secure network thin client network topology used in the business setting. Figure 17 shows an example system 900 for providing secure storage data backup, according to a possible embodiment of the present disclosure. In the system 900 shown, a virtual tape server 902 is connected to a secure storage appliance 904 via a data path 906, such as a SAN network using Fibre Channel or iSCSI communications. The virtual tape server 902 includes a management system 908, a backup subsystem interface 910, and a physical tape interface 912. The management system 908 provides an administrative interface for performing backup operations. The backup subsystem interface 910 receives data to be backed up onto tape, and logs backup operations. A physical tape interface 912 queues and coordinates transmission of data to be backed up to the secure storage appliance 904 via the network. The virtual tape server 902 is also connected to a virtual tape management database 914 that stores data regarding historical tape backup operations performed using the system 900.

The secure storage appliance 904 provides a virtual tape head assembly 916 which is analogous to a virtual disk but appears to the virtual tape

server 902 to be a tape head assembly to be addressed and written to. The secure storage appliance 904 connects to a plurality of tape head devices 918 capable of writing to magnetic tape, such as that typically used for data backup. The secure storage appliance 904 is configured as described above. The virtual tape head assembly 916 provides an interface to address data to be backed up, which is then cryptographically split and encrypted by the secure storage appliance and stored onto a plurality of distributed magnetic tapes using the tape head devices 918 (as opposed to a generalized physical storage device, such as the storage devices of Figures 3-4).

In use, a network administrator could allocate virtual disks that would be presented to the virtual tape head assembly 916. The virtual tape administrator would allocate these disks for storage of data received from the client through the virtual tape server 902. As data is written to the disks, it would be cryptographically split and encrypted via the secure storage appliance 904.

The virtual tape administrator would present virtual tapes to a network (e.g. an IP or data network) from the virtual tape server 902. The data in storage on the tape head devices 918 is saved by the backup functions provided by the secure storage appliance 904. These tapes are mapped to the virtual tapes presented by the virtual tape head assembly 916. Information is saved on tapes as a collection of shares, as previously described.

An example of a tape backup configuration illustrates certain advantages of a virtual tape server over the standard tape backup system as described above in conjunction with Figure 2. In one example of a tape backup configuration, share 1 of virtual disk A, share 1 of virtual disk B, and other share 1's can be saved to a tape using the tape head devices 918. Second shares of each of

these virtual disks could be stored to a different tape. Keeping the shares of a virtual tape separate preserves the security of the information, by distributing that information across multiple tapes. This is because more than one tape is required to reconstitute data in the case of a data restoration. Data for a volume is restored by restoring the appropriate shares from the respective tapes. In certain embodiments an interface that can automatically restore the shares for a volume can be provided for the virtual tape assembly. Other advantages exist as well.

Now referring to Figure 18, one possible arrangement of a thin client network topology is shown in which secure storage is provided. In the network 950 illustrated, a plurality of thin client devices 952 are connected to a consolidated application server 954 via a secured network connection 956.

The consolidated application server 954 provides application and data hosting capabilities for the thin client devices 952. In addition, the consolidated application server 954 can, as in the example embodiment shown, provide specific subsets of data, functionality, and connectivity for different groups of individuals within an organization. In the example embodiment shown, the consolidated application server 954 can connect to separate networks and can include separate, dedicated network connections for payroll, human resources, and finance departments. Other departments could have separate dedicated communication resources, data, and applications as well. The consolidated application server 954 also includes virtualization technology 958, which is configured to assist in managing separation of the various departments' data and application accessibility.

The secured network connection 956 is shown as a secure Ethernet connection using network interface cards 957 to provide network connectivity at the

server 954. However, any of a number of secure data networks could be implemented as well.

The consolidated application server 954 is connected to a secure storage appliance 960 via a plurality of host bus adapter connections 961. The secure storage appliance 960 is generally arranged as previously described in Figures 3-16. The host bus adapter connections 961 allow connection via a SAN or other data network, such that each of the dedicated groups on the consolidated application server 954 has a dedicated data connection to the secure storage appliance 960, and separately maps to different port logical unit numbers (LUNs). The secure storage appliance 960 then maps to a plurality of physical storage devices 962 that are either directly connected to the secure storage appliance 960 or connected to the secure storage appliance 960 via a SAN 964 or other data network.

In the embodiment shown, the consolidated application server 954 hosts a plurality of guest operating systems 955, shown as guest operating systems 955a-c. The guest operating systems 955 host user-group-specific applications and data for each of the groups of individuals accessing the consolidated application server. Each of the guest operating systems 955a-c have virtual LUNs and virtual NIC addresses mapped to the LUNs and NIC addresses within the server 954, while virtualization technology 958 provides a register of the mappings of LUNS and NIC addresses of the server 954 to the virtual LUNs and virtual NIC addresses of the guest operating systems 955a-c. Through this arrangement, dedicated guest operating systems 955 can be mapped to dedicated LUN and NIC addresses, while having data that is isolated from that of other groups, but shared across common physical storage devices 962.

As illustrated in the example of Figure 18, the physical storage devices 962 provide a typical logistical arrangement of storage, in which a few storage devices are local to the secure storage appliance, while a few of the other storage devices are remote from the secure storage appliance 960. Through use of (1) virtual disks that are presented to the various departments accessing the consolidated application server 954 and (2) shares of virtual disks assigned to local and remote storage, each department can have its own data securely stored across a plurality of locations with minimal hardware redundancy and improved security.

Although Figures 17-18 present a few options for applications of the secure storage appliance and secure network storage of data as described in the present disclosure, it is understood that further applications are possible as well. Furthermore, although each of these applications is described in conjunction with a particular network topology, it is understood that a variety of network topologies could be implemented to provide similar functionality, in a manner consistent with the principles described herein.

Now referring to Figures 19-24, various additional details are provided relating to internal details of handling I/O requests (e.g. read and write operation requests) in a secure storage appliance. In the various methods and systems disclosed in the below-described figures, state-based processing of data blocks is performed, allowing the secure storage appliance to perform sub-tasks as resources of the secure storage appliance become available for use. In such a manner, the secure storage appliance can improve throughput of processed data and I/O requests related to that data, based on these "pipelined" operations.

Referring now to Figure 19, a state diagram 1000 for simultaneous state-based cryptographic splitting in a secure storage appliance is shown, according

to aspects of the present disclosure. The state diagram represents states assignable to various stripes of data, represented as blocks of data written to or received from storage devices and managed in memory of a secure storage appliance. By assigning various states to the buffers and blocks of data stored in those buffers, a secure storage appliance using such states can employ thread-level parallelism to process multiple blocks of data (i.e. stripes).

In the embodiment shown, the state diagram 1000 includes an idle state 1002, a read state 1004, a decode state 1006, a transfer state 1008, an encode state 1010, and a write state 1012. The idle state 1002 represents a state in which a stripe (i.e. a block of data able to be stored in a buffer) is currently not in use. The buffer can include, for example, a direct buffer or a data buffer intended to hold a block of data (i.e. a stripe of data). So long as the state diagram remains in the idle state 1002 for that buffer, the buffer is available for reuse, signifying that no data is being tracked in that buffer. The idle state 1002 can be entered from any of the other states, upon failure of an operation, or upon completion of an I/O request.

The read state 1004 signifies that data is being read from a plurality of shares and is destined for storage in a buffer on the secure storage appliance. The read state 1004 can be entered from the idle state any time the data being accessed is not present in memory, or upon retrying a previously unsuccessful read or decode operation.

The decode state 1006 signifies that data read (e.g. while the buffer is associated with the read state 1004) has occurred, and that currently the plurality of secondary data blocks are being decoded to form the block of data stored in the stripe. The decode state 1006 generally signifies that the data is being operated on by a cryptographic decoding operation, such as through use of a parser driver as

previously described. The decode state 1006 can be entered, for example, from the read state 1004 upon determination of a successful read and available parser module, or upon retrying a previously failed decode operation.

The transfer state 1008 indicates that the I/O request received at the secure storage appliance is being transferred into or out from the block of data held in the buffer. In the case of a write I/O request, the transfer state 1008 corresponds to writing data into the block of data, and marking the block of data as dirty (i.e. the data stored on physical storage devices is not up to date). In the case of a read I/O request, the transfer state 1008 corresponds to return of some or all of the block of data to a client device from the buffer. The transfer state 1008 can be entered, for example, from the decode states 1006 upon determining that a stripe is present (i.e. that the block of data making up the stripe is present in a buffer).

The transfer state 1008 can also be entered from the idle state 1002 in case either the stripe is already present (e.g. based on action in response to a different I/O request) or in the case that a full block write is taking place (in which case a read of that block is unnecessary, as the entire block will be overwritten).

The encode state 1010 signifies that the transfer state 1008 has completed, such that the data in the buffer is the most up-to-date data related to that block. The encode state 1010 corresponds to operation of the parser module of a secure storage appliance to cryptographically split and encrypt the data in the block of data. The encode state 1010 can be entered from the transfer state 1008 upon determination that the transfer state has completed and that the parser module is available. The encode state 1010 can also be entered from itself, such as upon retry of a failed encode operation.

The write state 1012 signifies completion of the encode state 1010, and schedules writing of the encoded data to a plurality of shares associated with the volume and strip to which the data is stored. The write state 1012 can track the existence of the buffer in an outstanding write list (e.g. as described above in conjunction with Figure 6) or other write operation. The write state 1012 can be entered from the encode state 1010 or upon reentry from itself, in the case of a failed write.

Additional states can be included as well, depending upon whether any additional processing actions are required which may use a resource of the secure storage appliance which may require scheduling and coordination of use.

The state diagram 1000 of Figure 19 can be implemented in software of the secure storage appliance to track the state of a number of data buffers that may be present in the secure storage appliance. In certain embodiments, the data buffers can be held in cache or RAM memory of any of the embodiments of the secure storage appliance previously described.

Figure 20 shows a flowchart of methods and systems 1100 for simultaneous state-based cryptographic splitting in a secure storage appliance, according to aspects of the present disclosure. The flowchart tracks processing of a single buffer and related block of data in the secure storage appliance. As illustrated, the methods and systems 1100 split each I/O request into a plurality of tasks, thereby allowing each I/O request to be managed in parallel and executed as resources in the secure storage appliance (read and write data lines, buffers, parser driver, etc) become available.

The system 1100 is instantiated at a start operation 1102, which corresponds to initial operation of a secure storage appliance or connection of the

secure storage appliance to a client device such that the secure storage appliance can begin receiving I/O requests. Operational flow proceeds to a request receipt module 1104 which receives an I/O request (e.g. a read or write request) associated with a particular block of data on a volume. The block of data, as referred to herein, corresponds to a block of data as expected to be received by the client device, rather than the cryptographically split secondary data blocks stored on the shares of the physical storage device.

Operational flow proceeds to a stripe presence determination operation 1106. The stripe presence determination operation 1106 determines whether the stripe related to the received I/O request is present in the secure storage appliance. This may be the case, for example, if the stripe (i.e. the block of data) has previously been requested by a different I/O operation and is present in a buffer of the secure storage appliance. The stripe presence determination operation 1106 also determines whether the I/O request is a full block write (and therefore there is no need to acquire the data block prior to performing a read or write).

If the stripe is not present in the secure storage appliance (and the I/O request is not a full block write), operational flow branches "no" from the stripe presence determination operation 1106 to a read module 1108. The read module 1108 initiates a read process to obtain a block of data from a volume by accessing cryptographically split secondary data blocks on a plurality of shares on a plurality of storage devices. During execution of the read module 1108, a buffer can also be reserved for the read block of data, and the buffer state can be set to a read state, as described in Figure 19, above.

A read assessment operation 1110 determines whether the read module executed successfully. If the read assessment operation 1110 determines

that the read module 1108 did not execute successfully, operational flow branches "no" and returns to the read module to retry the read operation. In certain embodiments, after a number of failed read assessment operations, operational flow fails, and the entire system 1100 is restarted.

If the read assessment operation 1110 determines that the read module 1108 executed successfully, operational flow branches "yes" to a decode module 1112. The decode module 1112 receives the cryptographically split secondary data blocks, and reconstitutes the block of data from those secondary data blocks. In certain embodiments, this can be accomplished by using a parser driver, as previously explained in conjunction with Figure 6. During operation of the decode module, the state of the buffer reserved for use in conjunction with the block of data can be set to a decode state, as described above in Figure 19.

A decode assessment operation 1114 determines whether the decode module 1112 executed successfully, by checking the correctness of the block of data output to a buffer from the parser driver or other software/hardware used to reconstitute the block of data. If the decode assessment operation 1114 determines that the decode module 1112 executed successfully, operational flow branches "yes" to a transfer module 1116. If the decode assessment operation 1114 determines that the decode module 1112 failed, operational flow branches "no" and returns to the read module 1108 to retry the reading and decoding process. In such an instance, the state of the buffer is changed from the decode state to the read state, and the read operation is reattempted.

In an alternative embodiment, if the decode assessment operation 1114 determines that the decode module 1112 failed, operational flow can branch

"no" and return to the decode module 1112 to retry the decoding process only (e.g. as shown in Figure 19).

After successful decoding of a block of data identified in the overall system 1100, a desired block of data is residing in a buffer on the secure storage appliance, or a full block write is to be performed. Operational flow proceeds to a transfer operation 1116 either (1) from the decode assessment operation 1114, as described above, or, (2) if a stripe was previously present in the secure storage appliance and detected by the stripe presence determination operation 1106 or was a full block write. The transfer module associates the I/O request with the block of data (now in unencrypted, whole, clear text form) stored in a system buffer, and I/O requests related to that buffer are processed (e.g. in FIFO order). The transfer module 1116 either transfers in data relating to a write request addressing a data location within the block of data, or copies out data from the buffer related to a read request addressing a location within the block of data. If a write request is executed, then the data block will be marked as "dirty" using a flag or other means to indicate that it contains changed data. During operation of the transfer module 1116, the state of the buffer reserved for use in conjunction with the block of data can be set to a transfer state, as described above in Figure 19.

Related to that selected I/O request for processing, operational flow proceeds to an update determination operation 1118. The update determination operation determines whether data in a stripe has been updated (e.g. by a write of a full or partial data block to the buffer). If the stripe has updated data, operational flow branches "yes" to an encode module 1120. The encode module 1120 applies cryptographic splitting to the now-updated data held in a buffer on the secure storage appliance, to generate a plurality of secondary data blocks in accordance with the

techniques described above. The encode module 1120 can do so by, for example, passing the data block that is the subject of the I/O request to a parser driver in the secure storage appliance. During operation of the encode module, the state of the buffer reserved for use in conjunction with the block of data can be set to an encode state, as described above in Figure 19.

Operational flow proceeds to an encode assessment operation 1122, which determines whether the encoding of data was successful. If the encode was successful, operational flow branches "yes" and proceeds from the encode assessment operation 1122 to a write module 1124. If the encode was not successful, operational flow branches "no" and returns to the encode module 1120 to retry the encoding operation.

The write module 1124 schedules a write operation of the secondary data blocks to the plurality of shares on the physical storage devices that are associated with the volume to which the I/O is addressed and where the block of data resides. The write module 1124 in certain embodiments, does so by adding the secondary data blocks to an outstanding write list, which schedules a write operation upon the availability of a network connection (e.g. a SAN network connection such as a Fibre Channel or iSCSI) to a physical storage device. During operation of the write module, the state of the buffer reserved for use in conjunction with the block of data can be set to a write state, as described above in Figure 19.

Operational flow proceeds to a write assessment operation 1126, which determines whether the write operation completed successfully. If the write does complete successfully, operational flow branches "yes" and proceeds to a subsequent I/O determination operation 1128. If the write does not complete

successfully, operational flow branches "no" and returns to the write module 1124 to retry the write operation.

The subsequent I/O determination operation 1128 assesses whether an additional I/O request is present and which relates to the block of data. If an additional I/O request is present and awaiting execution, operational flow branches "yes" and returns to the transfer module 1116, to process that subsequent I/O request. If no additional I/O request is present, operational flow branches "no" to an end operation 1130.

Referring back to the update determination operation 1118, if the stripe has not been updated, no write operation back to a physical storage device is necessary. Therefore, operational flow branches "no" from the update determination operation and completes, terminating at end operation 1130. Additionally, and as previously described, if the I/O tracking operation determines that no additional I/O requests exist with respect to that block of data, operational flow branches "no" to the end operation 1130. Upon reaching the end operation 1130, the state can be set to an idle state, and the buffer can be made available other use, as described above in Figure 19.

Although in the system 1100 a specific set of functional modules is presented, no particular ordering of modules is required or implied. Additional states and modules can be included in the system 1100 as well, depending upon the determination of the data block status or the type of I/O request made.

Now referring to Figures 21-22, additional details regarding encoding and decoding a block of data in a secure storage device are provided in further detail. Figure 21 shows a flowchart of methods and systems for reconstituting data in a secure storage appliance, according to a possible aspect of the present

disclosure. The methods and systems 1200 described herein can correspond, in various aspects, to particular steps performed in a decode operation in association with a read or write I/O request.

The system 1200 is instantiated at a start operation 1202, which corresponds to initial scheduling of a decode operation using a parser driver of a secure storage appliance, such as any of the secure storage appliances described above. Operational flow proceeds to an obtain data module 1204, which obtains encoded data from an encoded data buffer pool and assigns a free buffer or direct buffer for storage of decoded data. The encoded data, in various embodiments, corresponds to a number of secondary data blocks that represent a cryptographically split block of data.

Operational flow proceeds to a reconstitution module 1206, which reconstitutes a block of data from the secondary data blocks. The reconstitution module 1206 generally corresponds to the decode module of Figure 20, and can, in certain embodiments, operate using a parser driver as described above in Figure 6.

Operational flow proceeds to a success determination operation 1208, which determines whether the operation performed by the decode module 1206 was successful. If the success determination operation 1208 determines that the reconstitution module 1206 has reconstituted the block of data successfully, operational flow branches "yes" to a transfer scheduling module 1210. The transfer scheduling module 1210 schedules a transfer to occur in accordance with the I/O request received by the secure storage appliance. If the I/O request is a write request, the transfer scheduling module 1210 schedules a write of received data to update the data that has been decoded. If the I/O request is a read request, the transfer scheduling module 1210 schedules a return of requested data to be sent to

the client device sending the read request, the timing of which occurs based on the availability of the connection to the client device. From the transfer scheduling module 1210, operational flow proceeds to an end operation 1212, signifying completion of the decode flow.

If the success determination operation 1208 determines that the reconstitution module 1206 has not reconstituted the block of data, operational flow branches "no" to a read scheduling module 1214, which schedules a read operation to occur, thereby retrying the request of the secondary data blocks of data from which the block of data (i.e. stripe) is reconstituted. From the read scheduling module 1214, operational flow proceeds to the end operation 1212, which represents completion of the current read and decode operation and thereby allowing the system to restart, e.g. retrying to read the block or failing and freeing the parser driver to act on another set of secondary data blocks.

Figure 22 shows a flowchart of methods and systems for cryptographically splitting data in a secure storage appliance, according to a possible aspect of the present disclosure. The methods and systems 1300 of the present disclosure generally correspond to processing of an encoding and writing portion of an I/O request, providing additional detail regarding certain portions of the overall data flow of Figure 20, above. The system 1300 is instantiated at a start operation 1302, which corresponds to initial scheduling of an encode operation using a parser driver of a secure storage appliance, such as any of the secure storage appliances described above. Operational flow proceeds to an obtain buffer module 1304, which obtains buffers for use in encoding data. The data block represents a clear text, set size data block that can be encoded into a number of secondary data blocks that represent the cryptographically split block of data.

Operational flow proceeds to an encode module 1306, which reconstitutes a block of data from the secondary data blocks. The encode module 1306 generally corresponds to the encode module of Figure 19, and can, in certain embodiments, operate using a parser driver as described above in Figure 6.

Operational flow proceeds to a success determination operation 1308, which determines whether the operation performed by the encode module 1306 was successful. If the success determination operation 1308 determines that the encode module 1306 has cryptographically split the block of data successfully, operational flow branches "yes" to a write scheduling module 1310. The write scheduling module 1310 schedules a write of the secondary data blocks to corresponding shares stored on physical storage devices connected to the secure storage appliance. From the write scheduling module 1310, operational flow proceeds to an end operation 1312, signifying completion of the encode flow.

If the success determination operation 1308 determines that the encode module 1306 has not encoded the block of data successfully, operational flow branches "no" to a transfer function module 1314, which reschedules a transfer function so that the I/O request can be reprocessed. From the transfer function module 1314, operational flow proceeds to the end operation 1312, which represents completion of the current operation and thereby allowing the system to restart, e.g. retrying to encode and write the block or failing and freeing the parser driver to act on another set of secondary data blocks.

Referring to Figures 21-22 generally, in various embodiments, each of the systems 1200, 1300 corresponds to an overall process which is tracked as a resource. In such embodiments, separate blocks of data may be operated on concurrently, and the state of each block can be tracked using states and other status

information, such as the states described in Figure 19 above. Figures 23-24 illustrate possible generalized applications of use of the state-enabled parallelism provided by the systems and methods of Figures 19-22, above.

Figure 23 shows a flowchart of methods and systems 1400 for managing data blocks in a secure storage appliance, according to a possible embodiment of the present disclosure. The systems 1400 disclosed operate within a secure storage appliance, and provide state-based management of blocks of data to provide the possibility of pipelined operation of the secure storage appliance to improve throughput and I/O request handling.

The system 1400 as shown is instantiated at a start operation 1402, which corresponds to initial operation of a secure storage appliance in conjunction with a client device and a plurality of physical storage devices. From the start operation 1402, operational flow proceeds to a data receipt module 1404. The data receipt module 1404 receives a block of data associated with a volume. The block of data is associated with an I/O request, such as a read or write request, and can be received either from a client device (e.g. in the case of a write request) or from a physical storage device (e.g. in the case of a read request). In the case the block of data is received from a physical storage request, the block of data may be a block referred to herein as a secondary data block, such that the secondary block of data represents a cryptographically split portion of a block of data as it would be viewed or presented to a client device. In further embodiments, additional blocks of data can be received as well.

Operational flow proceeds to a data storage module 1406. The data storage module 1406 stores the block of data received by the data receipt module 1404 and stores that data in a buffer. The buffer can be any of a number of buffers

available within a secure storage appliance, such as a direct buffer, any of a number of work buffers, a number of secondary buffers used to hold secondary data blocks (e.g. in the case of a read request), or other types or sizes of buffers.

Operational flow proceeds to a state association module 1408. The state association module 1408 associates the stripe with a state from among a plurality of states assignable to stipes in the system. Any of a number of states may be assigned to the stripe, depending upon the currently-pending action to be taken on data stored in the buffer (or signifying the lack of meaningful data in the buffer if the buffer has been released due to a completed I/O request). Example states are illustrated in Figure 19, above; however, other states may be possible as well.

Operational flow proceeds to a data processing module 1410. The data processing module 1410 processes the block of data by performing a cryptographic operation on it. In the case of a write operation in which a block of data is to be written to a physical storage device from a work buffer, the data processing module corresponds to cryptographic splitting of the block of data into a plurality of secondary blocks of data for storage. In the case of a read operation or a partial write operation (less than an entire block being modified), data from a physical storage device must be retrieved and reconstituted from secondary blocks of data, so an inverse function is performed. Examples of these operations are illustrated in the flowcharts of Figures 21-22, above.

While the data processing module 1410 remains in operation, the overall system preferably maintains the state of the stripe so that the secure storage appliance can track resource usage based on states of stipes. Other resource tracking arrangements are possible as well.

Operational flow proceeds to a state update module 1412. The state update module changes the state of the stripe maintaining the block of data after the data processing module 1410 completes operation, for example, once a write operation or read operation completes. In various embodiments, the state update module 1412 can change states according to the state transitions illustrated in Figure 19, above.

Operational flow within the system proceeds to an end operation 1414, which ends the process of managing the data block within the designated state.

Although Figure 23 is illustrated as including specific functionality occurring in a specified order, it is understood that the module ordering is not required, other than as necessary to maintain different states for a stripe at different stages of I/O request execution.

Figure 24 shows a flowchart of methods and systems 1500 for managing I/O requests in a secure storage appliance, according to a possible embodiment of the present disclosure. The methods and systems as described herein represent an arrangement in which multiple I/O requests can be handled in parallel, such as by tracking the state of each stripe being acted upon by I/O requests and allowing processing of an I/O request as a resource. In the context of the systems and methods described herein, these resources can include: the parser driver software and/or encryption/decryption hardware used in cryptographic splitting and reconstituting data; a data line or network connection (e.g. host bus adapter port) available between the secure storage appliance and one or more of the physical storage devices; a data connection between the secure storage appliance and a client device; a buffer, such as a work buffer, and encrypted secondary buffer, or a direct

buffer; or tracking resources available within the appliance. Other resources can be included as well.

Operational flow is instantiated at a start operation 1502, which corresponds to initial setup to allow a secure storage appliance to communicate with a client device and a plurality of physical storage devices in a network such as those described herein. Operational flow proceeds to a request receipt module 1504, which receives a plurality of I/O requests at the secure storage appliance. Each of the I/O requests received by the request receipt module 1504 corresponds to a volume and a block of data on that volume, where the volume is associated with a plurality of shares on physical storage devices. Example I/O requests will generally include the type of request (e.g. a read or write request), a location related to the request (i.e. the address of a portion of a block of data or a block of data related to the request), and, if a write operation, data to be written to the location. Other data can be transmitted as well.

Operational flow proceeds to a storage module 1506. The storage module stores blocks of data in buffers of the secure storage device. Each of the blocks of data are associated with one or more of the plurality of I/O requests. For example, the blocks of data can be reconstituted blocks of data stored in work buffers in response to read I/O requests or write I/O requests addressing only a partial block. Or, the blocks of data can include a block of data to be written to a device storage location.

Operational flow proceeds to a state association module 1508, which associates a state with each of the stripes in the secure storage appliance. The state association module 1508 can associate any of a number of states with a stripe, generally indicating the current processing state of the stripe. For example the state

assigned to the stripe can indicate how far the data associated with the stripe is processed by a currently-active I/O request. Example states are illustrated in Figure 19, above, but other states may be available as well.

Operational flow proceeds to a resource availability determination operation 1510. The resource availability determination operation 1510 determines which resource is necessary to be used next sequentially by the data in each of the buffers, and determines whether that resource is currently available. If the resource availability determination operation 1510 determines that a requested resource is available, operational flow branches "yes" and proceeds to a resource application module 1512. The resource application module 1512 applies the resource to the data in the buffer, thereby performing a required operation to process the I/O request, such as reading data, decoding data, transferring I/O requests, encoding data, writing data, or idling. Operational flow proceeds to an end operation 1514 upon completion of the resource application module 1512.

If the resource availability determination operation 1510 determines that the requested resource is not available, operational flow branches "no", issues the appropriate I/O request, and waits for the appropriate system event or events to signify that the resource to become available. Once the resource becomes available, operational flow can proceed to the resource application module 1512, above.

Optionally, the resource availability determination operation 1510 includes a time-out feature in which an operation is deemed to have failed if a resource does not become available to it within a set period of time. In other embodiments, the resource availability determination operation 1510 requires that the current I/O request and buffer must wait to complete its next operational step. However, other buffers associated with other I/O requests can be processed, so long

as the same resource is not required or used. In still further embodiments, the system uses an interrupt-based scheme to trigger use of a resource by the data in the buffer, in which a thread is notified when a resource can be allocated for its use.

Through use of the systems and methods herein, it is understood that each I/O request is split into a number of tasks, which can be pipelined to improve efficiency through the secure storage appliance.

It is recognized that the above networks, systems, and methods operate using computer hardware and software in any of a variety of configurations. Such configurations can include computing devices, which generally include a processing device, one or more computer readable media, and a communication device. Other embodiments of a computing device are possible as well. For example, a computing device can include a user interface, an operating system, and one or more software applications. Several example computing devices include a personal computer (PC), a laptop computer, or a personal digital assistant (PDA). A computing device can also include one or more servers, one or more mass storage databases, and/or other resources.

A processing device is a device that processes a set of instructions. Several examples of a processing device include a microprocessor, a central processing unit, a microcontroller, a field programmable gate array, and others. Further, processing devices may be of any general variety such as reduced instruction set computing devices, complex instruction set computing devices, or specially designed processing devices such as an application-specific integrated circuit device.

Computer readable media includes volatile memory and non-volatile memory and can be implemented in any method or technology for the storage of

information such as computer readable instructions, data structures, program modules, or other data. In certain embodiments, computer readable media is integrated as part of the processing device. In other embodiments, computer readable media is separate from or in addition to that of the processing device. Further, in general, computer readable media can be removable or non-removable. Several examples of computer readable media include, RAM, ROM, EEPROM and other flash memory technologies, CD-ROM, digital versatile disks (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium that can be used to store desired information and that can be accessed by a computing device. In other embodiments, computer readable media can be configured as a mass storage database that can be used to store a structured collection of data accessible by a computing device.

A communications device establishes a data connection that allows a computing device to communicate with one or more other computing devices via any number of standard or specialized communication interfaces such as, for example, a universal serial bus (USB), 802.11 a/b/g network, radio frequency, infrared, serial, or any other data connection. In general, the communication between one or more computing devices configured with one or more communication devices is accomplished via a network such as any of a number of wireless or hardwired WAN, LAN, SAN, Internet, or other packet-based or port-based communication networks.

The above specification, examples and data provide a complete description of the manufacture and use of the composition of the invention. Since many embodiments of the invention can be made without departing from the spirit and scope of the invention, the invention resides in the claims hereinafter appended.

Claims:

1. A method of managing data blocks in a secure storage appliance, the method comprising:

receiving a block of data associated with a volume, the volume associated with a plurality of shares stored on a plurality of physical storage devices;

storing the block of data in a buffer;

associating the block of data with a state from among a plurality of states, each of the states corresponding to a status of the block of data;

processing the block of data by performing at least one cryptographic operation on the block of data; and

upon completion of processing the block of data, updating the state of the block of data.

2. The method of claim 1, wherein processing the block of data includes cryptographically splitting the block of data into a plurality of secondary data blocks.

3. The method of claim 1, wherein processing the block of data includes reconstituting a primary block of data from a plurality of secondary blocks of data, the plurality of secondary blocks of data including the block of data.

4. The method of claim 1, wherein the plurality of states includes at least one of a read state, a decode state, an idle state, a transfer state, an encode state, or a write state.

5. The method of claim 1, further comprising, while processing the block of data, assigning a state to the block of data indicating that the block of data is being processed.

6. The method of claim 1, wherein receiving the block of data includes receiving the block of data from a client device.

7. The method of claim 5, wherein the buffer is a work buffer.

8. The method of claim 1, wherein processing the block of data includes reconstituting the block of data from a plurality of secondary data blocks stored in the plurality of shares.

9. A method of managing I/O requests in a secure storage appliance, the method including:

receiving an I/O request at the secure storage appliance, the I/O request associated with a volume, the volume associated with a plurality of shares stored on a plurality of physical storage devices;

determining whether a block of data referenced by the I/O request is present in a buffer;

transferring the block of data to a buffer and associating the block of data with a transfer state;

determining whether the block of data in the buffer is updated; and

processing the block of data.

10. The method of claim 9, wherein processing the block of data includes determining whether the data block has been updated.

11. The method of claim 10, further comprising, upon determining that the data block has been updated, cryptographically splitting the block of data into a plurality of secondary data blocks and storing the plurality of secondary data blocks on the plurality of physical storage devices.

12. The method of claim 11, further comprising, while cryptographically splitting the block of data, associating the block of data with an encode state.

13. The method of claim 11, further comprising, while storing the plurality of secondary data blocks on the plurality of physical storage devices, associating the block of data with a write state.

14. The method of claim 9, wherein transferring the block of data to a buffer includes receiving the data block from a client device.

15. The method of claim 9, further comprising, prior to transferring the block of data to a buffer:

reading a plurality of secondary data blocks stored in the plurality of shares; and

reconstituting the block of data from the plurality of secondary data blocks.

16. The method of claim 15, further comprising, while reconstituting the block of data, associating the block of data with a decode state.

17. A secure storage appliance comprising;

a plurality of buffers, each buffer capable of holding a block of data having a state selected from among a plurality of states;

a programmable circuit capable of accessing the plurality of buffers, the programmable circuit configured to execute program instructions to:

receive an I/O request, the I/O request associated with a volume, the volume associated with a plurality of shares stored on a plurality of physical storage devices communicatively connected to the secure storage appliance;

determine whether a block of data referenced by the I/O request is present in a buffer;

transfer the block of data to a buffer among the plurality of buffers;

determine whether the block of data in the buffer is updated; and

process the block of data.

18. The secure storage appliance of claim 17, wherein the plurality of states includes at least one of a read state, a decode state, an idle state, a transfer state, an encode state, or a write state.

19. The secure storage appliance of claim 17, wherein the programmable circuit is further programmed to, while transferring the block of data to a buffer, associating the block of data with a transfer state.

20. The secure storage appliance of claim 17, wherein the plurality of shares store cryptographically split data stored to the volume.

21. A secure storage appliance comprising:

a plurality of buffers, each buffer capable of holding a block of data having a state selected from among a plurality of states;

a programmable circuit capable of accessing the plurality of buffers, the programmable circuit configured to execute program instructions to:

receive a block of data associated with a volume, the volume associated with a plurality of shares stored on a plurality of physical storage devices;

store the block of data in a buffer from among the plurality of buffers;

associate the buffer with a state corresponding to a status of the block of data;

process the block of data by performing at least one cryptographic operation on the block of data; and

update the state of the buffer upon completion of processing the block of data.

22. The secure storage appliance of claim 21, wherein the programmable circuit is configured to execute program instructions to cryptographically split the block of data into a plurality of secondary data blocks.

23. The secure storage appliance of claim 21, wherein the programmable circuit is configured to execute program instructions to reconstitute a primary block of data from a plurality of secondary blocks of data, the plurality of secondary blocks of data including the block of data.

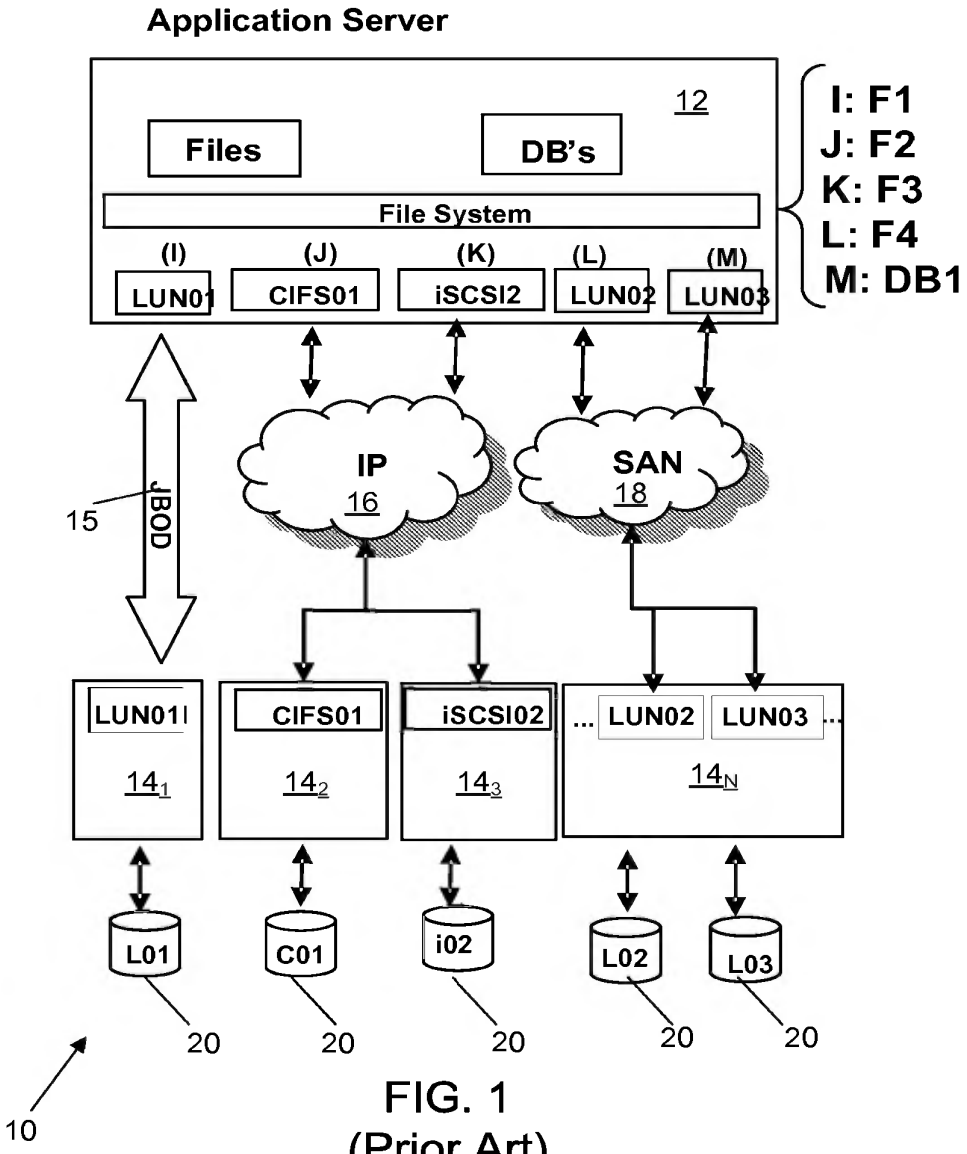


FIG. 1
(Prior Art)

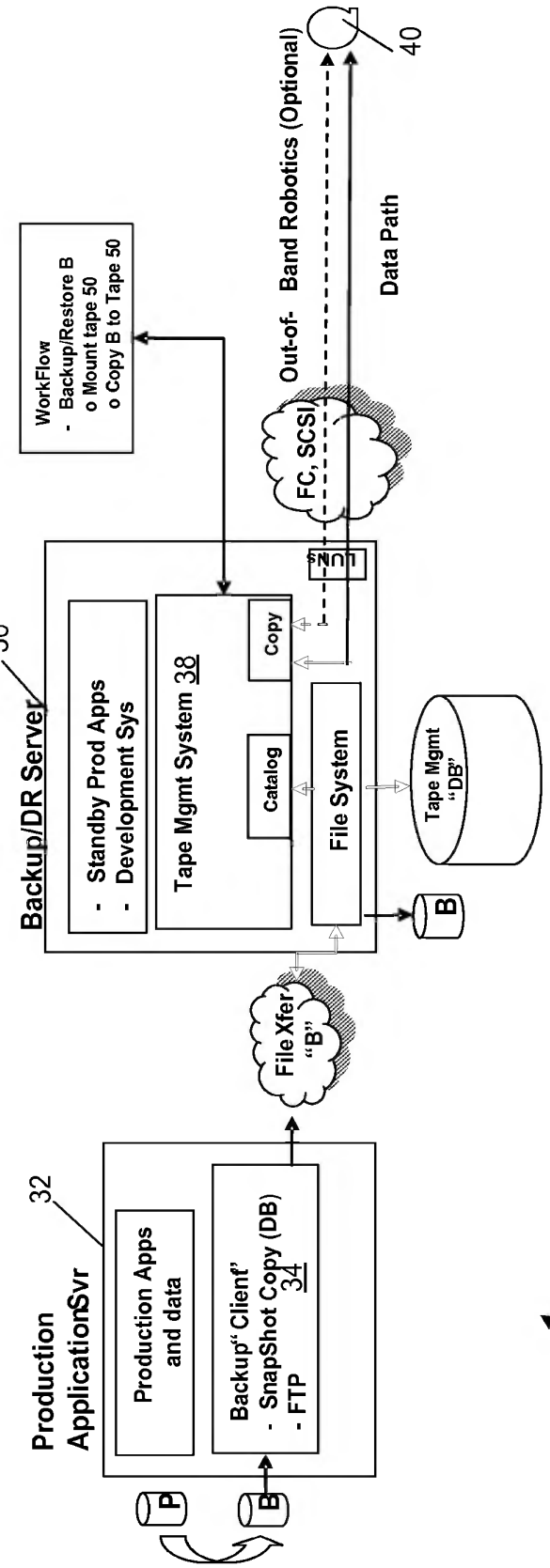


FIG. 2
(Prior Art)

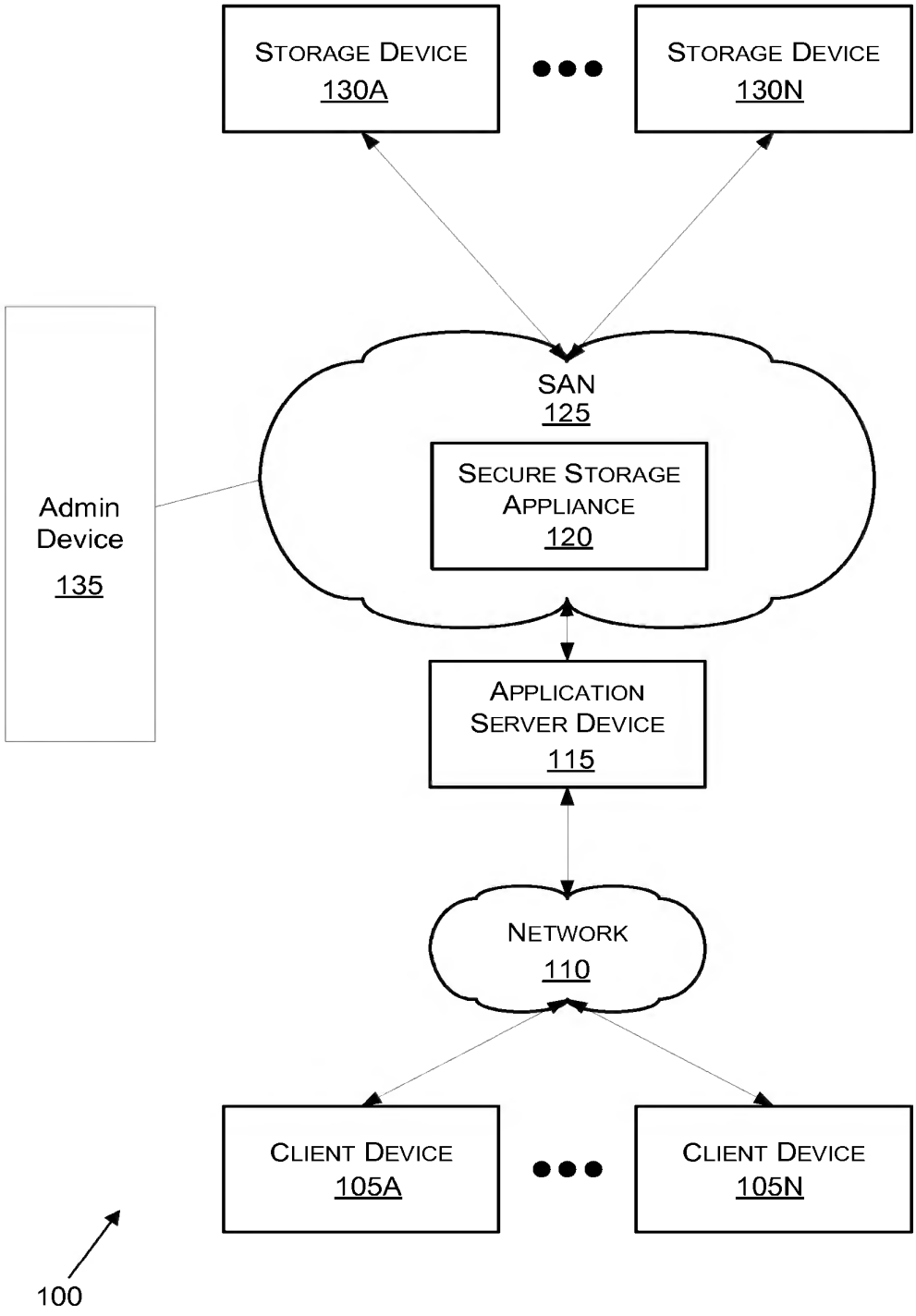

STORAGE DEVICE
130A
STORAGE DEVICE
130N
SAN
125
SECURE STORAGE
APPLIANCE
120
Admin
Device
135
APPLICATION
SERVER DEVICE
115
NETWORK
110
CLIENT DEVICE
105A
CLIENT DEVICE
105N
100

FIG. 3

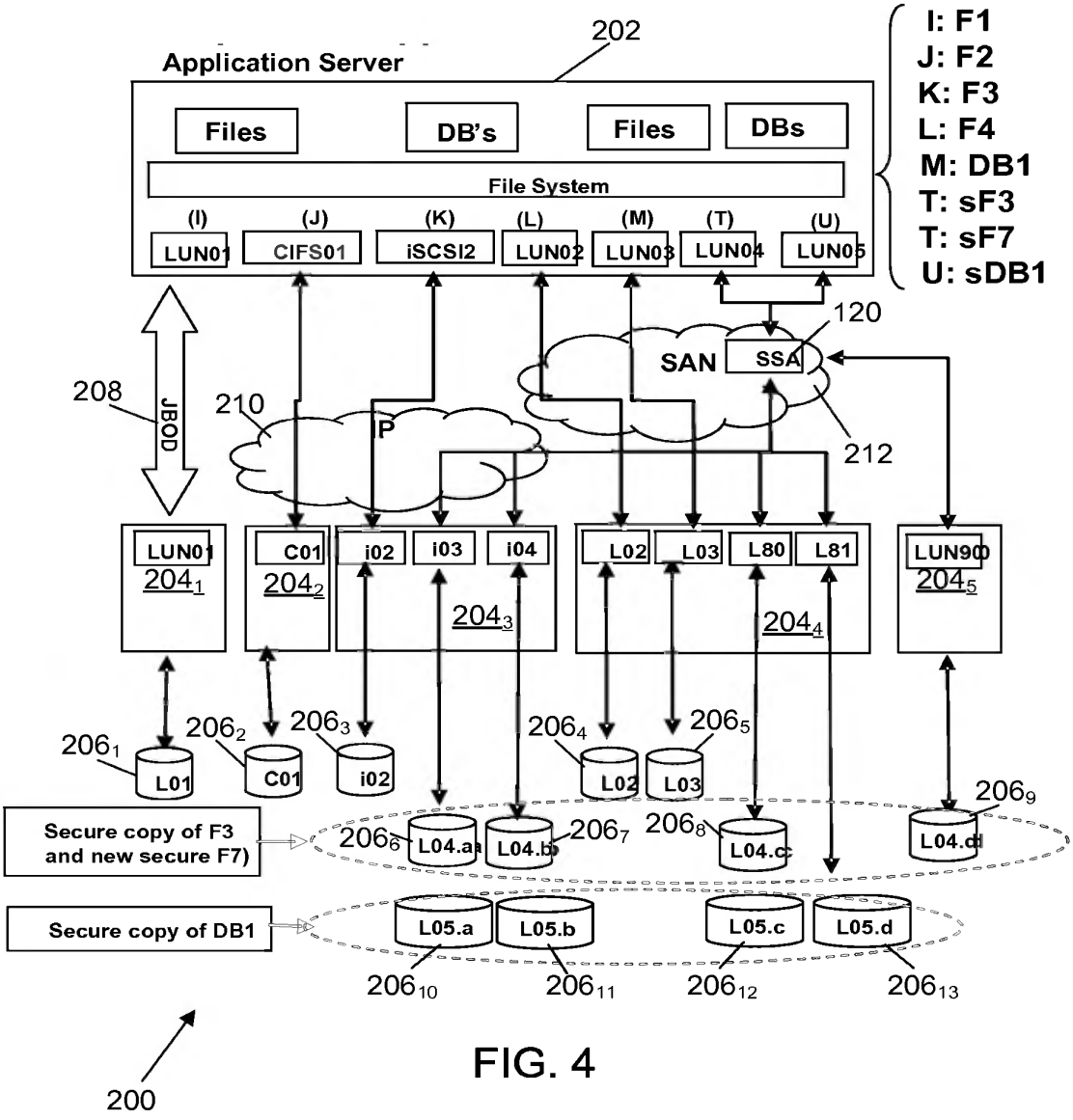

202
Application Server
Files
DB's
Files
DBs
File System
(I)
(J)
(K)
(L)
(M)
(T)
(U)
LUN01
CIFS01
iSCSI2
LUN02
LUN03
LUN04
LUN05
I: F1
J: F2
K: F3
L: F4
M: DB1
T: sF3
T: sF7
U: sDB1
120
SAN
SSA
208
JBOD
210
P
212
LUN01
2041
C01
2042
i02
i03
i04
2043
L02
L03
L80
L81
2044
LUN90
2045
2061
2062
2063
2064
2065
L01
C01
i02
L02
L03
2069
Secure copy of F3
and new secure F7)
2066
L04.a
L04.b
2067
2068
L04.c
L04.d
Secure copy of DB1
L05.a
L05.b
L05.c
L05.d
20610
20611
20612
20613
200

FIG. 4

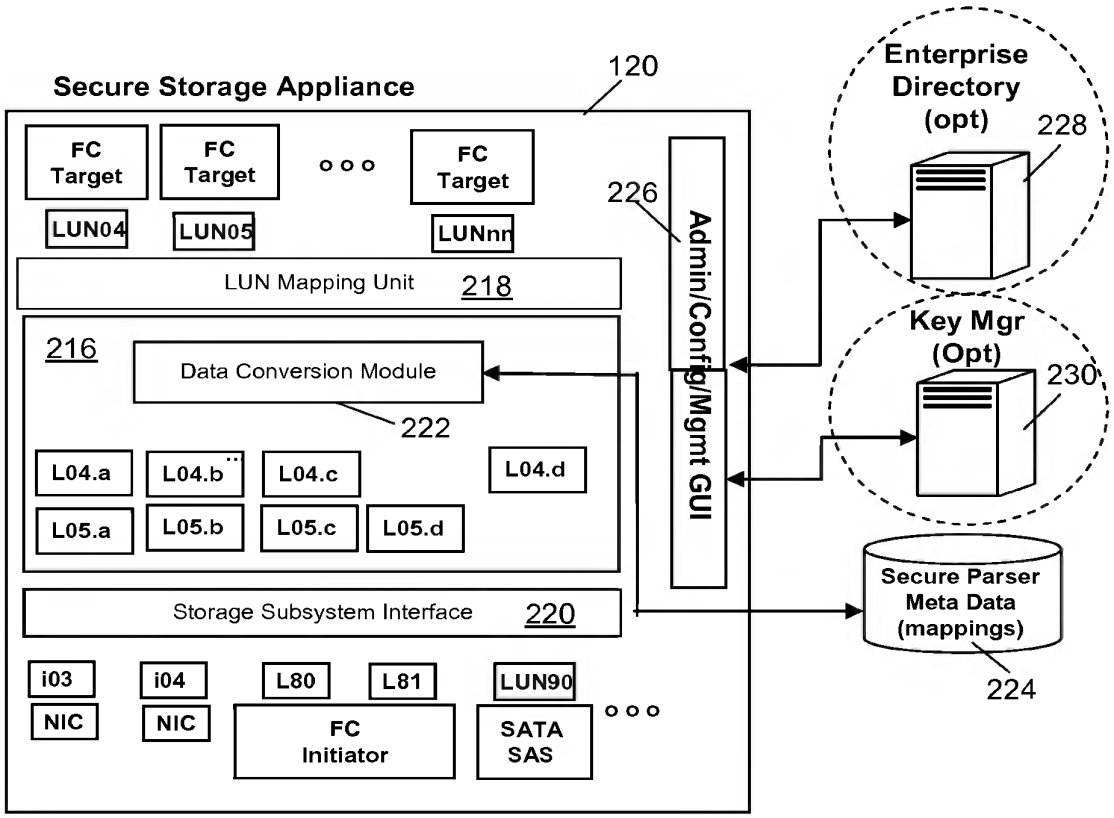

Secure Storage Appliance
120
FC Target
FC Target
FC Target
LUN04
LUN05
LUNnn
LUN Mapping Unit 218
216
Data Conversion Module
222
L04.a
L04.b
L04.c
L04.d
L05.a
L05.b
L05.c
L05.d
Storage Subsystem Interface 220
i03
i04
L80
L81
LUN90
NIC
NIC
FC Initiator
SATA SAS
226
Admin/Config/Mgmt GUI
Enterprise Directory (opt)
228
Key Mgr (Opt)
230
Secure Parser Meta Data (mappings)
224

FIG. 5

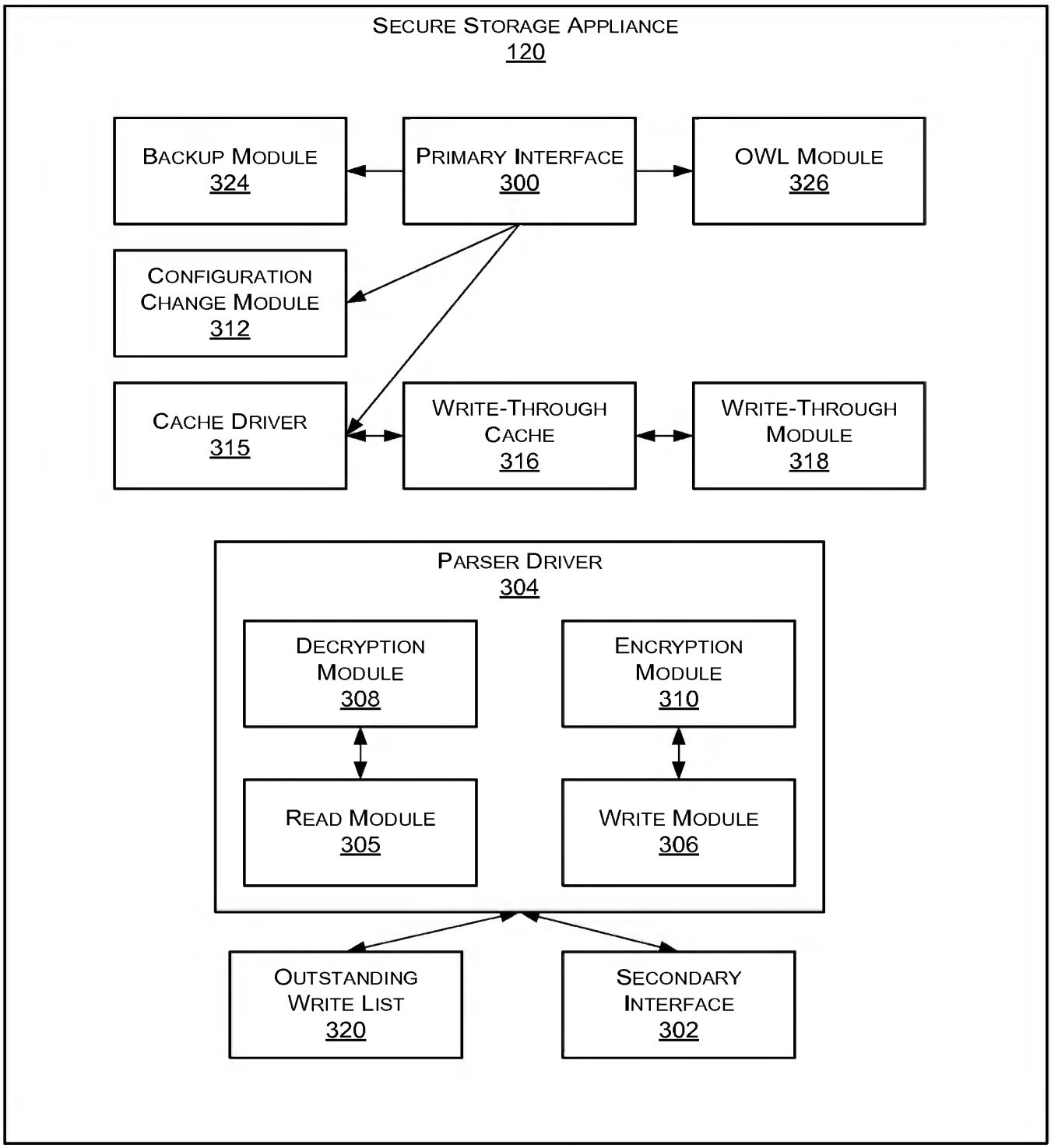

SECURE STORAGE APPLIANCE
120
BACKUP MODULE
324
PRIMARY INTERFACE
300
OWL MODULE
326
CONFIGURATION CHANGE MODULE
312
CACHE DRIVER
315
WRITE-THROUGH CACHE
316
WRITE-THROUGH MODULE
318
PARSER DRIVER
304
DECRYPTION MODULE
308
ENCRYPTION MODULE
310
READ MODULE
305
WRITE MODULE
306
OUTSTANDING WRITE LIST
320
SECONDARY INTERFACE
302

FIG. 6

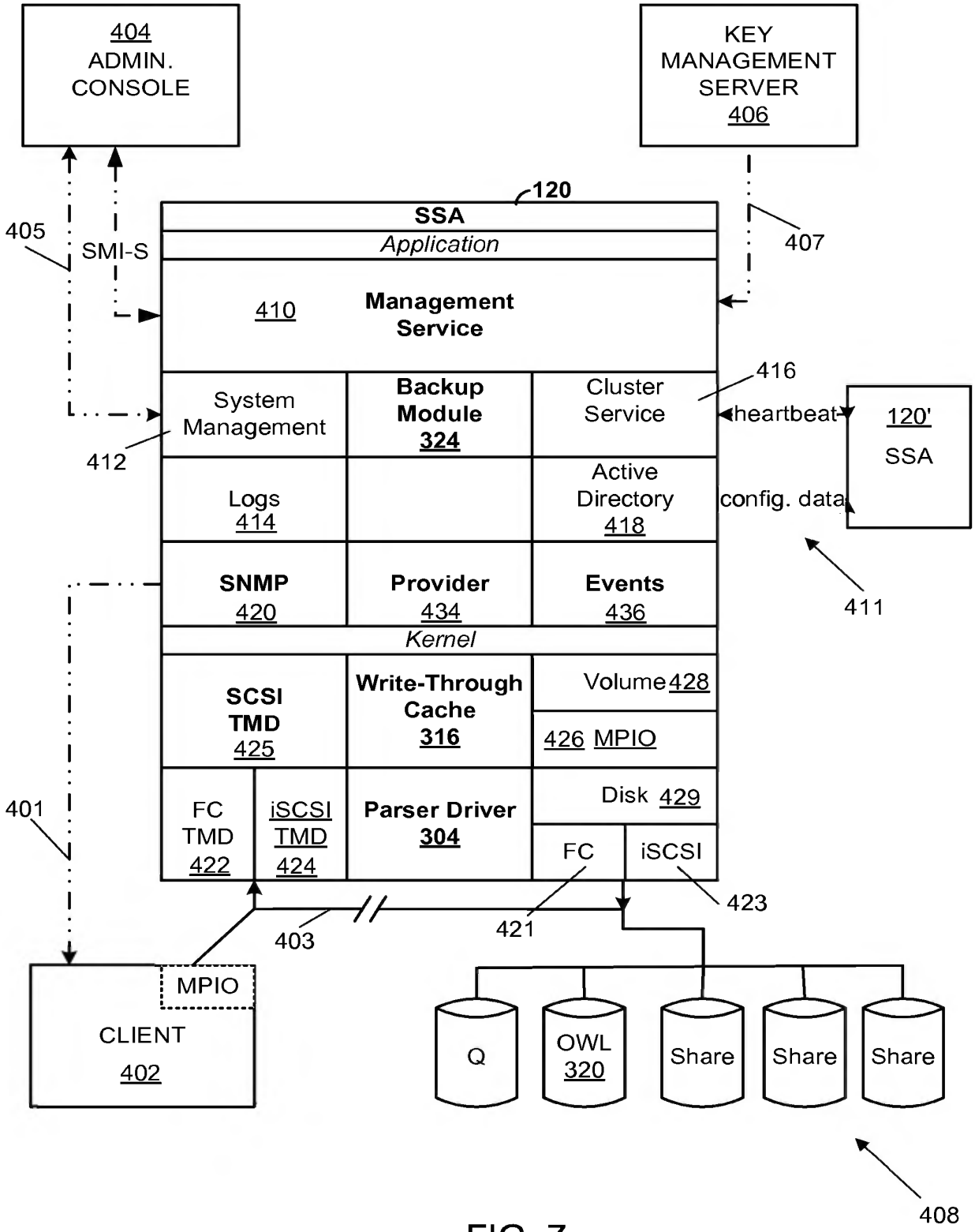

404
ADMIN.
CONSOLE
KEY
MANAGEMENT
SERVER
406
120
SSA
Application
405
SMI-S
407
410
Management
Service
416
System
Management
412
Backup
Module
324
Cluster
Service
heartbeat
120'
SSA
Logs
414
Active
Directory
418
config. data
411
SNMP
420
Provider
434
Events
436
Kernel
SCSI
TMD
425
Write-Through
Cache
316
Volume 428
426 MPIO
401
FC
TMD
422
iSCSI
TMD
424
Parser Driver
304
Disk 429
FC
iSCSI
423
403
421
MPIO
CLIENT
402
Q
OWL
320
Share
Share
Share
408

FIG. 7

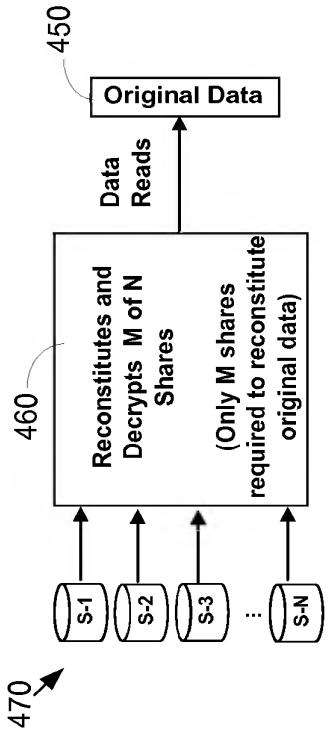

450
Original Data
Data Reads
460
Reconstitutes and Decrypts M of N Shares
(Only M shares required to reconstitute original data)
S-1
S-2
S-3
S-N
470

FIG. 9

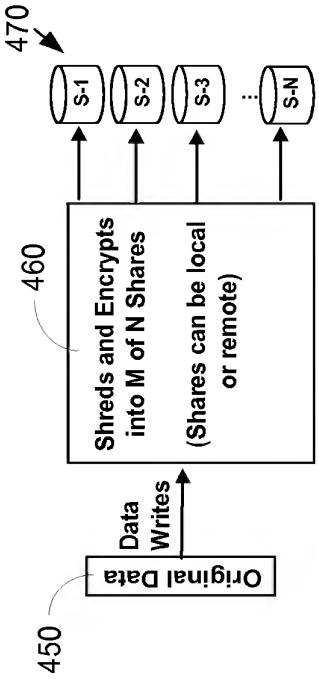

470
S-1
S-2
S-3
S-N
460
Shreds and Encrypts into M of N Shares
(Shares can be local or remote)
Data Writes
Original Data
450

FIG. 8

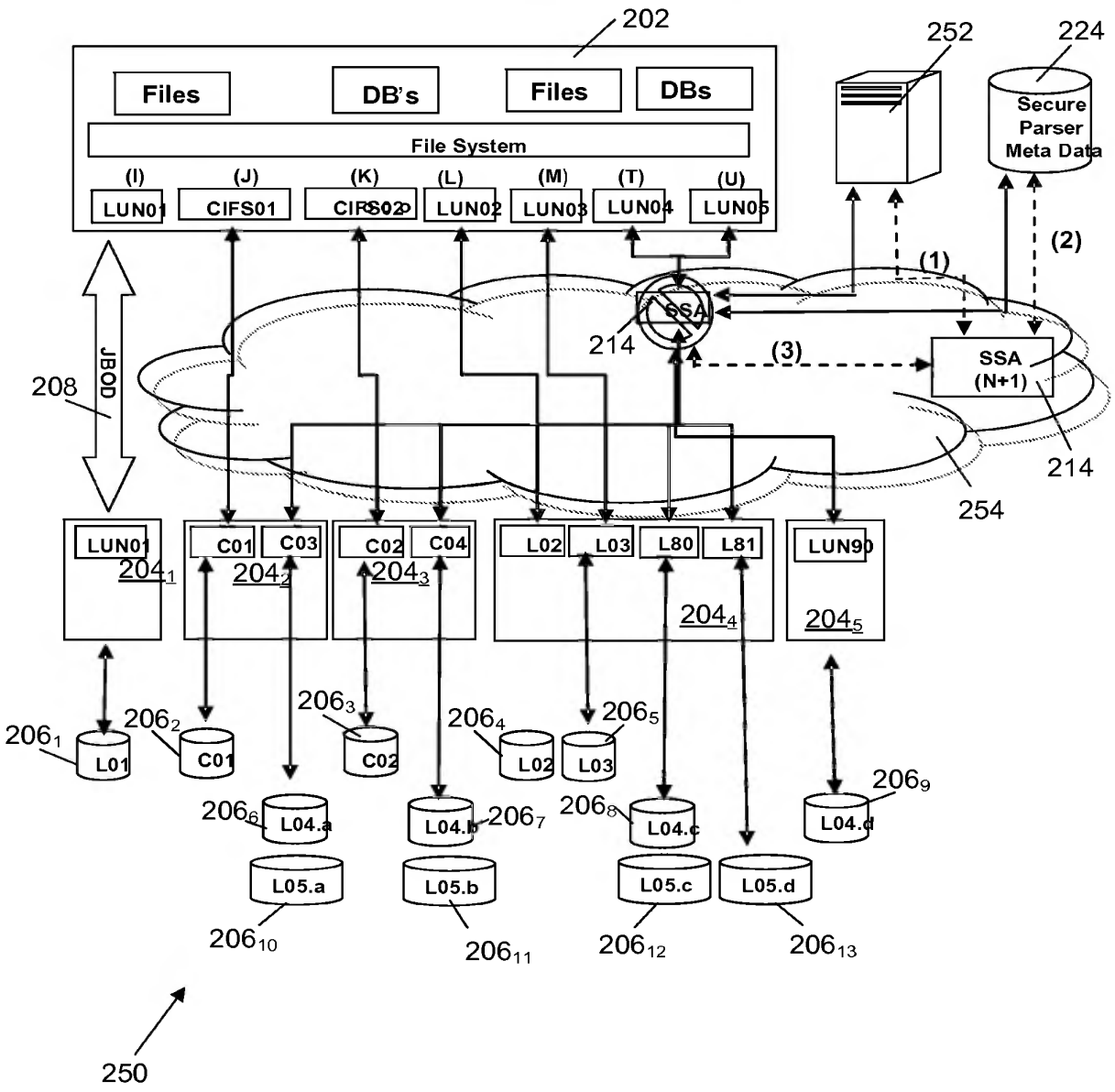

202
Files
DB's
Files
DBs
File System
(I)
(J)
(K)
(L)
(M)
(T)
(U)
LUN01
CIFS01
CIFS02
LUN02
LUN03
LUN04
LUN05
252
224
Secure Parser Meta Data
(1)
(2)
(3)
SSA
214
SSA (N+1)
214
208
JBOD
254
LUN01
C01
C03
C02
C04
L02
L03
L80
L81
LUN90
204_1
204_2
204_3
204_4
204_5
206_1
206_2
206_3
206_4
206_5
206_9
L01
C01
C02
L02
L03
L04.d
206_6
L04.a
L04.b
206_7
206_8
L04.c
L05.a
L05.b
L05.c
L05.d
206_{10}
206_{11}
206_{12}
206_{13}
250

FIG. 10

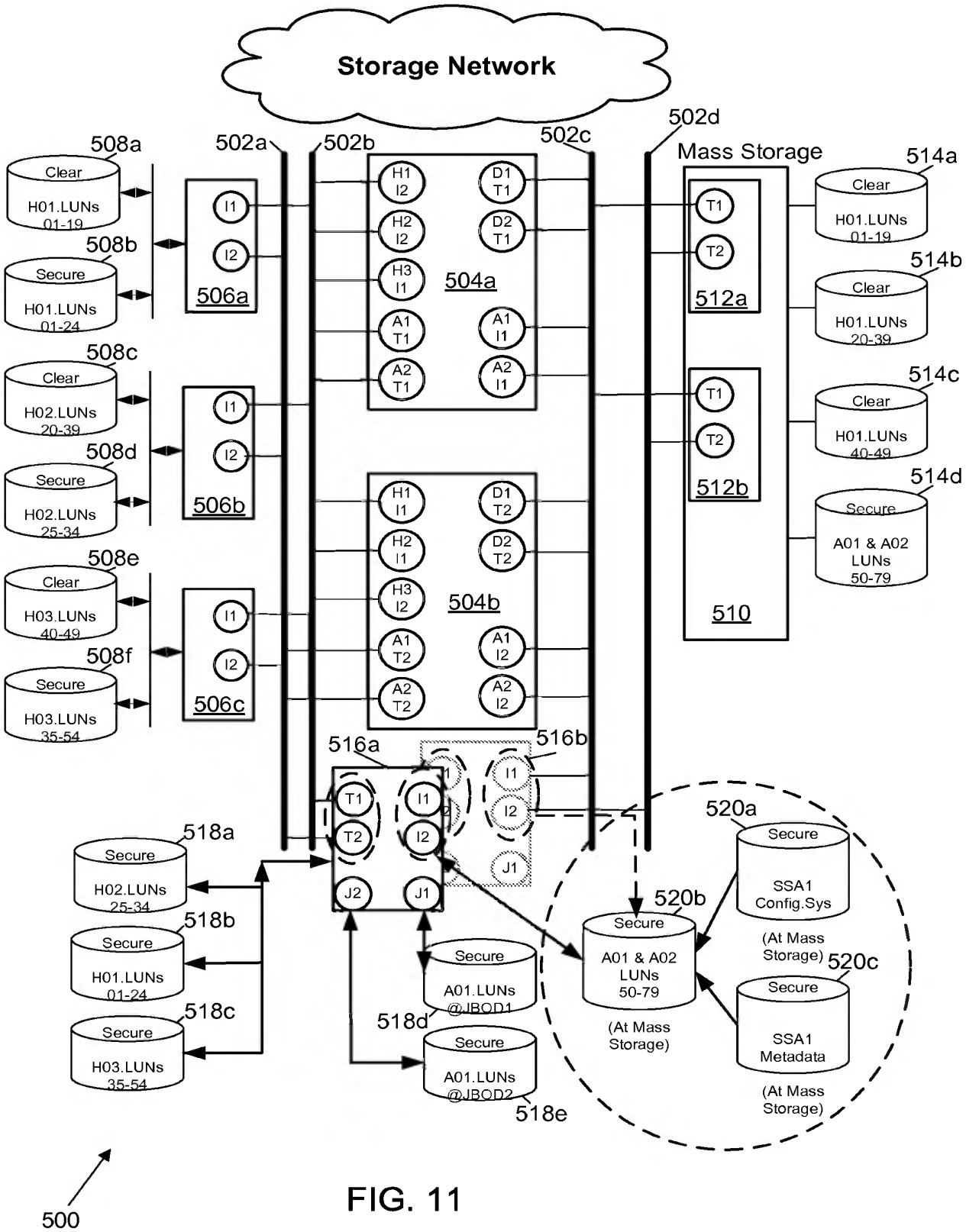

Storage Network
502a
502b
502c
502d
508a
Clear
H01.LUNs 01-19
508b
Secure
H01.LUNs 01-24
508c
Clear
H02.LUNs 20-39
508d
Secure
H02.LUNs 25-34
508e
Clear
H03.LUNs 40-49
508f
Secure
H03.LUNs 35-54
I1
I2
506a
506b
506c
H1 I2
H2 I2
H3 I1
A1 T1
A2 T1
D1 T1
D2 T1
A1 I1
A2 I1
504a
H1 I1
H2 I1
H3 I2
A1 T2
A2 T2
D1 T2
D2 T2
A1 I2
A2 I2
504b
Mass Storage
T1
T2
512a
512b
510
514a
Clear
H01.LUNs 01-19
514b
Clear
H01.LUNs 20-39
514c
Clear
H01.LUNs 40-49
514d
Secure
A01 & A02 LUNs 50-79
516a
516b
J1
J2
518a
Secure
H02.LUNs 25-34
518b
Secure
H01.LUNs 01-24
518c
Secure
H03.LUNs 35-54
518d
Secure
A01.LUNs @JBOD1
518e
Secure
A01.LUNs @JBOD2
520a
Secure
SSA1 Config.Sys
(At Mass Storage)
520b
Secure
A01 & A02 LUNs 50-79
(At Mass Storage)
520c
Secure
SSA1 Metadata
(At Mass Storage)
500

FIG. 11

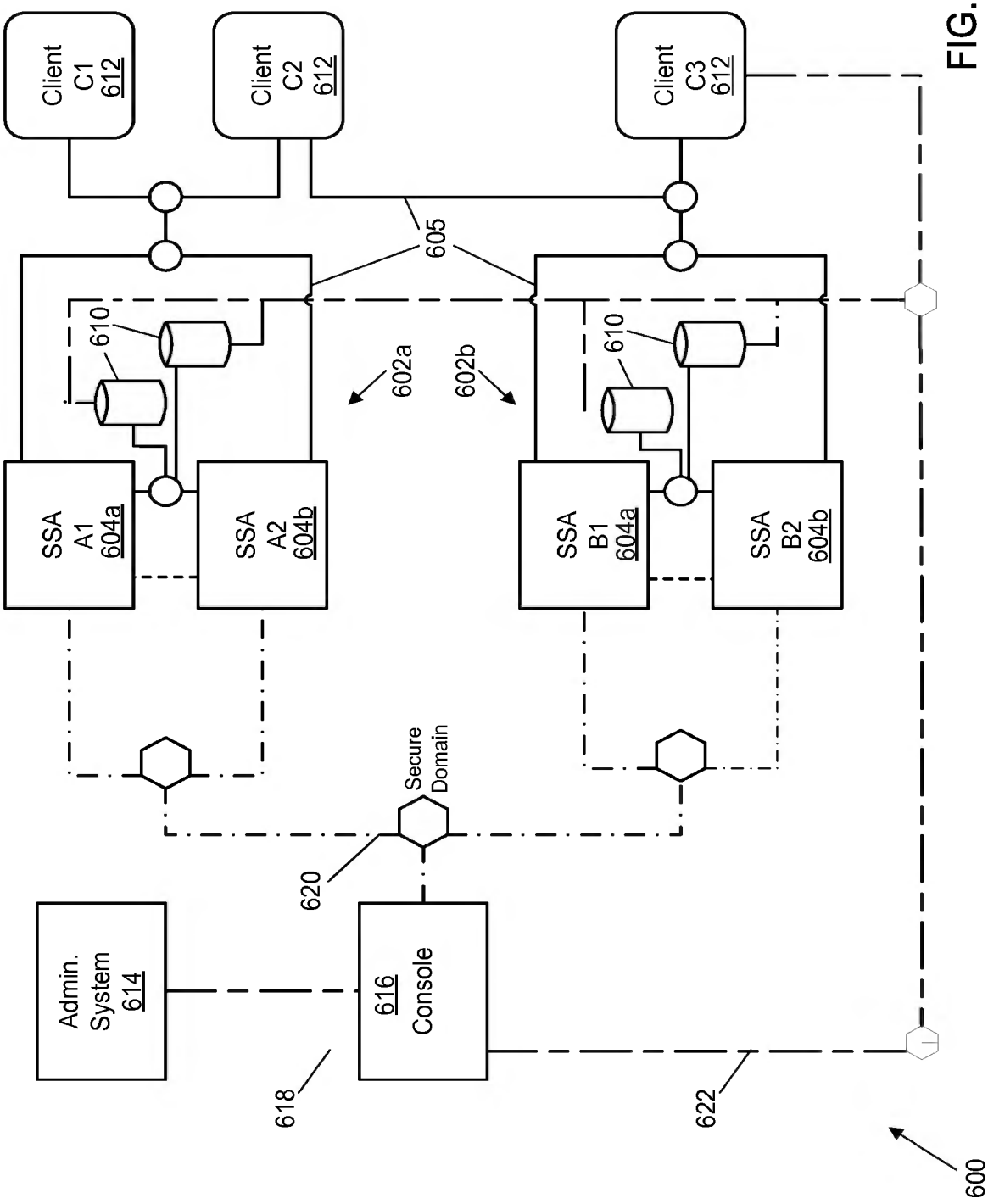

Client C1 612
Client C2 612
Client C3 612
605
610
610
602a
602b
SSA A1 604a
SSA A2 604b
SSA B1 604a
SSA B2 604b
Secure Domain
620
Admin. System 614
616 Console
618
622
600

FIG. 12

11/23

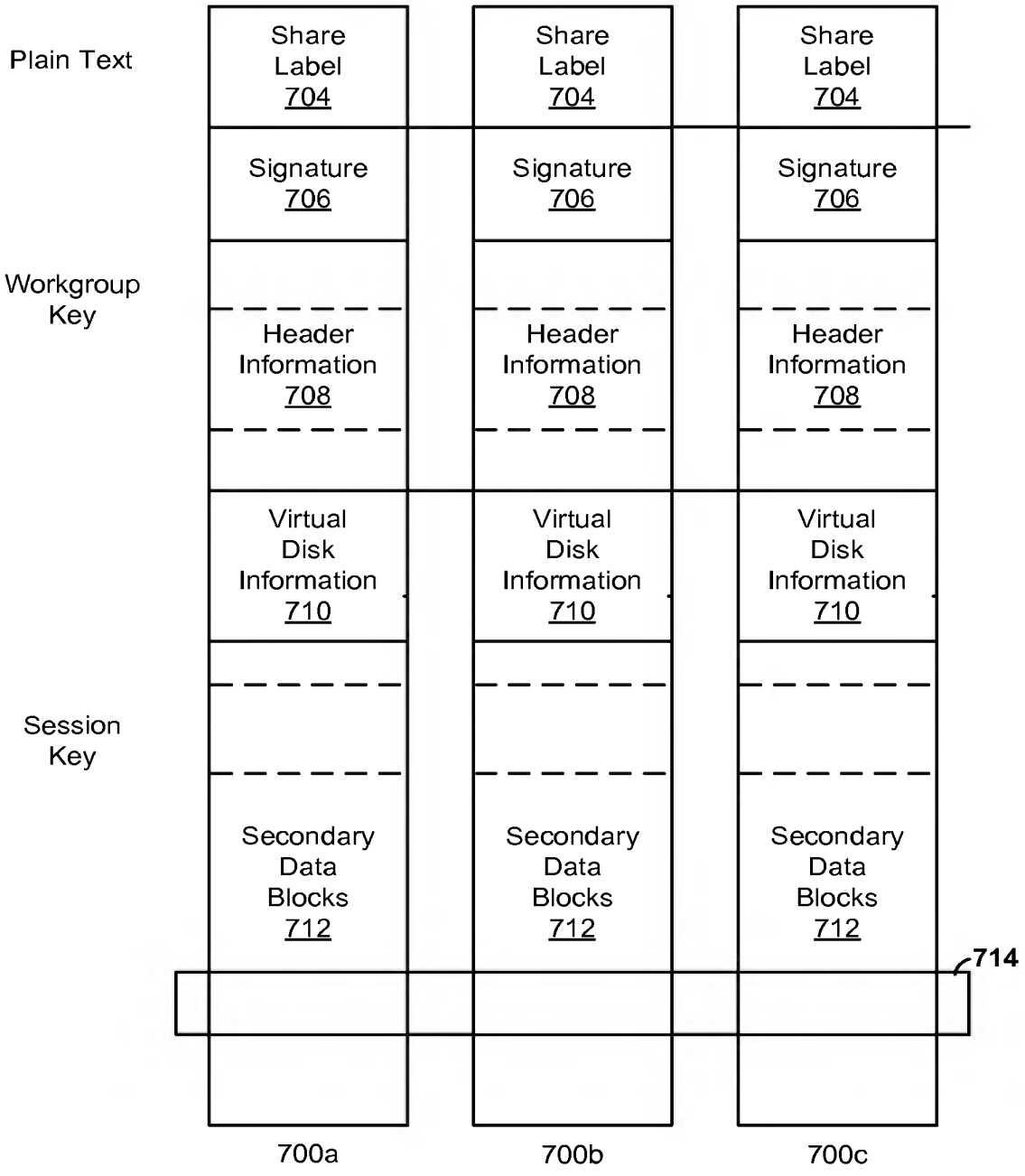

Plain Text
Share Label 704
Signature 706
Workgroup Key
Header Information 708
Virtual Disk Information 710
Session Key
Secondary Data Blocks 712
714
700a
700b
700c

FIG. 13

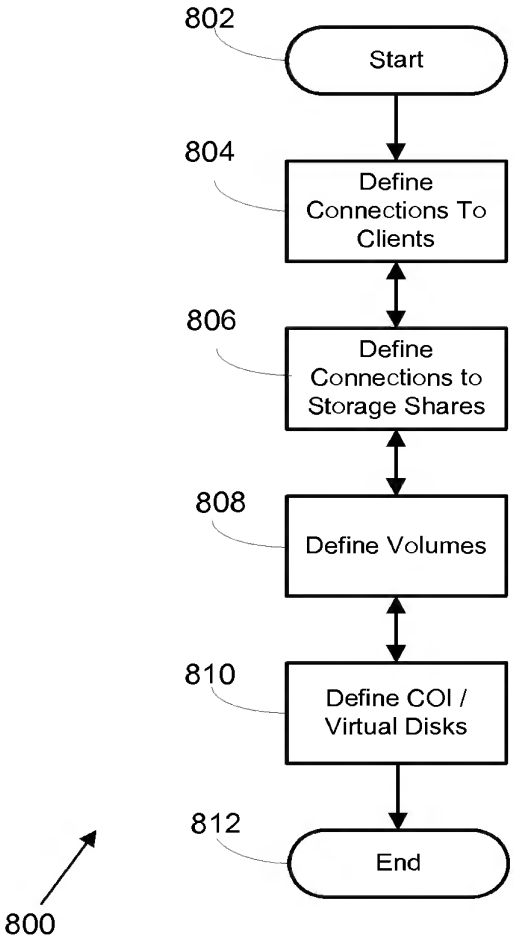

802
Start
804
Define Connections To Clients
806
Define Connections to Storage Shares
808
Define Volumes
810
Define COI / Virtual Disks
812
End
800

FIG. 14

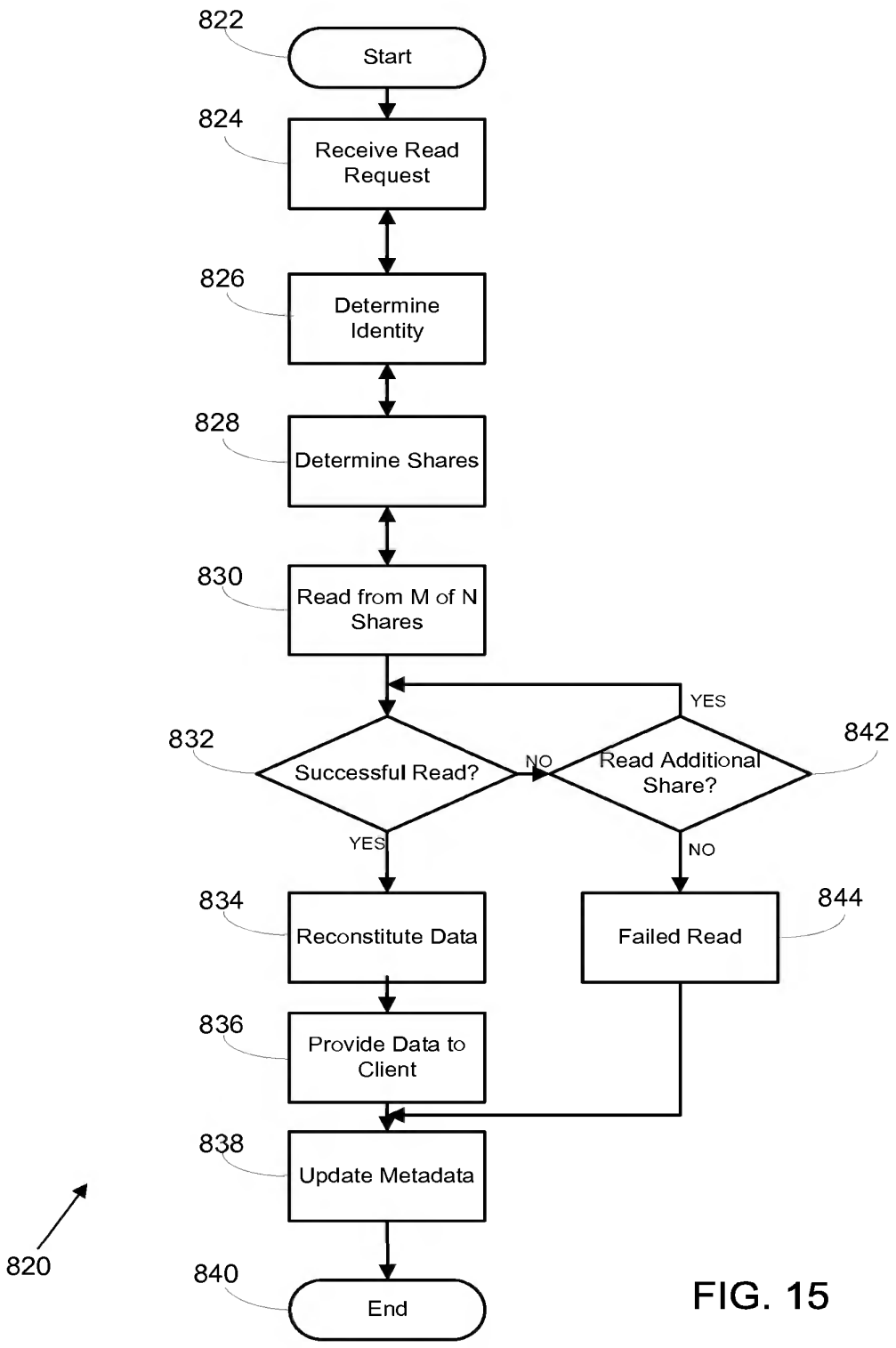

822
Start
824
Receive Read Request
826
Determine Identity
828
Determine Shares
830
Read from M of N Shares
832
Successful Read?
NO
YES
842
Read Additional Share?
YES
NO
834
Reconstitute Data
844
Failed Read
836
Provide Data to Client
838
Update Metadata
840
End
820

FIG. 15

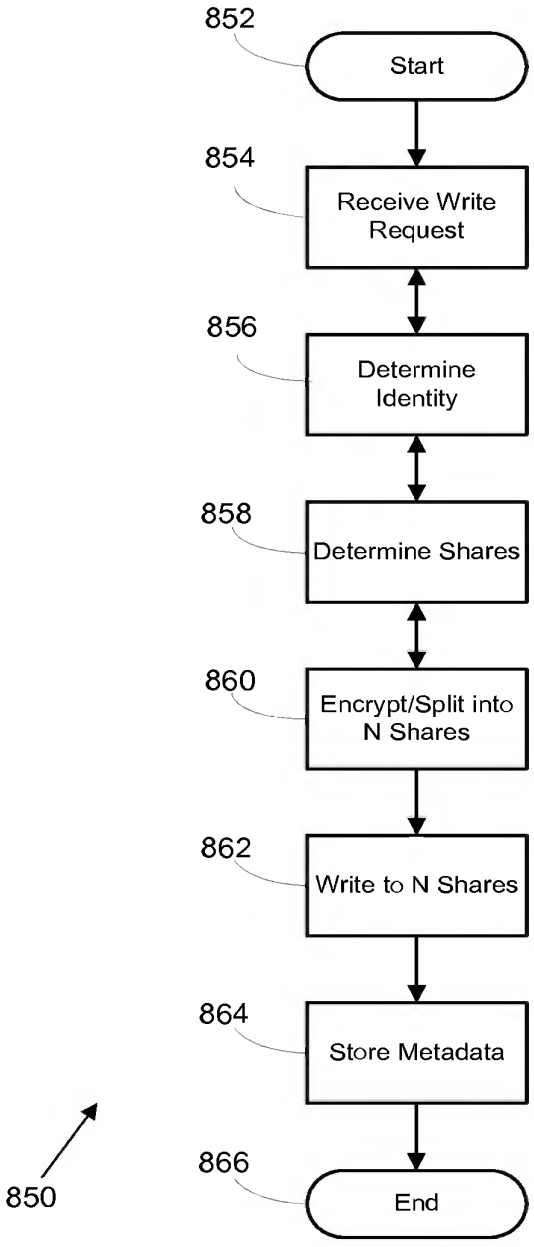

852
Start
854
Receive Write Request
856
Determine Identity
858
Determine Shares
860
Encrypt/Split into N Shares
862
Write to N Shares
864
Store Metadata
866
End
850

FIG. 16

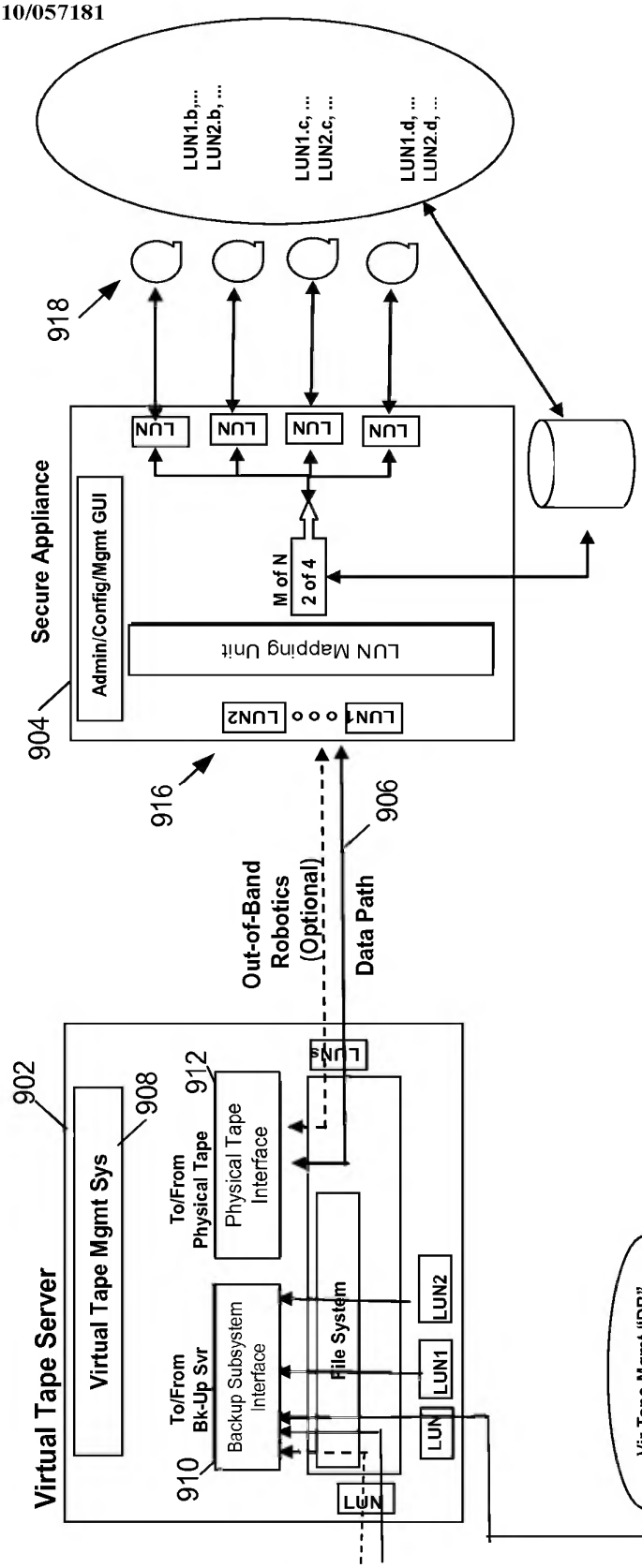

LUN1.b,...
LUN2.b, ...
LUN1.c, ...
LUN2.c, ...
LUN1.d, ...
LUN2.d, ...
918
LUN
LUN
LUN
LUN
Secure Appliance
Admin/Config/Mgmt GUI
M of N
2 of 4
LUN Mapping Unit
LUN1
LUN2
904
916
906
Out-of-Band
Robotics
(Optional)
Data Path
902
Virtual Tape Server
Virtual Tape Mgmt Sys
908
912
To/From
Physical Tape
Physical Tape
Interface
LUNs
To/From
Bk-Up Svr
Backup Subsystem
Interface
File System
LUN2
LUN1
LUN
LUN
910
914
Vir Tape Mgmt "DB"
->Tape 50 VT disk image
->Tape 173 VT disk image
-> 50.VTI on Tape xx
-> 173.VTI on Tape yy
900

FIG. 17

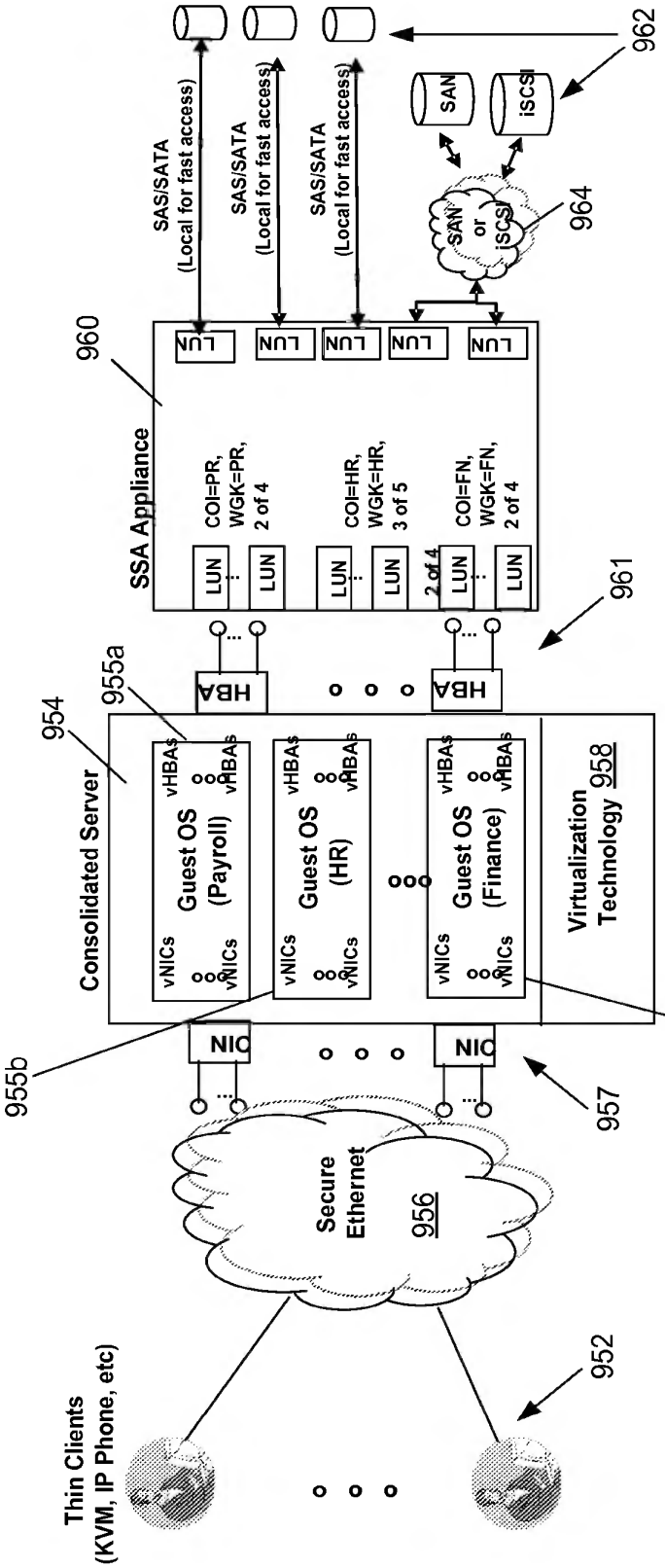

962
SAN
iSCSI
SAS/SATA (Local for fast access)
SAS/SATA (Local for fast access)
SAS/SATA (Local for fast access)
SAN or iSCSI
964
960
LUN
SSA Appliance
COI=PR, WGK=PR, 2 of 4
COI=HR, WGK=HR, 3 of 5
COI=FN, WGK=FN, 2 of 4
961
HBA
955a
954
Consolidated Server
vHBAs
Guest OS (Payroll)
Guest OS (HR)
Guest OS (Finance)
vNICs
Virtualization Technology 958
955b
955c
NIC
957
Secure Ethernet 956
950
952
Thin Clients (KVM, IP Phone, etc)

FIG. 18

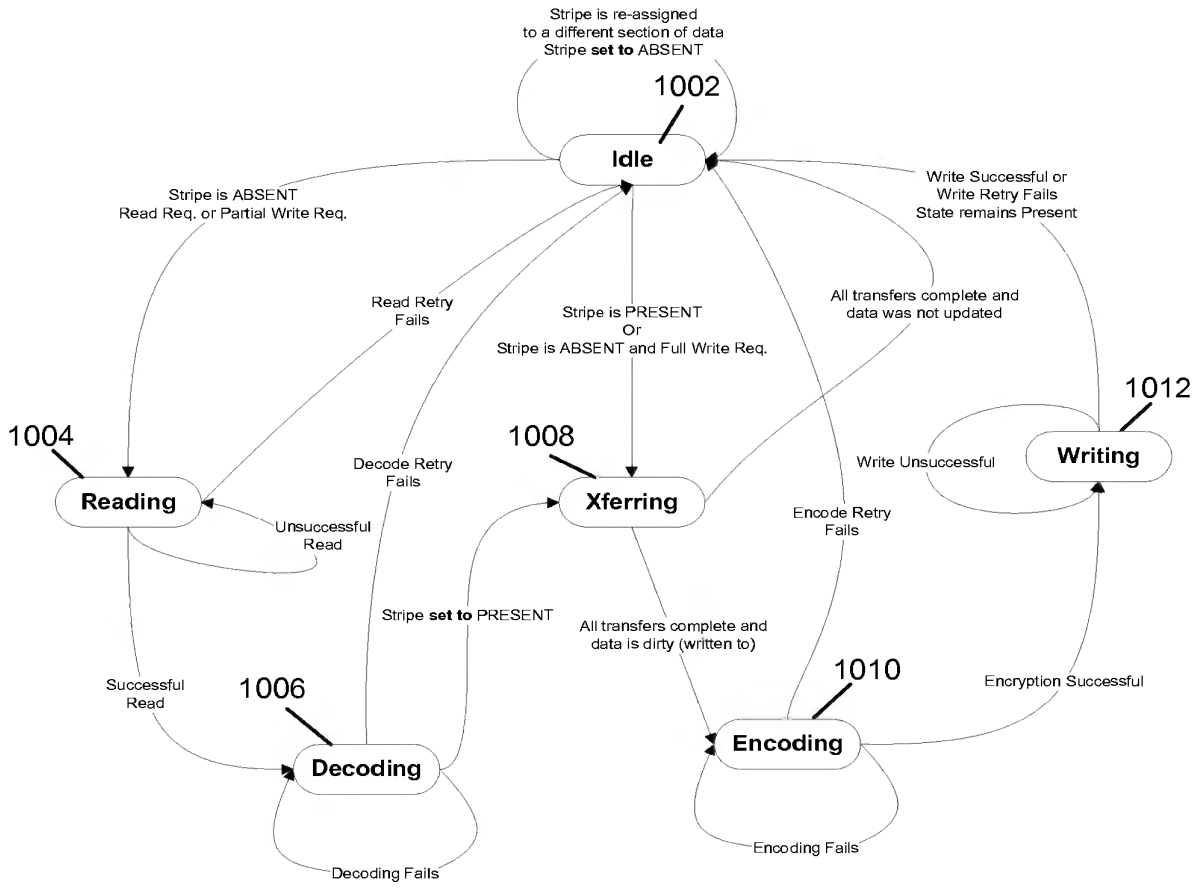

Stripe is re-assigned
to a different section of data
Stripe set to ABSENT
1002
Idle
Stripe is ABSENT
Read Req. or Partial Write Req.
Write Successful or
Write Retry Fails
State remains Present
Read Retry
Fails
Stripe is PRESENT
Or
Stripe is ABSENT and Full Write Req.
All transfers complete and
data was not updated
1012
1004
1008
Reading
Xferring
Writing
Decode Retry
Fails
Write Unsuccessful
Unsuccessful
Read
Encode Retry
Fails
Stripe set to PRESENT
All transfers complete and
data is dirty (written to)
1010
Successful
Read
1006
Encryption Successful
Decoding
Encoding
Decoding Fails
Encoding Fails
1000

FIG. 19

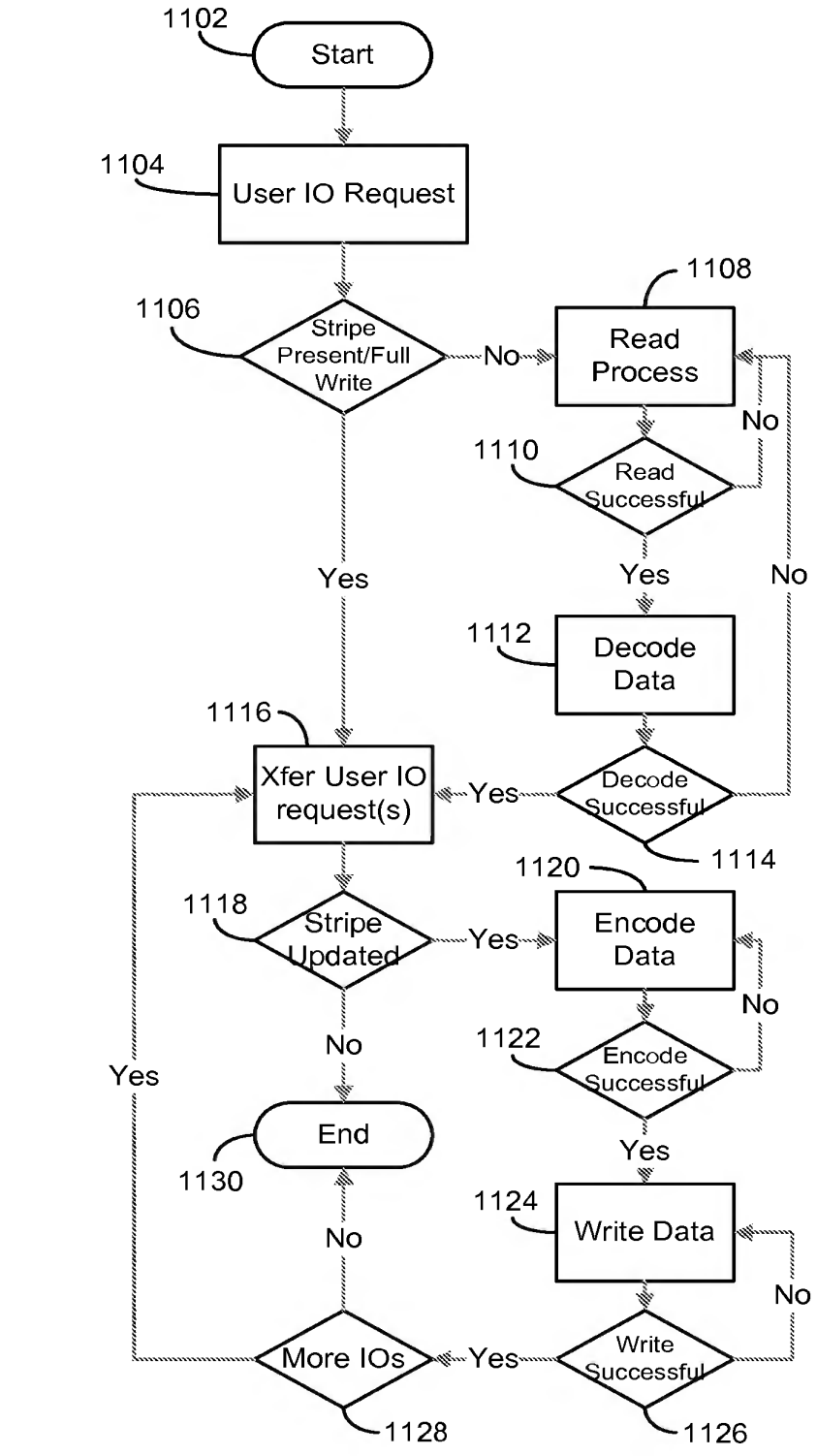

1102
Start
1104
User IO Request
1106
Stripe Present/Full Write
No
1108
Read Process
No
1110
Read Successful
Yes
No
Yes
1112
Decode Data
1116
Xfer User IO request(s)
Yes
Decode Successful
1114
1120
1118
Stripe Updated
Yes
Encode Data
No
1122
Encode Successful
No
Yes
Yes
End
1130
1124
Write Data
No
No
More IOs
Yes
Write Successful
1128
1126
1100

FIG. 20

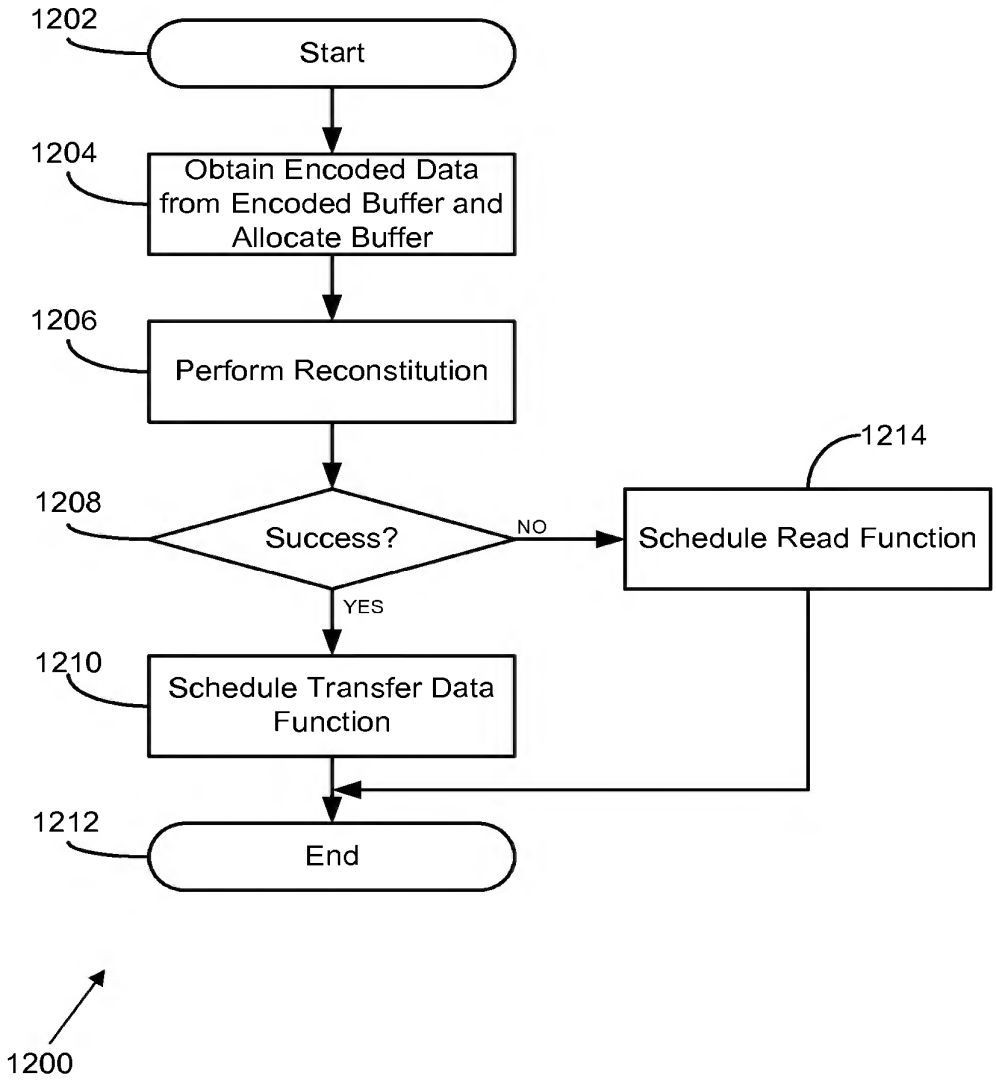

1202
Start
1204
Obtain Encoded Data from Encoded Buffer and Allocate Buffer
1206
Perform Reconstitution
1208
Success?
NO
1214
Schedule Read Function
YES
1210
Schedule Transfer Data Function
1212
End
1200

FIG. 21

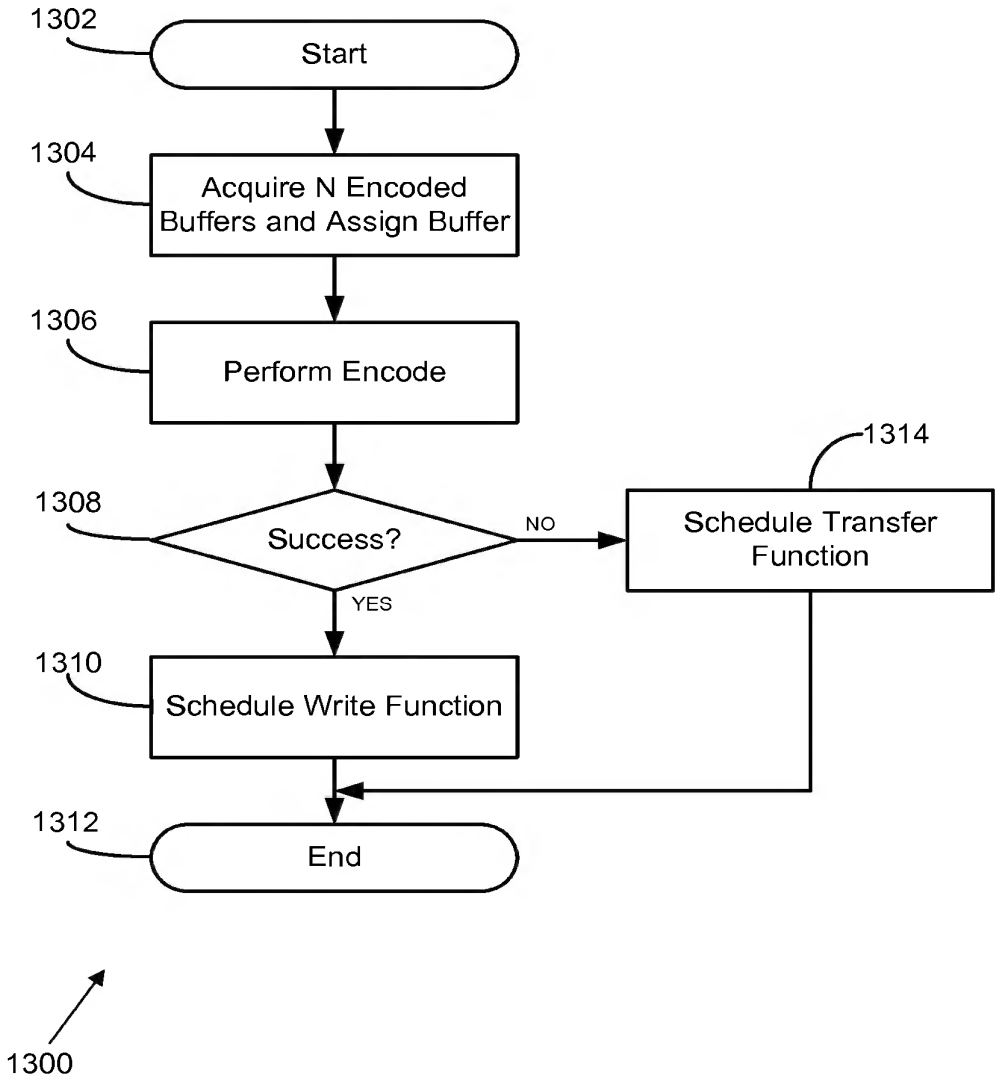

1302
Start
1304
Acquire N Encoded Buffers and Assign Buffer
1306
Perform Encode
1308
Success?
NO
YES
1314
Schedule Transfer Function
1310
Schedule Write Function
1312
End
1300

FIG. 22

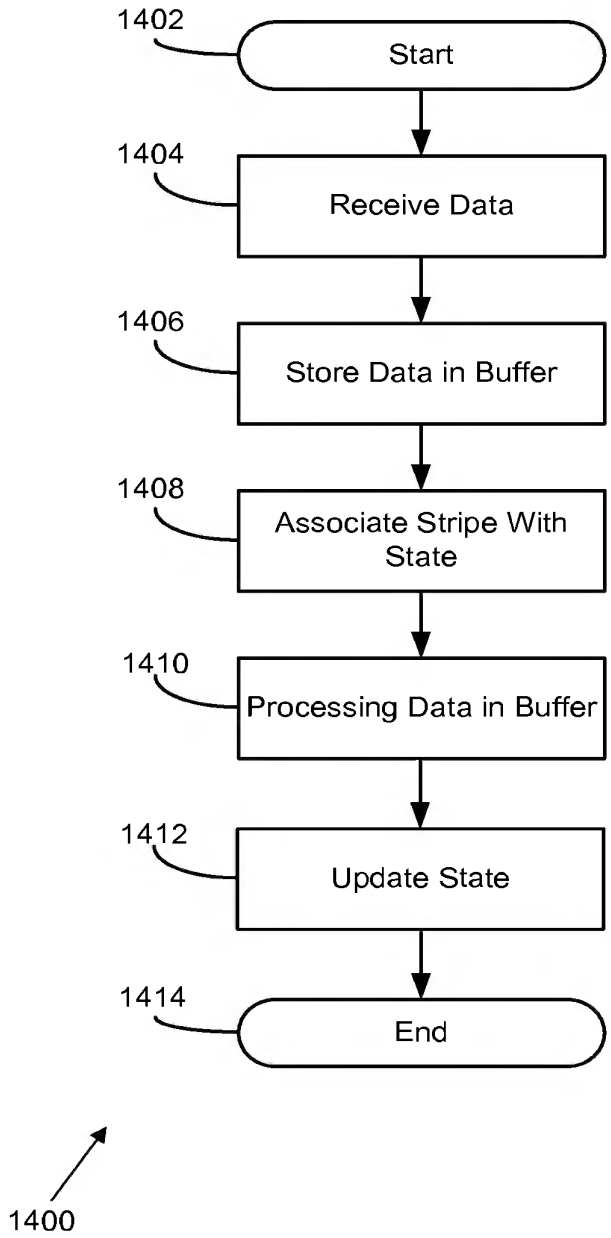

1402
Start
1404
Receive Data
1406
Store Data in Buffer
1408
Associate Stripe With State
1410
Processing Data in Buffer
1412
Update State
1414
End
1400

FIG. 23

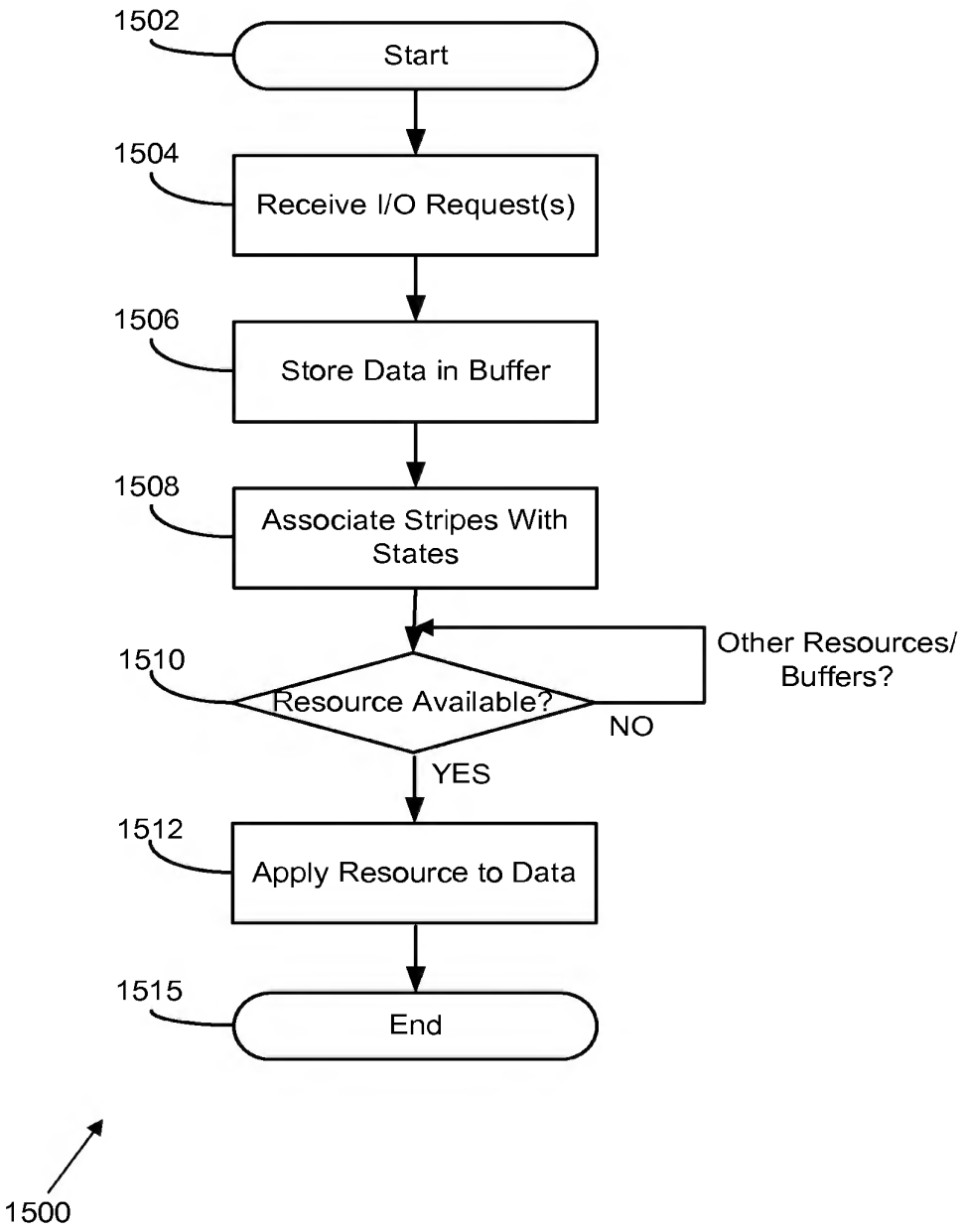

1502
Start
1504
Receive I/O Request(s)
1506
Store Data in Buffer
1508
Associate Stripes With States
1510
Resource Available?
Other Resources/ Buffers?
NO
YES
1512
Apply Resource to Data
1515
End
1500

FIG. 24

Electronic Patent Application Fee Transmittal

Application Number:	13371363
Filing Date:	10-Feb-2012
Title of Invention:	SECURE DATA PARSER METHOD AND SYSTEM
First Named Inventor/Applicant Name:	Rick L. Orsini
Filer:	Matthew Sammuel Bertenthal/Joanne Ryan
Attorney Docket Number:	104093-0002-105

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

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

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Docket No.: 104093-0002-105
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Orsini et al.

Application No.: 13/371,363 | Confirmation No.: 7984

Filed: February 10, 2012 | Art Unit: 2492

For: SECURE DATA PARSER METHOD AND SYSTEM | Examiner: M.W. Chao

RESPONSE TO NON-FINAL OFFICE ACTION

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

Dear Madam:

INTRODUCTORY COMMENTS

In response to the Office Action dated May 14, 2012, please amend the above-identified U.S. Patent application as follows.

Amendments to the Specification are reflected on page 2 of this reply.

Remarks/Arguments begin on page 3 of this reply.

31053937_1

Docket No.: 104093-0002-105
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Orsini et al.

Application No.: 13/371,363 | Confirmation No.: 7984

Filed: February 10, 2012 | Art Unit: 2492

For: SECURE DATA PARSER METHOD AND SYSTEM | Examiner: M. W. Chao

INFORMATION DISCLOSURE STATEMENT (IDS)

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

Dear Madam:

Pursuant to 37 CFR 1.56, 1.97 and 1.98, the attention of the Patent and Trademark Office is hereby directed to the references listed on the attached PTO/SB/08. It is respectfully requested that the information be expressly considered during the prosecution of this application, and that the references be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Information Disclosure Statement is filed more than three months after the U.S. filing date, OR more than three months after the date of entry of the national stage of a PCT application, AND after the mailing date of the first Office Action on the merits, whichever occurs first, but before the mailing date of any of a Final Office Action, a Notice of Allowance (37 CFR 1.97(c)) or an action that otherwise closes prosecution in the application.

31155279_1

In accordance with 37 CFR 1.98(a)(2)(ii), Applicants have not submitted copies of U.S. patents and U.S. patent applications. Applicants submit herewith copies of non-patent literature in accordance with 37 CFR 1.98(a)(2).

In accordance with 37 CFR 1.97(g), the filing of this Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 CFR 1.56(a) exists. In accordance with 37 CFR 1.97(h), the filing of this Information Disclosure Statement shall not be construed to be an admission that any patent, publication or other information referred to therein is "prior art" for this invention unless specifically designated as such.

Notice of Related Patent Applications

The Examiner is advised that the following patent applications contain subject matter that may be related to the pending claims in the present application. In particular, applicants would like to draw the Examiner's attention to the fact that substantive examination may have occurred in these cases. For these cases, copies of any Office Actions that have issued and Replies that have been filed in these cases are submitted herewith. For Application No. 12/148,365, only a copy of the final Office Action, Appeal Brief, and subsequent non-final Office Action are submitted herewith, as the claims in the application have been rejected with the same references throughout prosecution. Applicants invite the Examiner to review these documents or any future substantive documents that will issue or be filed in any of the below cases. By bringing the following applications to the Examiner's attention, applicants do not waive any applicable confidentiality provisions of 35 U.S.C. 122.

Application No.	**Publication No.**	**Attorney Docket No.**	**Filing Date**	**Status**
12/148,365	US 2008-0244277	104093-0001-102	4/18/2008	Pending
13/024,791	US 2011-0179287	104093-0001-103	2/10/2011	Pending
13/024,804	US 2011-0179271	104093-0001-104	2/10/2011	Pending
13/399,923	Not published	104093-0001-105	2/17/2012	Pending

13/371,361	Not published	104093-0002-104	2/10/2012	Pending
13/371,364	Not published	104093-0002-106	2/10/2012	Pending

It is submitted that the Information Disclosure Statement is in compliance with 37 CFR 1.98 and the Examiner is respectfully requested to consider the listed references.

Please charge our Deposit Account No. 06-1075 in the amount of $180.00 covering the fee set forth in 37 CFR 1.17(p). 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, under Order No. 104093-0002-105.

Dated: June 29, 2012

Respectfully submitted,

Electronic signature: /Matthew S. Bertenthal/
Matthew Samuel Bertenthal
Registration No.: 61,129
ROPES & GRAY LLP
1900 University Avenue
6th Floor
Palo Alto, California 94303-2284
(650) 617-4000
(617) 235-9492 (Fax)
Attorneys/Agents For Applicant

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 August 2002 (08.08.2002)

PCT

(10) International Publication Number
WO 02/062032 A2

(51) International Patent Classification[7]: H04L 29/00

(21) International Application Number: PCT/US01/50069

(22) International Filing Date:
21 December 2001 (21.12.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/258,127 22 December 2000 (22.12.2000) US

(71) Applicant: **THE CHARLES STARK DRAPER LABORATORY, INC.** [US/US]; 555 Technology Square, Cambridge, MA 02139 (US).

(72) Inventors: **SHU, Li**; 20 Acre Road, Billerica, MA 01821 (US). **POPPE, Dorothy, C.**; 169 Sheridan Avenue #2, Medford, MA 02155 (US).

(74) Agent: **ROSE, Jamie, H.**; Testa, Hurwitz & Thibeault, LLP, High Street Tower, 125 High Street, Boston, MA 02110 (US).

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

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

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

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

WO 02/062032 A2

(54) Title: METHOD AND SYSTEM FOR SECURE EXCHANGE OF MESSAGES

(57) Abstract: The invention features an apparatus and method for transmitting a file. The apparatus includes a file splitter that splits the file into a plurality of message segments. Each message segment includes an address of the destination. The apparatus also includes a file encapsulator. The file encapsulator encapsulates at least one of the plurality of message segments. The encapsulation conceals the address of the destination during transmission of the at least one encapsulated message segment to one or more trusted nodes. The trusted nodes retransmit the message segments to the destination for reassembly of the file at the destination.

METHOD AND SYSTEM FOR SECURE EXCHANGE OF MESSAGES

Cross-Reference to Related Case

This claims the benefit of and priority to U.S. Provisional Patent Application Serial No. 60/258,127, filed December 22, 2000, the entirety of which is incorporated herein by reference.

Technical Field

The invention generally relates to electronic communications, and, more particularly, to security in network-based communications.

Background Information

Message security is of particular concern in modern, network-based communications. Communications often occur between devices such as computers operating in a non-secure network, such as the Internet. It is generally desirable to protect communications from eavesdropping and tampering.

Generally, three approaches have been used to provide secure communications: a secure network; a secure host with security protocols; and encryption of communications. A secure network typically requires steps be taken to protect the network from intruders. Such steps can include special communications protocols or special hardware, for example, use of a secure, optical network backbone. In such cases, secure communications, if at all possible, are limited to the confines of the secure network.

The secure host approach includes installation of a security protocol on network host computers to monitor network communications. The protocol provides review and control of

network communications to guard against theft and tampering. This approach requires the host computers to implement a security protocol that operates at Layer 3 or 4 of the Open Systems Interconnection (OSI) model.

A variety of encryption devices or software tools can protect data communications from theft and tampering. For example, keyed encryption techniques are common. Such techniques typically require that a sender and a recipient of a message share some information regarding an encryption algorithm and encryption/decryption key to enable the recipient to de-encrypt a message.

Message packet headers are particularly vulnerable to tampering because the packet header typically cannot be encrypted. Variants of the above general schemes have been proposed to respond to this problem. Further, message packets can be modified to enable detection of tampering and hence the potential of an altered message packet. Alternatively, a message can be disguised to appear as an ordinary message to fool an eavesdropper. The ordinary appearing message would have a distinct meaning to a recipient based on prior agreement between the sender and the recipient.

The above described approaches to message security are ineffective when a secure network or encryption methods are unavailable or not desired.

Summary of the Invention

The invention generally involves secure data transmission over a network. The invention is particularly suited to message transmission over a network that has multiple pathways. Various embodiments of the invention can defeat eavesdroppers wishing to intercept or interfere with a message. A solution is provided for the problem of the publicly visible addresses that are typically associated with transmitted communications.

The invention is suited to protect various types of communications. The communications may be digital electronic communications and may include, for example, messages and data. The communications may be sent via a network in the form of packets. The network may be, for example, a wired, wireless or optical network. In the following discussion, the terms "communication", "message", "file" and "data" are all used to express the general idea of information transmitted between parties. The particular form that the information assumes during transmission may be binary, as found in modern digital communications.

Improved security is accomplished by use of one or more trusted intermediaries, i.e. nodes, to relay communications between parties, for example, a source and a destination. The ultimate destination of the communication is generally concealed from all but the intermediary. Thus, an intermediary receives a message or other communication from a source, examines the concealed address of the destination and forwards the communication to the destination.

When the intermediary forwards a communication, the source can be concealed while the destination address of the next trusted intermediary, which may be the final destination of the

packet, is now publicly observable. In this manner, an eavesdropper cannot simultaneously discern the source and destination of a communication.

An eavesdropper attempting to intercept a message sent between two parties must therefore overcome multiple difficulties. If an eavesdropper observes transmissions such as data packets leaving a source, it cannot correctly identify the ultimate or real destination of each data packet. If the eavesdropper observes data packets arriving at a destination, it cannot correctly identify the original source of each packet. Thus, an eavesdropper may be impeded from identifying messages sent from a particular original source to a particular final destination.

An intermediary can perform the same function for two-way or multi-party communications. The node can be, for example, a network node. The node can be a computer server or a radio transceiver (e.g. a mobile telephone).

Splitting the message into message segments can make message interception and tampering more difficult. An eavesdropper must then intercept multiple segments to obtain the message, and still will not know the source or the destination. To further complicate interception, the ultimate destination addresses of the segments can be concealed when the segments are transmitted to one or more trusted nodes. An eavesdropper seeking messages or segments addressed to a particular destination may then only perceive the message segments as being addressed to the intermediary, and thus fail to intercept them.

Moreover, increasing the number of pathways used for transmission of message segments or data packets provides additional security. An eavesdropper must then monitor and intercept communications along multiple pathways to attempt to obtain all the message segments required for reconstruction of a

message. Message segments can be encrypted to impede an eavesdropper still further.

Accordingly, in a first aspect, the invention features an apparatus for transmitting a file. The file can include data or a message, or both. It can be in binary form, as for a typical computer data file. It can be a file of any form as utilized in electronic, electro-magnetic, and optical network-based communications. The apparatus includes a file splitter that splits the file into a plurality of message segments. Each message segment includes an address of the destination.

The term "transmit" as used herein means the directing of a file from any source location to any destination location. The actual transmission of a file may occur via all suitable techniques of file transfer, including, but not limited to, standard file-transfer protocols via an electronic or optical network.

The apparatus also includes a file encapsulator. The file encapsulator encapsulates at least one of the plurality of message segments. The encapsulation conceals the address of the true origin and ultimate destination during transmission of at least one encapsulated message segment to one or more trusted nodes. The trusted nodes may re-encapsulate the message and retransmit the message segments to the destination for reassembly of the file at the final destination.

The file splitter may also include a file converter. The file converter converts the file into N message segments. The file can be reassembled from a subset of any M of the message segments, where N and M are positive integers, and $N > M \geq 1$.

The apparatus may further include a file encoder. The file encoder encodes the file prior to splitting of the file by the file splitter.

The file encoder, file encapsulator and file splitter may include, for example, integrated circuits, such as microprocessors. A single integrated circuit or microprocessor may include the file encoder, file encapsulator and file splitter. One or more microprocessors may implement software that enables the functioning of the file encoder, file encapsulator or file splitter. Any of the file encapsulator, the file splitter and the file encoder may be implemented in software, firmware or hardware (e.g. as an application-specific integrated circuit). The software may be designed to run on general-purpose equipment or specialized processors dedicated to the functionality herein described.

In second aspect, the invention involves a method of secure transmission of a file from a source to a destination. The method includes splitting the file into a plurality of message segments. Each message segment includes an address of the destination.

The method further includes encapsulating at least one of the plurality of message segments to conceal the address of the origin and destination. At least one encapsulated message segment is transmitted to one or more trusted nodes. The one or more trusted nodes retransmit at least one message segment to the destination for reassembly of the file at the destination.

The process of splitting the file may include converting the file into N message segments. The N message segments may enable reassembly of the file from a subset of any M of the message segments, where N and M are positive integers, and $N > M \geq 1$.

Retransmitting at least one message segment may include transmitting at least M of the N message segments to the destination. The file can be reassembled after at least M of the N message segments arrive at the destination.

Transmitting to one or more trusted nodes may include

transmitting more than one message segment via multiple pathways of a communications network. In another embodiment, the method further includes encoding the file. Encoding the file may include enciphering the file.

Encapsulating at least one message segment may include enciphering at least one of the message segments. Encapsulating may further include adding forwarding instructions to the message segment. The forwarding instructions instruct one of the trusted nodes to forward the message segment towards the destination. The forwarding instructions may include the address of the destination. Encapsulating may further include addressing each one of the plurality of message segments to one of the plurality of trusted nodes.

The foregoing and other objects, aspects, features, and advantages of the invention will become more apparent from the following description and from the claims.

Brief Description of the Drawings

In the drawings, like reference characters generally refer to the same parts throughout the different views. Also, the drawings are not necessarily to scale, emphasis instead generally being placed upon illustrating the principles of the invention.

FIG. 1 illustrates an embodiment of a communication of a message from a source to a destination.

FIG. 2 illustrates an embodiment of a communication of a message that provides improved message security.

FIG. 3 illustrates an embodiment of a method that provides message delivery assurance and security.

FIG. 4 illustrates an embodiment of spatial diversification of message transmission, which transmits split message segments along three paths through a network.

FIG. 5 illustrates an embodiment of reassembly of a message at a destination.

FIG. 6 illustrates an embodiment where obstruction of a single node does not deny message transmission.

FIG. 7 illustrates an embodiment where eavesdropping on a single link provides no information.

FIG. 8 illustrates an embodiment with integration of data encryption into an encoder and a decoder.

FIG. 9 illustrates an embodiment with integration of data encryption into the a splitter and a assembler.

FIG. 10 illustrates an embodiment of an apparatus for transmitting a file via a communications network.

FIG. 11 illustrates an embodiment of N message segment identifiers attached to N message segments.

FIG. 12 illustrates an embodiment of an apparatus for transmitting a file.

FIG. 13 illustrates an embodiment of an encapsulated message segment addressed to a trusted node.

FIG. 14 illustrates an embodiment of a message segment addressed to a destination.

Description

The terms "file", "message", "data" and "data file" are herein understood to refer to any entity of data that may be transferred via analog or digital means. The entity may originate in analog or digital form, and, at various times, may be stored in analog or digital form. The entity is capable of transfer between two distinct physical locations via, in

particular, electronic, wireless and optically based communications.

Although, as explained above, the present invention may be applied to any form of data or message, particularly high security can be achieved by splitting a message into multiple segments sent over different network pathways. At the same time, this approach also involves a greater degree of complexity than applications utilizing a single pathway.

Accordingly, for purposes of explanation, an advantageous technique of message splitting for multiple-pathway networks is described below in the section labeled "I". Then, in the section labeled "II", further embodiments of the invention are described, which have particular utility in connection with transmission of split messages via a single pathway or via multiple pathways.

I. Message Splitting and Spatially Diversified Message Routing for Increasing Transmission Assurance and Data Security Over Distributed Networks

An apparatus and method for data assurance in communication networks makes advantageous use of aspects of networked communication. Though the below discussion is applicable to communication networks generally, several embodiments are given for mobile ad-hoc networks (MANET), since some features are preferably applied to MANETs.

During a typical communications session (between, e.g., an originating node and a destination node), messages can be forwarded along multiple, variable data paths. Aggregation of a number of such paths forms a single "super path." In one embodiment, a method includes encoding a message, splitting the encoded result into distinct message segments, and sending each segment along a different path. A receiving node may reconstruct the original message without the requirement that all message

segments eventually reach the receiving node after traveling along their individual paths.

One embodiment includes a protocol that enables a sender to provide information to a destination, i.e., receiver node, about encoding and splitting algorithms that were used to process a message. Some embodiments include methods for inferring the status of the collection of links. Some embodiments include one or more algorithms for determining which combination of encoding and splitting algorithms to use in response to a current status of the links.

Hence, some embodiments enable dynamic adjustment in response to changing network communication conditions, in particular for a MANET. One such embodiment includes a set of encoding/decoding algorithms and a set of splitting/reassembling algorithms to permit an optimized response to the dynamic variations in the link characteristics. Modified algorithms can incorporate data security enhancement features.

For example, encoding algorithms may be used to prevent the deduction of any part of the original message from individual processed message segments. A minimum number of message segments may be required to reconstruct the original message. Further, encryption keys may be used to enhance security. In particular, security enhancement can be achieved by deterministically varying a set of splitting/reassembling algorithms.

Data assurance in networks can be adjusted to a desired level by choosing an appropriate encoding and splitting scheme to tolerate failures over a sufficiently large number of paths. Encoding redundancy can reduce or eliminate the need for message retransmission. Message delay may be reduced, and utilization of each link in the network may be increased. Generally, the benefit in overall network resource utilization and performance grows with the number of links, i.e., the number of directly

communicating node-pair combinations, and the expected number of relaying hops through which a packet is forwarded towards its destination.

In one aspect, the apparatus and method improve data security. As multiple message segments are required to decode the original message, an eavesdropper sniffing, e.g., packets traveling on a particular path cannot deduce much useful information. Additional security components or steps can improve the level of data security; for example, encoding mechanisms can be chosen to avoid exposing the original data bits directly and a bit-position scrambling mechanism can be incorporated before splitting of the message. This provides security gains that require almost no increase in system complexity or computational burden.

In one embodiment, a redundantly encoded message is transmitted by aggregating multiple paths in a MANET to form a single super-path. This aggregation provides robustness in view of the potentially drastic variation in individual links. The super-path has a collective characteristic that improves stability, and statistically resembles a fixed link pathway in comparison to a pathway through a conventional MANET.

The channel coding technique may first encode the message to inject the desired level of redundancy into the message, then split the encoded message into multiple segments, and then forward each segment along a different path. At the receiving end, the extra redundancy injected by the encoding method (via, e.g., erasure correcting codes) may permit reassembly of the original message without requiring the successful delivery of all message segments through their individual paths.

Encoding methods may be used to improve the data assurance to a desired level for a network, or example, a MANET. This is more effective for MANET-based communications than simply

adopting or adapting the two-pronged approach of fixed point-to-point channels (and conventional networks). The characteristics of the aggregated super-path more closely resemble that of the fixed point-to-point channel than that of the individual member paths in the aggregate. Moreover, the variation in the characteristics of the super-path is slower than the variation of individual member paths, and can be designed to become tractable.

As a result, the variation of super-path characteristics can become more sensitive to network communications congestion than to link-to-link communication variations, e.g., radio frequency channel variations, arising from movement of the nodes. Hence, in one embodiment, super-path characteristics are regularly or continuously analyzed, and encoding and splitting algorithms are selected from classes of encoding algorithms and splitting algorithms in response to a determined characteristic. Super-path characteristics may include, for example, the number of successfully received message segments and the identity of the paths through which message segments are successfully received.

The performance of these classes of algorithms can be rated. Protocols that implement measurement of super-path characteristics and dynamic selection of an optimum combination of encoding algorithms and splitting algorithms can also be rated. Rating of algorithms and protocols can permit improved optimization of selections.

Encoding and splitting of messages directly improves message security. Because the message segments are forwarded along distinct routes to the destination, an eavesdropper must simultaneously intercept multiple message segments before a successful recovery of the original message becomes possible. The mobility and the geographical distribution of the nodes in the network make this difficult, and splitting the message into more segments can increase the difficulty of recovery.

Furthermore, an encoding algorithm can be chosen that prevents message reconstruction without interception of at least a threshold portion of message segments.

Additional security is made possible by scrambling, even simple scrambling, of the positions of the encoded message bits, e.g. before splitting, to prevent message reconstruction by an eavesdropper even when the eavesdropper intercepts a sufficiently large number of message segments. Generally, scrambling and de-scrambling of bit positions requires many fewer operations to execute and complete than traditional encryption and decryption methods.

Some embodiments include a stand-alone protocol layer for insertion in the networking protocol layer. For example, the protocol layer can be inserted between the medium access control (MAC) layer and the networking layer of a communication system. The protocol layer may include mechanisms for monitoring or analyzing the characteristics of network links and a decision algorithm to dynamically choose one of a class of encoding and splitting algorithms based on the observed network link characteristics.

In one embodiment, when the link stability is low, the protocol layer switches to an encoding algorithm that tolerates more losses of the message segments and a message-splitting scheme that results in smaller segments, in an attempt to improve delivery assurance. In another embodiment, when the link stability improves, the protocol layer switches to an encoding algorithm that has requires more message segments to be received and a message-splitting scheme that uses larger segments, in an attempt to reduce the protocol overhead.

The impact of the proposed algorithm and the dynamic protocol can be measured at multiple levels of the network. The probability of delivery success in a single attempt can be

improved to any desired level by choosing an appropriate combination of encoding and splitting methods or algorithms. Generally, an entire message is not transmitted along a single path. Instead, a message is fragmented, i.e. split, and forwarded along multiple paths. The realized increase in data assurance general comes with an initial delay in transmission of message segments, or packets, due to the encoding and splitting. Generally, however, overall communications delays are improved because of the improved probability of completion of each message transmission in the first attempt.

Referring to **Figure 1**, an embodiment of a communication of a message from a source to a destination is illustrated. A message **1**, e.g., a block of message bits, is fed to an encoder **2**, e.g. a scrambling encoder. The encoder **2** injects redundancy into the message bit stream, which increases the number of bits in the message. The encoded message is fed to a message splitter **4**, which breaks the message into N message segments.

The N message segments are forwarded to the destination along different paths in a network **3**. An assembler **6** reassembles the encoded message as the segments are received. When the number of segments received reaches a specified threshold, a partially reassembled message is passed to a decoder **8**, e.g. an erasure decoder. The decoder recovers the original message **1**, using only the bits available from the partially assembled message. The threshold number of segments is determined by the selected coding scheme. Both the assembler **6** and the erasure decoder **8** may be implemented in hardware and/or as software modules.

Improving the probability of completed delivery of a message in a first attempt reduces both the average delay and the number of retransmissions required for deliver of messages through the network. Reducing the number of retransmissions decreases the

number of channel contentions in a network with multi-accessing nodes such as a MANET. This may significantly improve the utilization of both the links and the network, in terms of factors such as the number of data bits sent per usage of bandwidth, channel, link, battery power, etc. This in turn significantly improves the overall network throughput and efficiency.

Figure 2 illustrates an embodiment that provides improved message security. A sender **10** and a receiver **20** agree to use a combination of an encoding scheme and a splitting mechanism that splits each message into three segments for transmission via a MANET **23**. The MANET **23** includes several nodes **a-g**. The encoding scheme requires at least two message segments to reach the receiver for recovery of a split message. An eavesdropper is illustrated as intercepting message segments between nodes **c** and **e**; a jammer is illustrated as blocking transmission of message segments at node **f**. Three paths P_1, P_2, P_3 through the network **23** are a subset of all possible paths. Message security and integrity are maintained in spite of the efforts of the eavesdropper and the jammer.

The eavesdropper acquires only a message segment transmitted along path P_3. Because the number of message segments threshold is 2, the single segment does not provide any useful information to the eavesdropper. All three segments will reach the receiver **20**. The first two to arrive are used to reassemble the original message.

The jammer attacking node **f** prevents the message segment traveling on path P_3 from reaching the receiver **20**. The other two message segments, however, arrive, and the message is recovered. The jammer cannot prevent the receiver **20** from getting the message.

Several criteria may be used to assess the performance of alternative implementations of a decision algorithm and a dynamic protocol. Such criteria may include, for example:

- delivery assurance, the probability of successful receipt of a fully correct message (affected by the probability of link/node failure);
- security improvement, in terms of the number of message segments that must be acquired by an eavesdropper in order to reconstruct the original message; and
- improvement in effective bandwidth, the reduction in the number of required retransmissions as compared to, for example, the adaptation of the two-pronged approach to a MANET.

In one embodiment, a protocol is inserted into a network communications protocol stack, e.g., between the MAC and the networking layer. This protocol mechanism senses and predicts variations in the characteristics of the link aggregate, and dynamically chooses the best combination of encoding/decoding and splitting/reassembly algorithms from a set or class of algorithms. The attempt to optimize can seek a combination that adds the least overhead to achieve a specified probability of successful message delivery. The selection process may further include, e.g., consideration of message priority, other measures of message importance, or cost of latency.

Referring to **Figure 3**, one embodiment is illustrated of a method that provides message delivery assurance and security. The method includes encoding the message to inject redundancy into a message stream, and splitting the encoded message. The split, encoded message is forwarded along spatially diversified routes.

For example, a message, or message block, that includes k bits is processed through an encoder **2**, e.g., a scrambling encoder, that converts the message into an encoded message block of n bits, where n > k. A splitter **4** decomposes the output of the encoder **2** into N message segments, each segment including no more than [n/N] bits. "[n/N]" denotes the least integer greater than n/N. N, n and k are positive integers.

Figure 4 illustrates spatial diversification. Each of the N message segments is forwarded to the intended recipient, preferably along a different route. This gives spatial diversification to the routes used for transmission. Nodes **a-g** are a subset of network **23** nodes. The sender **10** forwards segments to the receiver **20** along path P_1 (including nodes **a** and **g**), path P_2 (including nodes **b** and **d**), and path P_3 (nodes **c**, **e**, and **f**). The different physical locations of the nodes forces the message segments to travel through different areas of the network. Link conditions and congestion in different areas may vary considerably.

Referring to **Figure 5**, the message segments are re-assembled as they are received at the receiver **20**. When a sufficiently large number of message segments is received, the partially assembled message is forwarded to a decoder **8**, e.g., an erasure decoder, which recovers the entire original message. Improved delivery assurance is achieved because not all message segments must be successfully received to permit the recipient to recover the original message.

In one embodiment, each message segment has a length of b, where $0 < b \leq [n/N]$. "[n/N]" denotes the least integer greater than n/N. Limitation of the value of b can assure that each encoded message bit exists in only one message segment. Because n must be greater than k, $[k/b] < N$. Hence, there are fewer than N segments when the shorter unencoded message is broken into

segments of length b. A longer, encoded message is obtained with N segments of length b.

The intended recipient can recover the original message with any subset of [k/b] segments of the N message segments, given an appropriate selection of the encoding scheme. Hence, the message recovery mechanism at the intended recipient can tolerate the loss of some of the message segments. This allows for losses due to, e.g., network congestion, broken links, interference or jamming. This may require n bits to be transmitted for every k message bits, where n > k. Advantages are realized, however, such as:

- n/k may be smaller than the number of bits that would be transmitted for each bit if an entire block is retransmitted; and
- the probability that the intended recipient correctly recovers the original message from a single transmission attempt is improved.

Examples of classes of error-correcting codes that can be utilized include Bose-Chaudhuri-Hocquenghem (BCH) codes, Convolutional codes, Hamming codes, Reed-Solomon codes, Golay codes, Turbo codes, and several other linear and nonlinear block codes.

Various embodiments provide significant security benefits. Referring to **Figure 6**, resistance to localized jamming is one benefit. Jamming, for example, disrupting transmission at a single network node or link, minimally impacts the functionality of the rest of the network. When a jammer located near node **f** has broken the continuity of path P_3, path P_1 and path P_2 are still able to deliver message segments, and the message is successfully decoded. To be effective at disruption, a jammer must be located close enough to either the sender **10** or receiver

20 to jam a significant number of message segments. For example, the probability of disruption in a mobile, military network is reduced by the requirement for close proximity of a hostile jammer.

Referring to **Figure 7**, another security benefit of some embodiments is the difficulty an eavesdropper experiences when trying to intercept messages. As illustrated in **Figure 7**, an eavesdropper is physically located between node **c** and node **e**, able to copy any message segment, e.g., data packet, that passes along path P_3. The eavesdropper must correctly receive a minimum of [k/b] message segments to recover a complete message. To receive the minimum number of segments, however, requires eavesdropping on other paths P_1, P_2.

Some embodiments prevent even partial message recovery by the eavesdropper. An appropriately chosen scrambling encoder (e.g., a non-systematic code) can be used to create a condition during which any subset of q message segments, with $q < [k/b]$, will prove insufficient to recover any subset of the original message. Similar to the jammer, the eavesdropper must be physically located very close to either the sender **10** or the intended recipient **20** to effectively intercept segments from multiple paths P_1, P_2, P_3.

The effectiveness of a local jammer is reduced by taking advantage of the nature of a distributed networking environment. Similarly, a single eavesdropper has a reduced ability to observe enough segments to allow an understanding of the communications carried by the network. As a result, the overall security of information carried by the entire network is significantly improved.

Some embodiments further improve security through use of data encryption by means of bit position scrambling. The selection of a scrambling encoder can be controlled with an encryption key. In some alternative embodiments, the actual bit scrambling can be accomplished in either an encoder or a splitter.

Referring to **Figures 8** and **9**, embodiments that utilize permutation are illustrated. **Figure 8** schematically shows the use of permutation by an encoder **2a**. **Figure 9** shows the use of permutation by a splitter **4a**. For example, even a simple use of an encryption key to alter bit positions in the encoded message, would require the eavesdropper to potentially search through n! possibilities.

Some embodiments that include a scrambling encoder employ an encoding scheme that provides one or both of the following features:

- the encoding scheme provides strong resilience against loss of message segments, preferably having the value of (k + e) as close to n as possible, where e is the number of message segment losses that the scheme can overcome, k is the original message length, and n is the encoded message length; and
- no bits in the original message are ascertainable from any message subset below a threshold number; for linear block codes, this generally requires use of non- systematic codes and that approximately half of the elements of a generating matrix elements have a value of 1.

In order for the assembler at the receiving node to correctly reassemble the message fragments, the content of each segment must be identified. In one embodiment, the information required for reassembly is reduced by inclusion of a numbering

scheme for the message segments. In a preferred embodiment, a segment carries identification that is a number assigned by the message splitter. This number may be a field in a protocol header that is attached to each message segment, or embedded in the message segment itself.

Additional protocol header fields may be included when encoding and splitting algorithms are altered dynamically to better suit the observed characteristic variations of the super-path. The additional fields can carry measurement data regarding the characteristics of the super-path as well as data that informs the destination node of the changes in the encoding and splitting algorithms. Inclusion of additional protocol header fields incurs additional transmission bandwidth for every hop. Hence, it is preferable to optimize choices of fields to minimize the resulting bandwidth expansion.

Referring to **Figure 10**, an embodiment of an apparatus **30** for transmitting a file via a communications network is illustrated. The apparatus **30** includes a file processor **31**, which may be implemented in hardware and/or as a software module, and a message segment transmitter **32**. The file processor converts files into N message segments that enable reassembly of the file from a subset of any M of the message segments. N and M are positive integers and $N > M \geq 1$.

The message segment transmitter **32**, which may be implemented in hardware and/or as a software module, transmits message segments to a receiver. The receiver can reassemble a file after receiving M of the N message segments.

The file processor **31** may comprise a file encoder **35** and an encoded file splitter **36** that convert a file into N message segments. The file encoder **35** may implement a class of encoding

algorithms in generating the message segments. The encoded file splitter **36** may implement a class of splitting algorithms.

The processor **31** may further comprise a communications network analyzer **37**, which may be implemented in hardware and/or as a software module, that determines the condition of a communications network. The processor **31** may also include a message segment parameter selector **38** (which also may be implemented in hardware and/or as a software module) that selects a set of values for M and N based on the determined condition to achieve a preselected probability of a successful transmission of M of the transmitted message segments.

Referring to **Figure 11**, the apparatus may include N message segment identifiers **33** that have a one-to-one association with the N message segments **34**. In the embodiment illustrated in Figure 11, message segments **34** are transmitted with their associated identifiers **33** to assist in reassembly of the message. The identifiers **33** can include, for example alphanumeric data. In one embodiment, during transmission, the identifiers **33** are binary numbers.

The above described and various other embodiments are of particular value when applied, for example, to ad-hoc networks, MANETs and conventional packet networks with distributed routing algorithms. Particular value accrues when applied to MANETs that include moderately mobile units.

II. Method and System for Secure Exchange of Messages

The security of information carried by a network may be improved when a sender and recipient utilize a trusted node as an intermediary for exchange of communications. A trusted node may be selected for its ability to securely and reliably forward communications, such as messages, message segments and storage

segments. For example, rather than addressing every message segment to an intended recipient, a message sender may address one or more of the message segments to one or more trusted nodes. In preferred embodiments, forwarding instructions are included with the message segments to enable forwarding of the segments to the intended recipient.

Various embodiments may be used to obscure the origin and destination of a message. Message interception is very difficult for an eavesdropper tapping a communication link, even if the link is in close proximity to either the sender or recipient. To deduce the messages of a particular conversation, all messages or message segments received by, or leaving, the recipient (who may also be a sender) must be captured. Further, some or all of the communications may be encrypted to further complicate the eavesdropper's task. Increasing the number of trusted nodes can dramatically increase the difficulty of message interception.

Referring to **Figures 12-14**, one embodiment of an apparatus for transmitting a file includes a file splitter **71** that splits the file into a plurality of message segments **81**. Each message segment includes forwarding instructions **82**, e.g., an address of the destination. The transmission of message segments **81** may occur via all suitable techniques of file transfer, including, but not limited to, standard file-transfer protocols via an electronic or optical network.

The apparatus also includes a file encapsulator **73**. The file encapsulator **73** encapsulates at least one of the plurality of message segments **81**. The encapsulation **83** conceals the address of the destination during transmission of the encapsulated message segment **81** to one or more trusted nodes.

A trusted node address **84**, which is publicly visible, is attached to the encapsulated message segment **81** to permit transmission of the message segment **81** to the corresponding

trusted node. The trusted node re-encapsulates and retransmits the message segment **81**, in part by examining the forwarding instructions **82** and making the address of the next destination, which may be the final destination address **85**, visible to the network.

The file splitter **71** may also include a file converter. The file converter converts the file into N message segments that permit reassembly of the file from a subset of any M of the message segments, where N and M are positive integers, and $N > M \geq 1$.

The apparatus may further include a file encoder **72**. The file encoder **72** encodes the file prior to splitting of the file by the file splitter **71**.

The file encoder **72**, file encapsulator **73** and file splitter **71** may include, for example, integrated circuits, such as microprocessors. A single integrated circuit or microprocessor may include the file encoder **72**, file encapsulator **73** and file splitter **71**. One or more microprocessors may implement software that enables the functioning of the file encoder **72**, file encapsulator **73** or file splitter **71**. Any of the file encapsulator **73**, the file splitter **71** and the file encoder **72** may be implemented in software, firmware or hardware (e.g. as an application-specific integrated circuit). The software may be designed to run on general-purpose equipment or specialized processors dedicated to the functionality herein described.

An embodiment of a method of secure transmission of a file from a source to a destination includes splitting the file into a plurality of message segments. Each message segment includes an address of the destination. The method may further include encoding the file. Encoding the file may include enciphering the file.

The process of splitting the file may include converting the file into N message segments. The N message segments may enable reassembly of the file from a subset of any M of the message segments, where N and M are positive integers, and $N > M \geq 1$.

The method also includes encapsulating at least one of the plurality of message segments to conceal the address of the destination. At least one encapsulated message segment is transmitted to one or more trusted nodes. Message segments may be transmitted via multiple pathways of a communications network.

The one or more trusted nodes retransmit the message segment to the destination for reassembly of the file at the destination. Retransmitting at least one message segment may include transmitting at least M of the N message segments to the destination. The message segment may be encapsulated during transmission from the trusted node to another trusted node or to the destination. The file can be reassembled after at least M of the N message segments arrive at the destination.

Encapsulating a message segment may include enciphering the message segments. Encapsulating may further include adding forwarding instructions to the message segment. The forwarding instructions instruct a receiving one of the trusted nodes to forward the message segment toward the destination. The forwarding instructions may include the address of the destination. Encapsulating may further include addressing each one of the plurality of message segments to one of the plurality of trusted nodes.

Some embodiments of a method of secure transmission of a file from a source to a destination include two or more stages of file splitting. In these embodiments, one or more message segments from a first file splitting step may be further split into additional message segments. A second splitting step may be advantageous, for example, when a node that transmits files via a

network has limited access to the network. For example, a node that transmits files via the Internet may have limited gateway access. The access may be limited, for example, to as few as one or two gateways.

The node might then split a file into a few message segments, for example three message segments, and transmit the message segments to the gateways. The gateways could further split one or more of the three message segments, and then forward message segments toward a destination via the Internet.

In some embodiments of a method, which include multiple splitting steps, the file is converted into N message segments that enable reassembly of the file from a subset of any M of the message segments. At least M of the N message segments are transmitted toward a destination for reassembly of the file after receiving M of the N message segments.

At least one of the transmitted segments is further converted into N_2 message segments that enable reassembly of the at least one message segment from a subset of any M_2 of the N_2 message segments, where N_2 and M_2 are positive integers and $N_2 > M_2 \geq 1$. At least M_2 of the N_2 message segments are transmitted toward the destination for reassembly of the at least one message segment prior to reassembly of the file.

The at least M_2 segments may be reassembled at the destination. Alternatively, the at least M_2 segments may be received and reassembled by an intermediate node. The reassembled segment may then be transmitted toward the final destination. Additional conversion steps and/or reassembly steps may be included at intermediate nodes in the network.

Various embodiments of the method and apparatus for secure exchange of messages may be applied to network-based communications. Relevant networks include, but are not limited to, local-area networks (LAN) or a wide area networks (WAN) such

as the Internet or the World Wide Web. Senders and receivers can be connected to a WAN either directly or via a LAN through a variety of connections including standard telephone lines, LAN or WAN links (e.g., T1, T3, 56kb, X.25), broadband connections (ISDN, DSL, Frame Relay, ATM), and wireless connections. The connections can be established using a variety of communication protocols (e.g., TCP/IP, IPX, SPX, NetBIOS, Ethernet, RS232, and direct asynchronous connections).

In some embodiments, the sender and receiver are comprised of appropriate computer hardware. Examples of such hardware include any personal computer (e.g., Windows or Macintosh operating system computer), Windows-based terminal, Network Computer, wireless device, information appliance, RISC Power PC device, X-device, workstation, mini computer, main frame computer or other computing device.

Alternatively, the sender or receiver can be a portable computing device such as a PDA or cell phone. As a further alternative, the sender or receiver can be any terminal (windows or non-windows based), or thin-client device operating according to a server-based computing model.

Variations, modifications, and other implementations of what is described herein will occur to those of ordinary skill in the art without departing from the spirit and the scope of the invention as claimed. Accordingly, the invention is to be defined not by the preceding illustrative description but instead by the spirit and scope of the following claims.

What is claimed is:

CLAIMS

1. An apparatus for transmitting a file, comprising:
   a file splitter that splits the file into a plurality of message segments, each message segment including an address of the destination; and
   a file encapsulator that encapsulates at least one of the plurality of message segments to conceal the address of the destination during transmission of at least one encapsulated message segment to one or more trusted nodes for retransmission by the one or more trusted nodes toward the destination for reassembly of the file at the destination.

2. The apparatus of claim 1 wherein the file splitter comprises a file converter that converts the file into N message segments that enable reassembly of the file from a subset of any M of the message segments, where N and M are positive integers, and $N > M \geq 1$.

3. The apparatus of claim 1 wherein a single processor includes the file splitter and the file encapsulator.

4. The apparatus of claim 1 further comprising a file encoder that encodes the file prior to splitting of the file by the file splitter.

5. A method of secure transmission of a file from a source to a destination, comprising the steps of:
   splitting the file into a plurality of message segments, each message segment including an address of the destination;
   encapsulating at least one of the plurality of message segments to conceal the address of the destination;
   transmitting at least one encapsulated message segment to one or more trusted nodes; and

causing retransmission of the at least one of the plurality of message segments from the one or more trusted nodes toward the destination for reassembly of the file at the destination.

6. The method claim 5 wherein the step of splitting the file comprises the step of converting the file into N message segments that enable reassembly of the file from a subset of any M of the message segments, where N and M are positive integers, and $N > M \geq 1$.

7. The method of claim 6 wherein the step of causing retransmission comprises causing splitting of the at least one message segment into N_2 message segments that enable reassembly of the at least one message segment from a subset of any M_2 of the N_2 message segments, where N_2 and M_2 are positive integers and $N_2 > M_2 \geq 1$; and causing transmission of at least M_2 of the N_2 message segments toward the destination for reassembly of the at least one message segment prior to reassembly of the file.

8. The method of claim 6 wherein the step of causing retransmission comprises the step of transmitting at least M of the N message segments to the destination for reassembly of the file after at least M of the N message segments arrive at the destination.

9. The method of claim 5 wherein the step of transmitting comprises the step of transmitting more than one message segment via multiple pathways of a communications network.

10. The method of claim 5 further comprising the step of encoding the file prior to transmission.

11. The method of claim 10 wherein the step of encoding the file comprises the step of enciphering the file.

12. The method of claim 5 wherein the step of encapsulating at least one of the plurality of message segments comprises the step of enciphering the at least one of the plurality of message segments.

13. The method of claim 5 wherein the step of encapsulating at least one of the plurality of message segments comprises the step of adding forwarding instructions to at least one of the plurality of message segments to instruct a receiving one of the plurality of trusted nodes to forward at least one of the plurality of message segments toward the destination.

14. The method of claim 5 wherein the step of encapsulating at least one of the plurality of message segments comprises the step of addressing each one of the plurality of message segments to one of the plurality of trusted nodes.

15. The method of claim 5 wherein the step of causing retransmission comprises causing splitting of the at least one of the plurality of message segments into a second plurality of message segments including an address of the destination; and causing transmission of the second plurality of message segments toward the destination.

16. The method of claim 15 further comprising the steps of causing reassembly of the at least one message segment; and causing transmission of the at least one reassembled message segment toward the receiver.

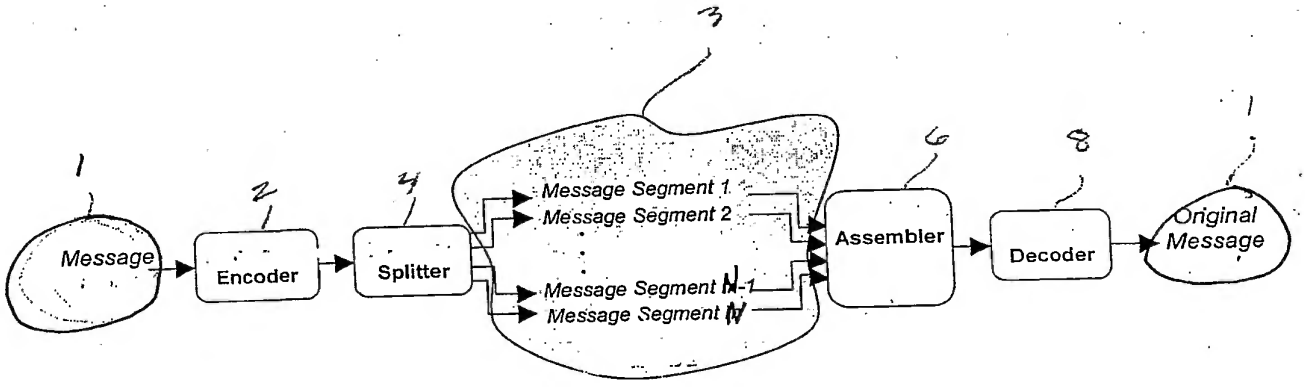


Figure 1

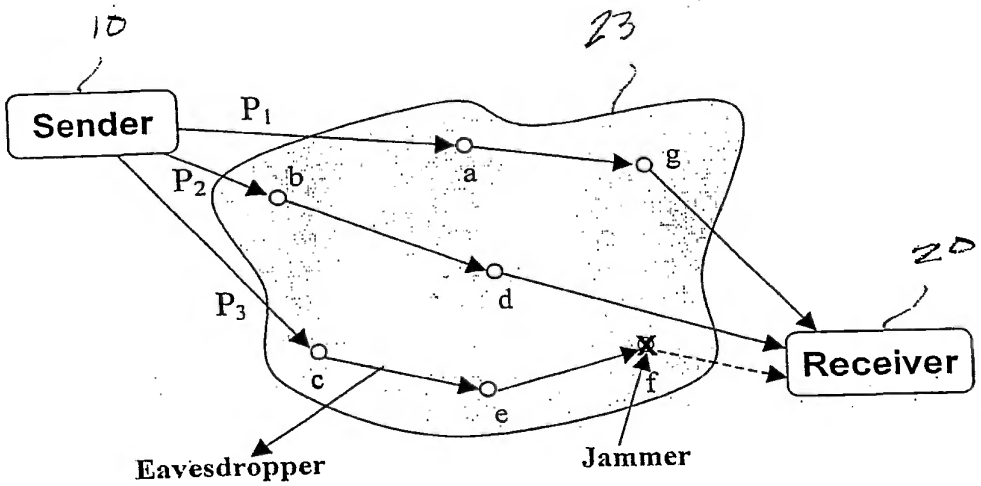


Figure 2

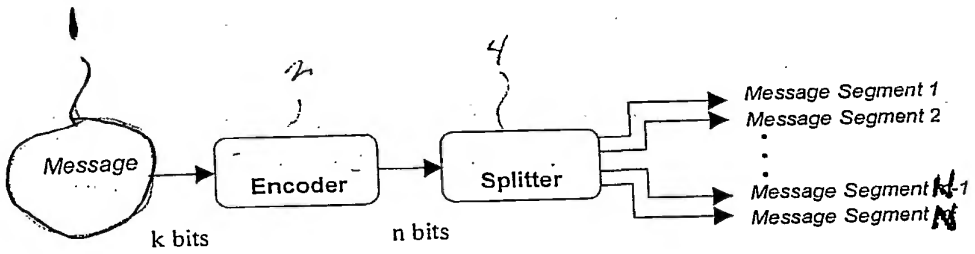


Figure 3

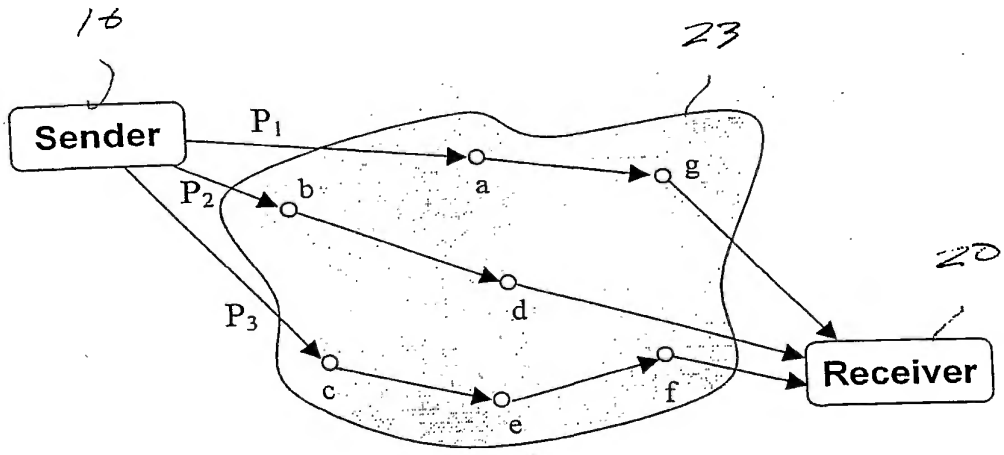


Figure 4

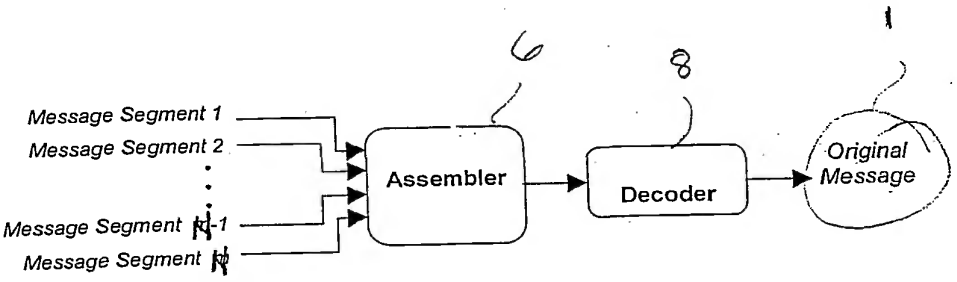


Figure 5

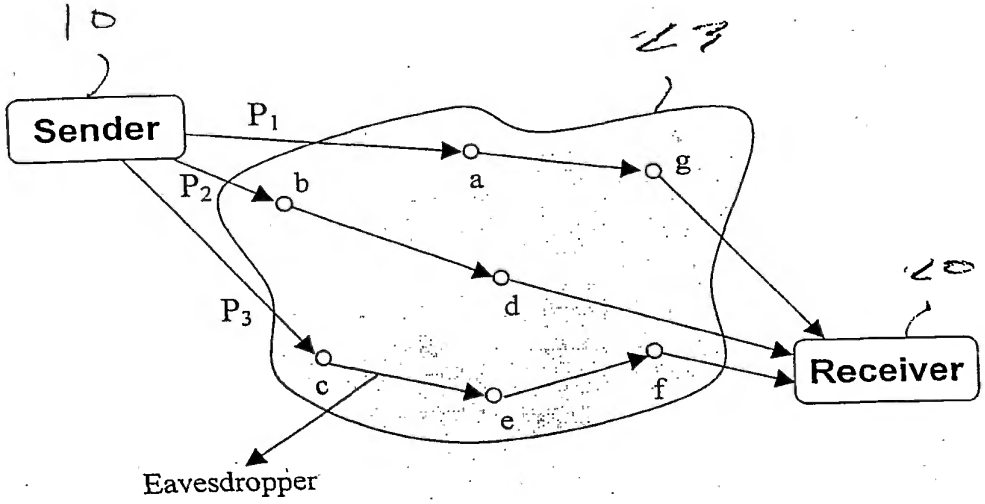


Figure 7

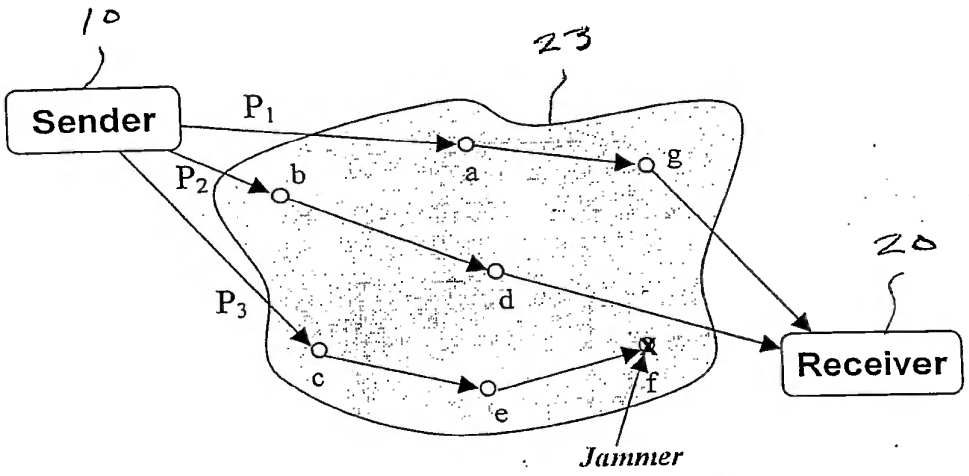


Figure 6

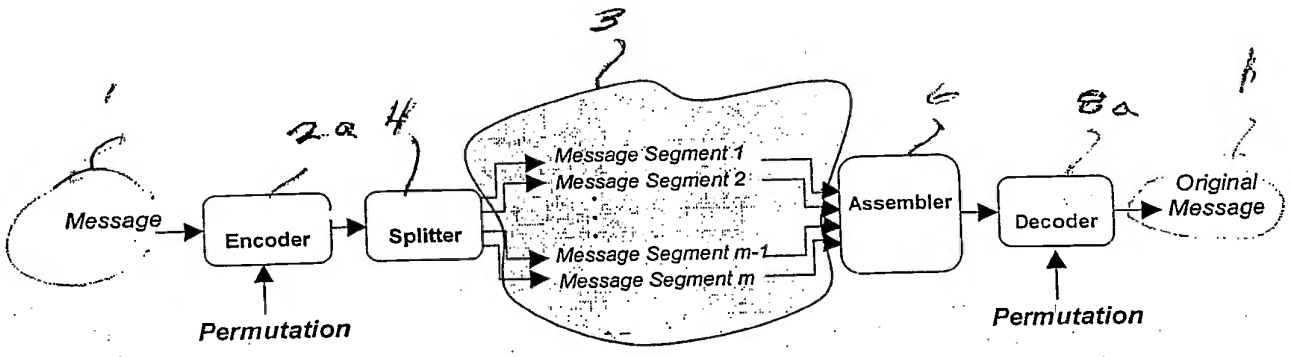


Figure 8

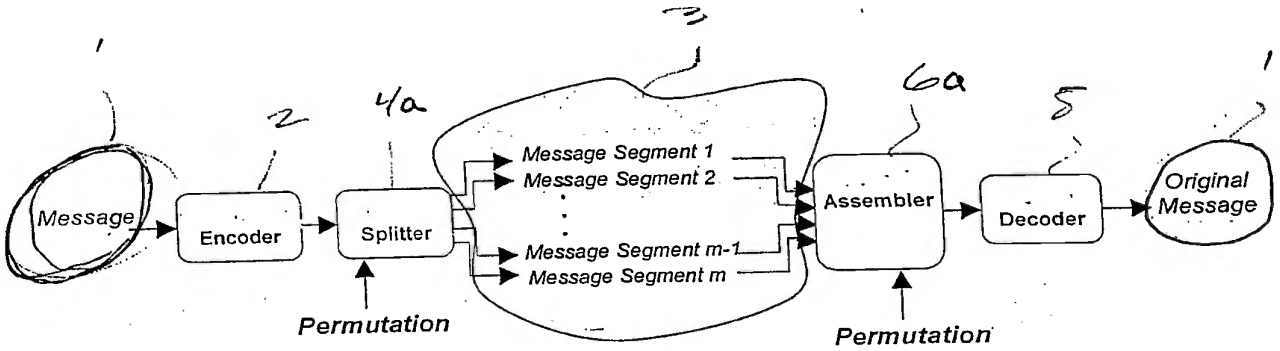

Message
Encoder
Splitter
Message Segment 1
Message Segment 2
Message Segment m-1
Message Segment m
Assembler
Decoder
Original Message
Permutation
Permutation

Figure 9

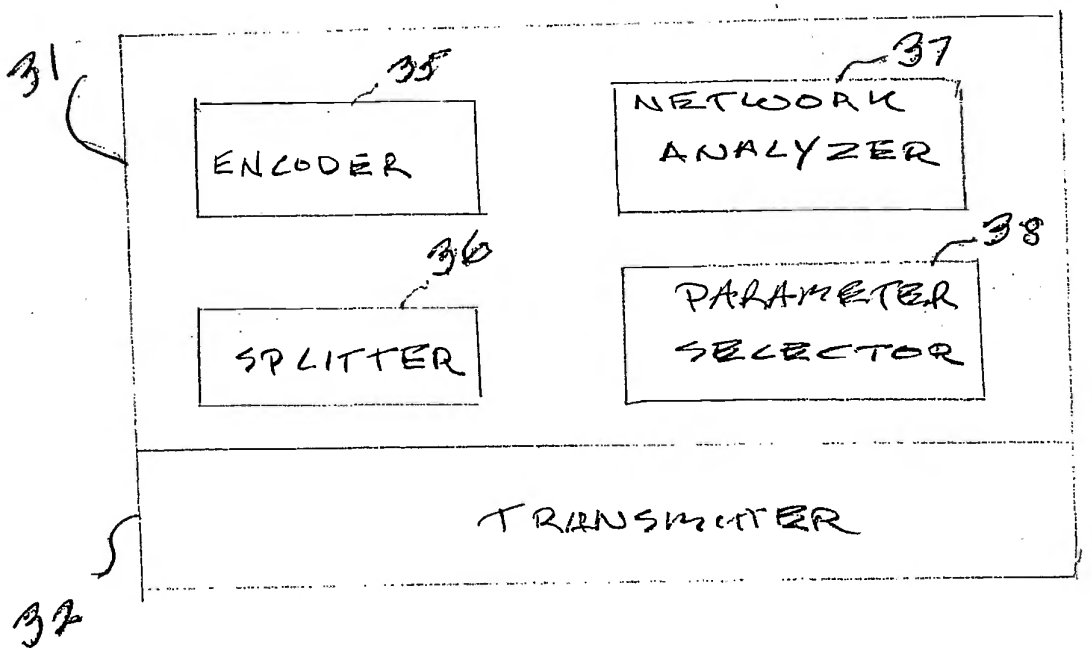

30
31
35
ENCODER
37
NETWORK ANALYZER
36
SPLITTER
38
PARAMETER SELECTOR
TRANSMITTER
32

FIG. 10

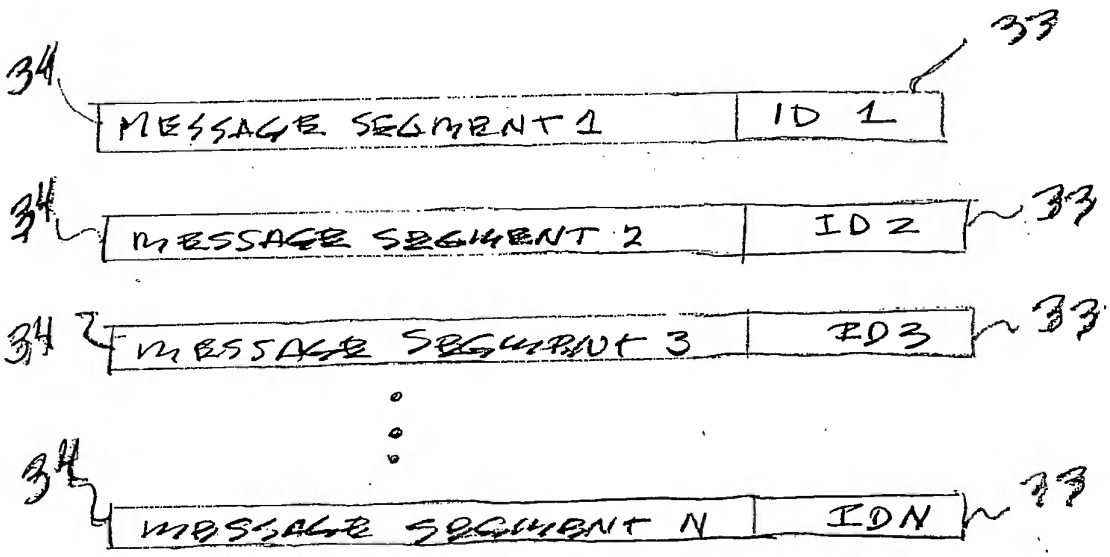

34
MESSAGE SEGMENT 1
ID 1
33
34
MESSAGE SEGMENT 2
ID 2
33
34
MESSAGE SEGMENT 3
ID 3
33
34
MESSAGE SEGMENT N
ID N
33

FIG. 11

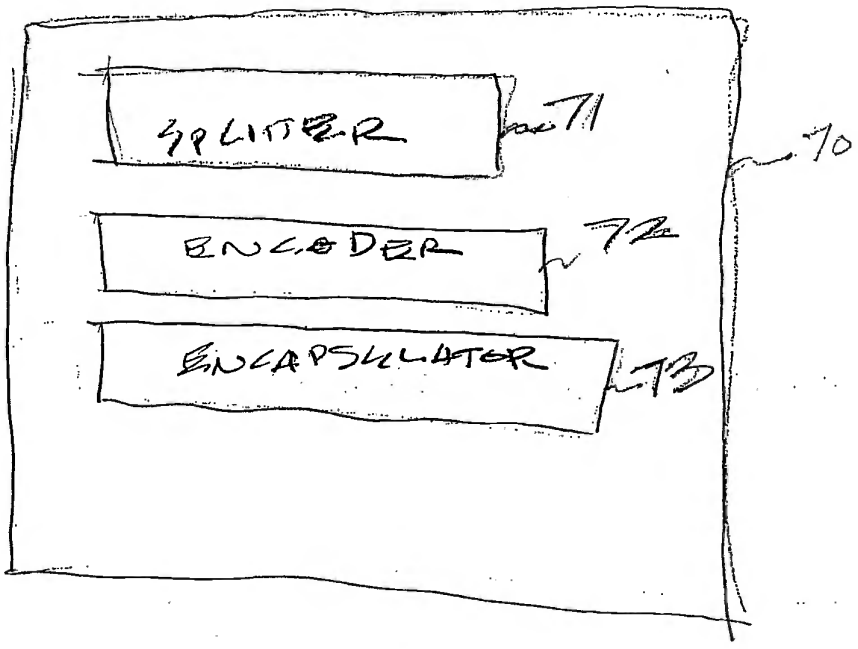


FIG. 12

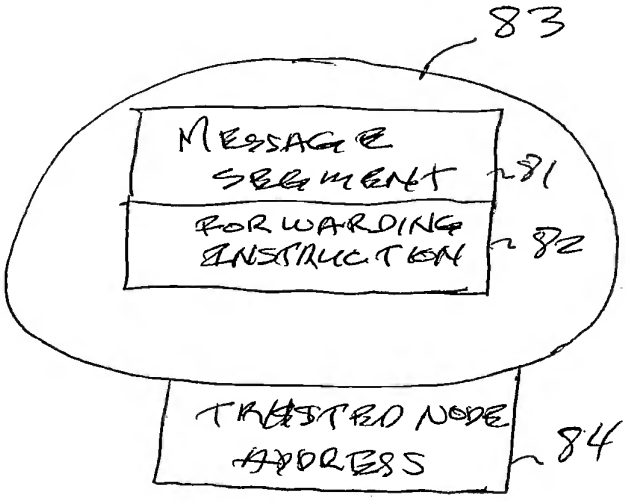

83
MESSAGE SEGMENT
81
FORWARDING INSTRUCTION
82
TRUSTED NODE ADDRESS
84

FIG. 13

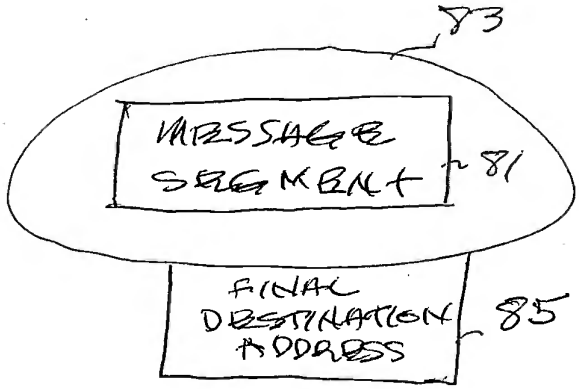

83
MESSAGE SEGMENT
81
FINAL DESTINATION ADDRESS
85

FIG. 14

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 August 2002 (08.08.2002)

PCT

(10) International Publication Number
WO 02/062032 A3

(51) International Patent Classification[7]: H04L 29/06, 29/08

(21) International Application Number: PCT/US01/50069

(22) International Filing Date:
21 December 2001 (21.12.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/258,127 22 December 2000 (22.12.2000) US

(71) Applicant: **THE CHARLES STARK DRAPER LABORATORY, INC.** [US/US]; 555 Technology Square, Cambridge, MA 02139 (US).

(72) Inventors: **SHU, Li**; 20 Acre Road, Billerica, MA 01821 (US). **POPPE, Dorothy, C.**; 169 Sheridan Avenue #2, Medford, MA 02155 (US).

(74) Agent: **ROSE, Jamie, H.**; Testa, Hurwitz & Thibeault, LLP, High Street Tower, 125 High Street, Boston, MA 02110 (US).

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

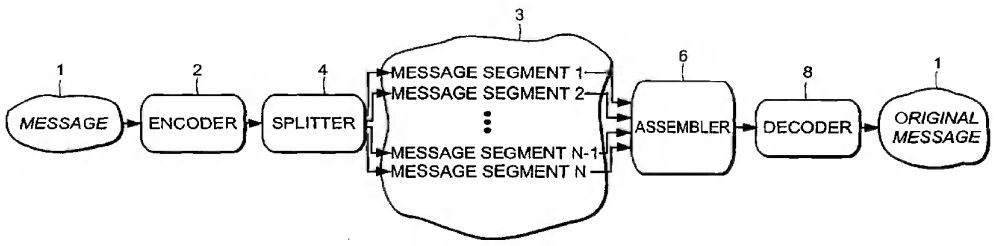
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ,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

Published:
— *with international search report*

(88) Date of publication of the international search report:
10 July 2003

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

(54) Title: METHOD AND SYSTEM FOR SECURE EXCHANGE OF MESSAGES



(57) Abstract: The invention features an apparatus and method for transmitting a file. The apparatus includes a file splitter that splits the file into a plurality of message segments. Each message segment includes an address of the destination. The apparatus also includes a file encapsulator. The file encapsulator encapsulates at least one of the plurality of message segments. The encapsulation conceals the address of the destination during transmission of the at least one encapsulated message segment to one or more trusted nodes. The trusted nodes retransmit the message segments to the destination for reassembly of the file at the destination.

WO 02/062032 A3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 01/50069

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04L29/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 00 27086 A (SCIENCE APPLICATIONS INTERNATIONAL CORPORATION) 11 May 2000 (2000-05-11)	1,3-5, 10-12
Y	claim 61	9
Y	MAXEMCHUK N F: "DISPERSITY ROUTING IN HIGH-SPEED NETWORKS" COMPUTER NETWORKS AND ISDN SYSTEMS, NORTH HOLLAND PUBLISHING. AMSTERDAM, NL, vol. 25, 1993, pages 645-661, XP000570119 ISSN: 0169-7552	9
A	page 645, left-hand column, paragraph 1 page 646, line R, paragraph 4 -page 647, left-hand column, paragraph 1	1-8, 10-16

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 November 2002	26/11/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Veen, G

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 01/50069

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0027086 A	11-05-2000	AU 1455300 A	22-05-2000
		AU 1600300 A	22-05-2000
		EP 1125414 A2	22-08-2001
		EP 1125419 A2	22-08-2001
		JP 2002529965 T	10-09-2002
		JP 2002529779 T	10-09-2002
		WO 0186911 A2	15-11-2001
		US 2002161925 A1	31-10-2002
		US 2002161884 A1	31-10-2002
		WO 0027090 A2	11-05-2000
		WO 0027086 A2	11-05-2000

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

CORRECTED VERSION

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 August 2002 (08.08.2002)

PCT

(10) International Publication Number
WO 2002/062032 A3

(51) International Patent Classification[7]: H04L 29/06, 29/08

(21) International Application Number:
PCT/US2001/050069

(22) International Filing Date:
21 December 2001 (21.12.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/258,127 22 December 2000 (22.12.2000) US

(71) Applicant: **THE CHARLES STARK DRAPER LABORATORY, INC.** [US/US]; 555 Technology Square, Cambridge, MA 02139 (US).

(72) Inventors: **SHU, Li**; 20 Acre Road, Billerica, MA 01821 (US). **POPPE, Dorothy, C.**; 169 Sheridan Avenue #2, Medford, MA 02155 (US).

(74) Agent: **ROSE, Jamie, H.**; Testa, Hurwitz & Thibeault, LLP, High Street Tower, 125 High Street, Boston, MA 02110 (US).

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

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

Published:
— *with international search report*

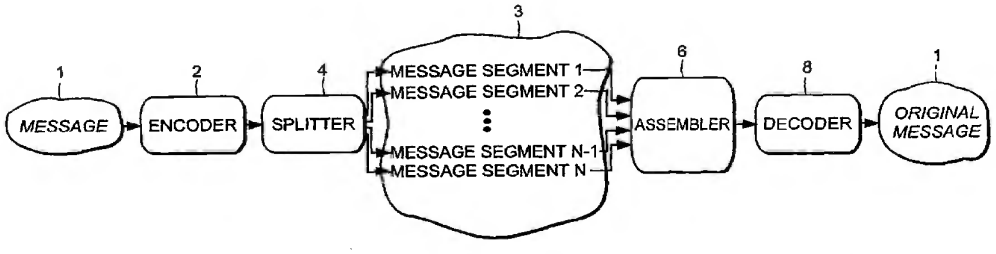
(88) Date of publication of the international search report:
10 July 2003

(48) Date of publication of this corrected version:
13 May 2004

(15) Information about Correction:
see PCT Gazette No. 20/2004 of 13 May 2004, Section II

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

(54) Title: METHOD AND SYSTEM FOR SECURE EXCHANGE OF MESSAGES



(57) Abstract: The invention features an apparatus and method for transmitting a file. The apparatus includes a file splitter that splits the file into a plurality of message segments. Each message segment includes an address of the destination. The apparatus also includes a file encapsulator. The file encapsulator encapsulates at least one of the plurality of message segments. The encapsulation conceals the address of the destination during transmission of the at least one encapsulated message segment to one or more trusted nodes. The trusted nodes retransmit the message segments to the destination for reassembly of the file at the destination.

WO 2002/062032 A3

METHOD AND SYSTEM FOR SECURE EXCHANGE OF MESSAGES

Cross-Reference to Related Case

This claims the benefit of and priority to U.S. Provisional Patent Application Serial No. 60/258,127, filed December 22, 2000, the entirety of which is incorporated herein by reference.

Technical Field

The invention generally relates to electronic communications, and, more particularly, to security in network-based communications.

Background Information

Message security is of particular concern in modern, network-based communications. Communications often occur between devices such as computers operating in a non-secure network, such as the Internet. It is generally desirable to protect communications from eavesdropping and tampering.

Generally, three approaches have been used to provide secure communications: a secure network; a secure host with security protocols; and encryption of communications. A secure network typically requires steps be taken to protect the network from intruders. Such steps can include special communications protocols or special hardware, for example, use of a secure, optical network backbone. In such cases, secure communications, if at all possible, are limited to the confines of the secure network.

The secure host approach includes installation of a security protocol on network host computers to monitor network communications. The protocol provides review and control of

network communications to guard against theft and tampering. This approach requires the host computers to implement a security protocol that operates at Layer 3 or 4 of the Open Systems Interconnection (OSI) model.

A variety of encryption devices or software tools can protect data communications from theft and tampering. For example, keyed encryption techniques are common. Such techniques typically require that a sender and a recipient of a message share some information regarding an encryption algorithm and encryption/decryption key to enable the recipient to de-encrypt a message.

Message packet headers are particularly vulnerable to tampering because the packet header typically cannot be encrypted. Variants of the above general schemes have been proposed to respond to this problem. Further, message packets can be modified to enable detection of tampering and hence the potential of an altered message packet. Alternatively, a message can be disguised to appear as an ordinary message to fool an eavesdropper. The ordinary appearing message would have a distinct meaning to a recipient based on prior agreement between the sender and the recipient.

The above described approaches to message security are ineffective when a secure network or encryption methods are unavailable or not desired.

Summary of the Invention

The invention generally involves secure data transmission over a network. The invention is particularly suited to message transmission over a network that has multiple pathways. Various embodiments of the invention can defeat eavesdroppers wishing to intercept or interfere with a message. A solution is provided for the problem of the publicly visible addresses that are typically associated with transmitted communications.

The invention is suited to protect various types of communications. The communications may be digital electronic communications and may include, for example, messages and data. The communications may be sent via a network in the form of packets. The network may be, for example, a wired, wireless or optical network. In the following discussion, the terms "communication", "message", "file" and "data" are all used to express the general idea of information transmitted between parties. The particular form that the information assumes during transmission may be binary, as found in modern digital communications.

Improved security is accomplished by use of one or more trusted intermediaries, i.e. nodes, to relay communications between parties, for example, a source and a destination. The ultimate destination of the communication is generally concealed from all but the intermediary. Thus, an intermediary receives a message or other communication from a source, examines the concealed address of the destination and forwards the communication to the destination.

When the intermediary forwards a communication, the source can be concealed while the destination address of the next trusted intermediary, which may be the final destination of the

packet, is now publicly observable. In this manner, an eavesdropper cannot simultaneously discern the source and destination of a communication.

An eavesdropper attempting to intercept a message sent between two parties must therefore overcome multiple difficulties. If an eavesdropper observes transmissions such as data packets leaving a source, it cannot correctly identify the ultimate or real destination of each data packet. If the eavesdropper observes data packets arriving at a destination, it cannot correctly identify the original source of each packet. Thus, an eavesdropper may be impeded from identifying messages sent from a particular original source to a particular final destination.

An intermediary can perform the same function for two-way or multi-party communications. The node can be, for example, a network node. The node can be a computer server or a radio transceiver (e.g. a mobile telephone).

Splitting the message into message segments can make message interception and tampering more difficult. An eavesdropper must then intercept multiple segments to obtain the message, and still will not know the source or the destination. To further complicate interception, the ultimate destination addresses of the segments can be concealed when the segments are transmitted to one or more trusted nodes. An eavesdropper seeking messages or segments addressed to a particular destination may then only perceive the message segments as being addressed to the intermediary, and thus fail to intercept them.

Moreover, increasing the number of pathways used for transmission of message segments or data packets provides additional security. An eavesdropper must then monitor and intercept communications along multiple pathways to attempt to obtain all the message segments required for reconstruction of a

message. Message segments can be encrypted to impede an eavesdropper still further.

Accordingly, in a first aspect, the invention features an apparatus for transmitting a file. The file can include data or a message, or both. It can be in binary form, as for a typical computer data file. It can be a file of any form as utilized in electronic, electro-magnetic, and optical network-based communications. The apparatus includes a file splitter that splits the file into a plurality of message segments. Each message segment includes an address of the destination.

The term "transmit" as used herein means the directing of a file from any source location to any destination location. The actual transmission of a file may occur via all suitable techniques of file transfer, including, but not limited to, standard file-transfer protocols via an electronic or optical network.

The apparatus also includes a file encapsulator. The file encapsulator encapsulates at least one of the plurality of message segments. The encapsulation conceals the address of the true origin and ultimate destination during transmission of at least one encapsulated message segment to one or more trusted nodes. The trusted nodes may re-encapsulate the message and retransmit the message segments to the destination for reassembly of the file at the final destination.

The file splitter may also include a file converter. The file converter converts the file into N message segments. The file can be reassembled from a subset of any M of the message segments, where N and M are positive integers, and $N > M \geq 1$.

The apparatus may further include a file encoder. The file encoder encodes the file prior to splitting of the file by the file splitter.

The file encoder, file encapsulator and file splitter may include, for example, integrated circuits, such as microprocessors. A single integrated circuit or microprocessor may include the file encoder, file encapsulator and file splitter. One or more microprocessors may implement software that enables the functioning of the file encoder, file encapsulator or file splitter. Any of the file encapsulator, the file splitter and the file encoder may be implemented in software, firmware or hardware (e.g. as an application-specific integrated circuit). The software may be designed to run on general-purpose equipment or specialized processors dedicated to the functionality herein described.

In second aspect, the invention involves a method of secure transmission of a file from a source to a destination. The method includes splitting the file into a plurality of message segments. Each message segment includes an address of the destination.

The method further includes encapsulating at least one of the plurality of message segments to conceal the address of the origin and destination. At least one encapsulated message segment is transmitted to one or more trusted nodes. The one or more trusted nodes retransmit at least one message segment to the destination for reassembly of the file at the destination.

The process of splitting the file may include converting the file into N message segments. The N message segments may enable reassembly of the file from a subset of any M of the message segments, where N and M are positive integers, and $N > M \geq 1$.

Retransmitting at least one message segment may include transmitting at least M of the N message segments to the destination. The file can be reassembled after at least M of the N message segments arrive at the destination.

Transmitting to one or more trusted nodes may include

transmitting more than one message segment via multiple pathways of a communications network. In another embodiment, the method further includes encoding the file. Encoding the file may include enciphering the file.

Encapsulating at least one message segment may include enciphering at least one of the message segments. Encapsulating may further include adding forwarding instructions to the message segment. The forwarding instructions instruct one of the trusted nodes to forward the message segment towards the destination. The forwarding instructions may include the address of the destination. Encapsulating may further include addressing each one of the plurality of message segments to one of the plurality of trusted nodes.

The foregoing and other objects, aspects, features, and advantages of the invention will become more apparent from the following description and from the claims.

Brief Description of the Drawings

In the drawings, like reference characters generally refer to the same parts throughout the different views. Also, the drawings are not necessarily to scale, emphasis instead generally being placed upon illustrating the principles of the invention.

FIG. 1 illustrates an embodiment of a communication of a message from a source to a destination.

FIG. 2 illustrates an embodiment of a communication of a message that provides improved message security.

FIG. 3 illustrates an embodiment of a method that provides message delivery assurance and security.

FIG. 4 illustrates an embodiment of spatial diversification of message transmission, which transmits split message segments along three paths through a network.

FIG. 5 illustrates an embodiment of reassembly of a message at a destination.

FIG. 6 illustrates an embodiment where obstruction of a single node does not deny message transmission.

FIG. 7 illustrates an embodiment where eavesdropping on a single link provides no information.

FIG. 8 illustrates an embodiment with integration of data encryption into an encoder and a decoder.

FIG. 9 illustrates an embodiment with integration of data encryption into the a splitter and a assembler.

FIG. 10 illustrates an embodiment of an apparatus for transmitting a file via a communications network.

FIG. 11 illustrates an embodiment of N message segment identifiers attached to N message segments.

FIG. 12 illustrates an embodiment of an apparatus for transmitting a file.

FIG. 13 illustrates an embodiment of an encapsulated message segment addressed to a trusted node.

FIG. 14 illustrates an embodiment of a message segment addressed to a destination.

Description

The terms "file", "message", "data" and "data file" are herein understood to refer to any entity of data that may be transferred via analog or digital means. The entity may originate in analog or digital form, and, at various times, may be stored in analog or digital form. The entity is capable of transfer between two distinct physical locations via, in

particular, electronic, wireless and optically based communications.

Although, as explained above, the present invention may be applied to any form of data or message, particularly high security can be achieved by splitting a message into multiple segments sent over different network pathways. At the same time, this approach also involves a greater degree of complexity than applications utilizing a single pathway.

Accordingly, for purposes of explanation, an advantageous technique of message splitting for multiple-pathway networks is described below in the section labeled "I". Then, in the section labeled "II", further embodiments of the invention are described, which have particular utility in connection with transmission of split messages via a single pathway or via multiple pathways.

I. Message Splitting and Spatially Diversified Message Routing for Increasing Transmission Assurance and Data Security Over Distributed Networks

An apparatus and method for data assurance in communication networks makes advantageous use of aspects of networked communication. Though the below discussion is applicable to communication networks generally, several embodiments are given for mobile ad-hoc networks (MANET), since some features are preferably applied to MANETs.

During a typical communications session (between, e.g., an originating node and a destination node), messages can be forwarded along multiple, variable data paths. Aggregation of a number of such paths forms a single "super path." In one embodiment, a method includes encoding a message, splitting the encoded result into distinct message segments, and sending each segment along a different path. A receiving node may reconstruct the original message without the requirement that all message

segments eventually reach the receiving node after traveling along their individual paths.

One embodiment includes a protocol that enables a sender to provide information to a destination, i.e., receiver node, about encoding and splitting algorithms that were used to process a message. Some embodiments include methods for inferring the status of the collection of links. Some embodiments include one or more algorithms for determining which combination of encoding and splitting algorithms to use in response to a current status of the links.

Hence, some embodiments enable dynamic adjustment in response to changing network communication conditions, in particular for a MANET. One such embodiment includes a set of encoding/decoding algorithms and a set of splitting/reassembling algorithms to permit an optimized response to the dynamic variations in the link characteristics. Modified algorithms can incorporate data security enhancement features.

For example, encoding algorithms may be used to prevent the deduction of any part of the original message from individual processed message segments. A minimum number of message segments may be required to reconstruct the original message. Further, encryption keys may be used to enhance security. In particular, security enhancement can be achieved by deterministically varying a set of splitting/reassembling algorithms.

Data assurance in networks can be adjusted to a desired level by choosing an appropriate encoding and splitting scheme to tolerate failures over a sufficiently large number of paths. Encoding redundancy can reduce or eliminate the need for message retransmission. Message delay may be reduced, and utilization of each link in the network may be increased. Generally, the benefit in overall network resource utilization and performance grows with the number of links, i.e., the number of directly

communicating node-pair combinations, and the expected number of relaying hops through which a packet is forwarded towards its destination.

In one aspect, the apparatus and method improve data security. As multiple message segments are required to decode the original message, an eavesdropper sniffing, e.g., packets traveling on a particular path cannot deduce much useful information. Additional security components or steps can improve the level of data security; for example, encoding mechanisms can be chosen to avoid exposing the original data bits directly and a bit-position scrambling mechanism can be incorporated before splitting of the message. This provides security gains that require almost no increase in system complexity or computational burden.

In one embodiment, a redundantly encoded message is transmitted by aggregating multiple paths in a MANET to form a single super-path. This aggregation provides robustness in view of the potentially drastic variation in individual links. The super-path has a collective characteristic that improves stability, and statistically resembles a fixed link pathway in comparison to a pathway through a conventional MANET.

The channel coding technique may first encode the message to inject the desired level of redundancy into the message, then split the encoded message into multiple segments, and then forward each segment along a different path. At the receiving end, the extra redundancy injected by the encoding method (via, e.g., erasure correcting codes) may permit reassembly of the original message without requiring the successful delivery of all message segments through their individual paths.

Encoding methods may be used to improve the data assurance to a desired level for a network, or example, a MANET. This is more effective for MANET-based communications than simply

adopting or adapting the two-pronged approach of fixed point-to-point channels (and conventional networks). The characteristics of the aggregated super-path more closely resemble that of the fixed point-to-point channel than that of the individual member paths in the aggregate. Moreover, the variation in the characteristics of the super-path is slower than the variation of individual member paths, and can be designed to become tractable.

As a result, the variation of super-path characteristics can become more sensitive to network communications congestion than to link-to-link communication variations, e.g., radio frequency channel variations, arising from movement of the nodes. Hence, in one embodiment, super-path characteristics are regularly or continuously analyzed, and encoding and splitting algorithms are selected from classes of encoding algorithms and splitting algorithms in response to a determined characteristic. Super-path characteristics may include, for example, the number of successfully received message segments and the identity of the paths through which message segments are successfully received.

The performance of these classes of algorithms can be rated. Protocols that implement measurement of super-path characteristics and dynamic selection of an optimum combination of encoding algorithms and splitting algorithms can also be rated. Rating of algorithms and protocols can permit improved optimization of selections.

Encoding and splitting of messages directly improves message security. Because the message segments are forwarded along distinct routes to the destination, an eavesdropper must simultaneously intercept multiple message segments before a successful recovery of the original message becomes possible. The mobility and the geographical distribution of the nodes in the network make this difficult, and splitting the message into more segments can increase the difficulty of recovery.

Furthermore, an encoding algorithm can be chosen that prevents message reconstruction without interception of at least a threshold portion of message segments.

Additional security is made possible by scrambling, even simple scrambling, of the positions of the encoded message bits, e.g. before splitting, to prevent message reconstruction by an eavesdropper even when the eavesdropper intercepts a sufficiently large number of message segments. Generally, scrambling and de-scrambling of bit positions requires many fewer operations to execute and complete than traditional encryption and decryption methods.

Some embodiments include a stand-alone protocol layer for insertion in the networking protocol layer. For example, the protocol layer can be inserted between the medium access control (MAC) layer and the networking layer of a communication system. The protocol layer may include mechanisms for monitoring or analyzing the characteristics of network links and a decision algorithm to dynamically choose one of a class of encoding and splitting algorithms based on the observed network link characteristics.

In one embodiment, when the link stability is low, the protocol layer switches to an encoding algorithm that tolerates more losses of the message segments and a message-splitting scheme that results in smaller segments, in an attempt to improve delivery assurance. In another embodiment, when the link stability improves, the protocol layer switches to an encoding algorithm that has requires more message segments to be received and a message-splitting scheme that uses larger segments, in an attempt to reduce the protocol overhead.

The impact of the proposed algorithm and the dynamic protocol can be measured at multiple levels of the network. The probability of delivery success in a single attempt can be

improved to any desired level by choosing an appropriate combination of encoding and splitting methods or algorithms. Generally, an entire message is not transmitted along a single path. Instead, a message is fragmented, i.e. split, and forwarded along multiple paths. The realized increase in data assurance general comes with an initial delay in transmission of message segments, or packets, due to the encoding and splitting. Generally, however, overall communications delays are improved because of the improved probability of completion of each message transmission in the first attempt.

Referring to **Figure 1**, an embodiment of a communication of a message from a source to a destination is illustrated. A message **1**, e.g., a block of message bits, is fed to an encoder **2**, e.g. a scrambling encoder. The encoder **2** injects redundancy into the message bit stream, which increases the number of bits in the message. The encoded message is fed to a message splitter **4**, which breaks the message into N message segments.

The N message segments are forwarded to the destination along different paths in a network **3**. An assembler **6** reassembles the encoded message as the segments are received. When the number of segments received reaches a specified threshold, a partially reassembled message is passed to a decoder **8**, e.g. an erasure decoder. The decoder recovers the original message **1**, using only the bits available from the partially assembled message. The threshold number of segments is determined by the selected coding scheme. Both the assembler **6** and the erasure decoder **8** may be implemented in hardware and/or as software modules.

Improving the probability of completed delivery of a message in a first attempt reduces both the average delay and the number of retransmissions required for deliver of messages through the network. Reducing the number of retransmissions decreases the

number of channel contentions in a network with multi-accessing nodes such as a MANET. This may significantly improve the utilization of both the links and the network, in terms of factors such as the number of data bits sent per usage of bandwidth, channel, link, battery power, etc. This in turn significantly improves the overall network throughput and efficiency.

Figure 2 illustrates an embodiment that provides improved message security. A sender **10** and a receiver **20** agree to use a combination of an encoding scheme and a splitting mechanism that splits each message into three segments for transmission via a MANET **23**. The MANET **23** includes several nodes **a-g**. The encoding scheme requires at least two message segments to reach the receiver for recovery of a split message. An eavesdropper is illustrated as intercepting message segments between nodes **c** and **e**; a jammer is illustrated as blocking transmission of message segments at node **f**. Three paths P_1, P_2, P_3 through the network **23** are a subset of all possible paths. Message security and integrity are maintained in spite of the efforts of the eavesdropper and the jammer.

The eavesdropper acquires only a message segment transmitted along path P_3. Because the number of message segments threshold is 2, the single segment does not provide any useful information to the eavesdropper. All three segments will reach the receiver **20**. The first two to arrive are used to reassemble the original message.

The jammer attacking node **f** prevents the message segment traveling on path P_3 from reaching the receiver **20**. The other two message segments, however, arrive, and the message is recovered. The jammer cannot prevent the receiver **20** from getting the message.

Several criteria may be used to assess the performance of alternative implementations of a decision algorithm and a dynamic protocol. Such criteria may include, for example:

- delivery assurance, the probability of successful receipt of a fully correct message (affected by the probability of link/node failure);
- security improvement, in terms of the number of message segments that must be acquired by an eavesdropper in order to reconstruct the original message; and
- improvement in effective bandwidth, the reduction in the number of required retransmissions as compared to, for example, the adaptation of the two-pronged approach to a MANET.

In one embodiment, a protocol is inserted into a network communications protocol stack, e.g., between the MAC and the networking layer. This protocol mechanism senses and predicts variations in the characteristics of the link aggregate, and dynamically chooses the best combination of encoding/decoding and splitting/reassembly algorithms from a set or class of algorithms. The attempt to optimize can seek a combination that adds the least overhead to achieve a specified probability of successful message delivery. The selection process may further include, e.g., consideration of message priority, other measures of message importance, or cost of latency.

Referring to **Figure 3**, one embodiment is illustrated of a method that provides message delivery assurance and security. The method includes encoding the message to inject redundancy into a message stream, and splitting the encoded message. The split, encoded message is forwarded along spatially diversified routes.

For example, a message, or message block, that includes k bits is processed through an encoder **2**, e.g., a scrambling encoder, that converts the message into an encoded message block of n bits, where n > k. A splitter **4** decomposes the output of the encoder **2** into N message segments, each segment including no more than [n/N] bits. "[n/N]" denotes the least integer greater than n/N. N, n and k are positive integers.

Figure 4 illustrates spatial diversification. Each of the N message segments is forwarded to the intended recipient, preferably along a different route. This gives spatial diversification to the routes used for transmission. Nodes **a-g** are a subset of network **23** nodes. The sender **10** forwards segments to the receiver **20** along path P_1 (including nodes **a** and **g**), path P_2 (including nodes **b** and **d**), and path P_3 (nodes **c**, **e**, and **f**). The different physical locations of the nodes forces the message segments to travel through different areas of the network. Link conditions and congestion in different areas may vary considerably.

Referring to **Figure 5**, the message segments are re-assembled as they are received at the receiver **20**. When a sufficiently large number of message segments is received, the partially assembled message is forwarded to a decoder **8**, e.g., an erasure decoder, which recovers the entire original message. Improved delivery assurance is achieved because not all message segments must be successfully received to permit the recipient to recover the original message.

In one embodiment, each message segment has a length of b, where $0 < b \leq [n/N]$. "[n/N]" denotes the least integer greater than n/N. Limitation of the value of b can assure that each encoded message bit exists in only one message segment. Because n must be greater than k, $[k/b] < N$. Hence, there are fewer than N segments when the shorter unencoded message is broken into

segments of length b. A longer, encoded message is obtained with N segments of length b.

The intended recipient can recover the original message with any subset of [k/b] segments of the N message segments, given an appropriate selection of the encoding scheme. Hence, the message recovery mechanism at the intended recipient can tolerate the loss of some of the message segments. This allows for losses due to, e.g., network congestion, broken links, interference or jamming. This may require n bits to be transmitted for every k message bits, where n > k. Advantages are realized, however, such as:

- n/k may be smaller than the number of bits that would be transmitted for each bit if an entire block is retransmitted; and
- the probability that the intended recipient correctly recovers the original message from a single transmission attempt is improved.

Examples of classes of error-correcting codes that can be utilized include Bose-Chaudhuri-Hocquenghem (BCH) codes, Convolutional codes, Hamming codes, Reed-Solomon codes, Golay codes, Turbo codes, and several other linear and nonlinear block codes.

Various embodiments provide significant security benefits. Referring to **Figure 6**, resistance to localized jamming is one benefit. Jamming, for example, disrupting transmission at a single network node or link, minimally impacts the functionality of the rest of the network. When a jammer located near node **f** has broken the continuity of path $\mathbf{P_3}$, path $\mathbf{P_1}$ and path $\mathbf{P_2}$ are still able to deliver message segments, and the message is successfully decoded. To be effective at disruption, a jammer must be located close enough to either the sender **10** or receiver

20 to jam a significant number of message segments. For example, the probability of disruption in a mobile, military network is reduced by the requirement for close proximity of a hostile jammer.

Referring to **Figure 7**, another security benefit of some embodiments is the difficulty an eavesdropper experiences when trying to intercept messages. As illustrated in **Figure 7**, an eavesdropper is physically located between node **c** and node **e**, able to copy any message segment, e.g., data packet, that passes along path P_3. The eavesdropper must correctly receive a minimum of [k/b] message segments to recover a complete message. To receive the minimum number of segments, however, requires eavesdropping on other paths P_1, P_2.

Some embodiments prevent even partial message recovery by the eavesdropper. An appropriately chosen scrambling encoder (e.g., a non-systematic code) can be used to create a condition during which any subset of q message segments, with $q < [k/b]$, will prove insufficient to recover any subset of the original message. Similar to the jammer, the eavesdropper must be physically located very close to either the sender **10** or the intended recipient **20** to effectively intercept segments from multiple paths P_1, P_2, P_3.

The effectiveness of a local jammer is reduced by taking advantage of the nature of a distributed networking environment. Similarly, a single eavesdropper has a reduced ability to observe enough segments to allow an understanding of the communications carried by the network. As a result, the overall security of information carried by the entire network is significantly improved.

Some embodiments further improve security through use of data encryption by means of bit position scrambling. The selection of a scrambling encoder can be controlled with an encryption key. In some alternative embodiments, the actual bit scrambling can be accomplished in either an encoder or a splitter.

Referring to **Figures 8** and **9**, embodiments that utilize permutation are illustrated. **Figure 8** schematically shows the use of permutation by an encoder **2a**. **Figure 9** shows the use of permutation by a splitter **4a**. For example, even a simple use of an encryption key to alter bit positions in the encoded message, would require the eavesdropper to potentially search through n! possibilities.

Some embodiments that include a scrambling encoder employ an encoding scheme that provides one or both of the following features:

- the encoding scheme provides strong resilience against loss of message segments, preferably having the value of (k + e) as close to n as possible, where e is the number of message segment losses that the scheme can overcome, k is the original message length, and n is the encoded message length; and
- no bits in the original message are ascertainable from any message subset below a threshold number; for linear block codes, this generally requires use of non- systematic codes and that approximately half of the elements of a generating matrix elements have a value of 1.

In order for the assembler at the receiving node to correctly reassemble the message fragments, the content of each segment must be identified. In one embodiment, the information required for reassembly is reduced by inclusion of a numbering

scheme for the message segments. In a preferred embodiment, a segment carries identification that is a number assigned by the message splitter. This number may be a field in a protocol header that is attached to each message segment, or embedded in the message segment itself.

Additional protocol header fields may be included when encoding and splitting algorithms are altered dynamically to better suit the observed characteristic variations of the super-path. The additional fields can carry measurement data regarding the characteristics of the super-path as well as data that informs the destination node of the changes in the encoding and splitting algorithms. Inclusion of additional protocol header fields incurs additional transmission bandwidth for every hop. Hence, it is preferable to optimize choices of fields to minimize the resulting bandwidth expansion.

Referring to **Figure 10**, an embodiment of an apparatus **30** for transmitting a file via a communications network is illustrated. The apparatus **30** includes a file processor **31**, which may be implemented in hardware and/or as a software module, and a message segment transmitter **32**. The file processor converts files into N message segments that enable reassembly of the file from a subset of any M of the message segments. N and M are positive integers and $N > M \geq 1$.

The message segment transmitter **32**, which may be implemented in hardware and/or as a software module, transmits message segments to a receiver. The receiver can reassemble a file after receiving M of the N message segments.

The file processor **31** may comprise a file encoder **35** and an encoded file splitter **36** that convert a file into N message segments. The file encoder **35** may implement a class of encoding

algorithms in generating the message segments. The encoded file splitter **36** may implement a class of splitting algorithms.

The processor **31** may further comprise a communications network analyzer **37**, which may be implemented in hardware and/or as a software module, that determines the condition of a communications network. The processor **31** may also include a message segment parameter selector **38** (which also may be implemented in hardware and/or as a software module) that selects a set of values for M and N based on the determined condition to achieve a preselected probability of a successful transmission of M of the transmitted message segments.

Referring to **Figure 11**, the apparatus may include N message segment identifiers **33** that have a one-to-one association with the N message segments **34**. In the embodiment illustrated in Figure 11, message segments **34** are transmitted with their associated identifiers **33** to assist in reassembly of the message. The identifiers **33** can include, for example alphanumeric data. In one embodiment, during transmission, the identifiers **33** are binary numbers.

The above described and various other embodiments are of particular value when applied, for example, to ad-hoc networks, MANETs and conventional packet networks with distributed routing algorithms. Particular value accrues when applied to MANETs that include moderately mobile units.

II. Method and System for Secure Exchange of Messages

The security of information carried by a network may be improved when a sender and recipient utilize a trusted node as an intermediary for exchange of communications. A trusted node may be selected for its ability to securely and reliably forward communications, such as messages, message segments and storage

segments. For example, rather than addressing every message segment to an intended recipient, a message sender may address one or more of the message segments to one or more trusted nodes. In preferred embodiments, forwarding instructions are included with the message segments to enable forwarding of the segments to the intended recipient.

Various embodiments may be used to obscure the origin and destination of a message. Message interception is very difficult for an eavesdropper tapping a communication link, even if the link is in close proximity to either the sender or recipient. To deduce the messages of a particular conversation, all messages or message segments received by, or leaving, the recipient (who may also be a sender) must be captured. Further, some or all of the communications may be encrypted to further complicate the eavesdropper's task. Increasing the number of trusted nodes can dramatically increase the difficulty of message interception.

Referring to **Figures 12-14**, one embodiment of an apparatus for transmitting a file includes a file splitter **71** that splits the file into a plurality of message segments **81**. Each message segment includes forwarding instructions **82**, e.g., an address of the destination. The transmission of message segments **81** may occur via all suitable techniques of file transfer, including, but not limited to, standard file-transfer protocols via an electronic or optical network.

The apparatus also includes a file encapsulator **73**. The file encapsulator **73** encapsulates at least one of the plurality of message segments **81**. The encapsulation **83** conceals the address of the destination during transmission of the encapsulated message segment **81** to one or more trusted nodes.

A trusted node address **84**, which is publicly visible, is attached to the encapsulated message segment **81** to permit transmission of the message segment **81** to the corresponding

trusted node. The trusted node re-encapsulates and retransmits the message segment **81**, in part by examining the forwarding instructions **82** and making the address of the next destination, which may be the final destination address **85**, visible to the network.

The file splitter **71** may also include a file converter. The file converter converts the file into N message segments that permit reassembly of the file from a subset of any M of the message segments, where N and M are positive integers, and $N > M \geq 1$.

The apparatus may further include a file encoder **72**. The file encoder **72** encodes the file prior to splitting of the file by the file splitter **71**.

The file encoder **72**, file encapsulator **73** and file splitter **71** may include, for example, integrated circuits, such as microprocessors. A single integrated circuit or microprocessor may include the file encoder **72**, file encapsulator **73** and file splitter **71**. One or more microprocessors may implement software that enables the functioning of the file encoder **72**, file encapsulator **73** or file splitter **71**. Any of the file encapsulator **73**, the file splitter **71** and the file encoder **72** may be implemented in software, firmware or hardware (e.g. as an application-specific integrated circuit). The software may be designed to run on general-purpose equipment or specialized processors dedicated to the functionality herein described.

An embodiment of a method of secure transmission of a file from a source to a destination includes splitting the file into a plurality of message segments. Each message segment includes an address of the destination. The method may further include encoding the file. Encoding the file may include enciphering the file.

The process of splitting the file may include converting the file into N message segments. The N message segments may enable reassembly of the file from a subset of any M of the message segments, where N and M are positive integers, and $N > M \geq 1$.

The method also includes encapsulating at least one of the plurality of message segments to conceal the address of the destination. At least one encapsulated message segment is transmitted to one or more trusted nodes. Message segments may be transmitted via multiple pathways of a communications network.

The one or more trusted nodes retransmit the message segment to the destination for reassembly of the file at the destination. Retransmitting at least one message segment may include transmitting at least M of the N message segments to the destination. The message segment may be encapsulated during transmission from the trusted node to another trusted node or to the destination. The file can be reassembled after at least M of the N message segments arrive at the destination.

Encapsulating a message segment may include enciphering the message segments. Encapsulating may further include adding forwarding instructions to the message segment. The forwarding instructions instruct a receiving one of the trusted nodes to forward the message segment toward the destination. The forwarding instructions may include the address of the destination. Encapsulating may further include addressing each one of the plurality of message segments to one of the plurality of trusted nodes.

Some embodiments of a method of secure transmission of a file from a source to a destination include two or more stages of file splitting. In these embodiments, one or more message segments from a first file splitting step may be further split into additional message segments. A second splitting step may be advantageous, for example, when a node that transmits files via a

network has limited access to the network. For example, a node that transmits files via the Internet may have limited gateway access. The access may be limited, for example, to as few as one or two gateways.

The node might then split a file into a few message segments, for example three message segments, and transmit the message segments to the gateways. The gateways could further split one or more of the three message segments, and then forward message segments toward a destination via the Internet.

In some embodiments of a method, which include multiple splitting steps, the file is converted into N message segments that enable reassembly of the file from a subset of any M of the message segments. At least M of the N message segments are transmitted toward a destination for reassembly of the file after receiving M of the N message segments.

At least one of the transmitted segments is further converted into N_2 message segments that enable reassembly of the at least one message segment from a subset of any M_2 of the N_2 message segments, where N_2 and M_2 are positive integers and $N_2 > M_2 \geq 1$. At least M_2 of the N_2 message segments are transmitted toward the destination for reassembly of the at least one message segment prior to reassembly of the file.

The at least M_2 segments may be reassembled at the destination. Alternatively, the at least M_2 segments may be received and reassembled by an intermediate node. The reassembled segment may then be transmitted toward the final destination. Additional conversion steps and/or reassembly steps may be included at intermediate nodes in the network.

Various embodiments of the method and apparatus for secure exchange of messages may be applied to network-based communications. Relevant networks include, but are not limited to, local-area networks (LAN) or a wide area networks (WAN) such

as the Internet or the World Wide Web. Senders and receivers can be connected to a WAN either directly or via a LAN through a variety of connections including standard telephone lines, LAN or WAN links (e.g., T1, T3, 56kb, X.25), broadband connections (ISDN, DSL, Frame Relay, ATM), and wireless connections. The connections can be established using a variety of communication protocols (e.g., TCP/IP, IPX, SPX, NetBIOS, Ethernet, RS232, and direct asynchronous connections).

In some embodiments, the sender and receiver are comprised of appropriate computer hardware. Examples of such hardware include any personal computer (e.g., Windows or Macintosh operating system computer), Windows-based terminal, Network Computer, wireless device, information appliance, RISC Power PC device, X-device, workstation, mini computer, main frame computer or other computing device.

Alternatively, the sender or receiver can be a portable computing device such as a PDA or cell phone. As a further alternative, the sender or receiver can be any terminal (windows or non-windows based), or thin-client device operating according to a server-based computing model.

Variations, modifications, and other implementations of what is described herein will occur to those of ordinary skill in the art without departing from the spirit and the scope of the invention as claimed. Accordingly, the invention is to be defined not by the preceding illustrative description but instead by the spirit and scope of the following claims.

What is claimed is:

CLAIMS

1. An apparatus for transmitting a file, comprising:
   a file splitter that splits the file into a plurality of message segments, each message segment including an address of the destination; and
   a file encapsulator that encapsulates at least one of the plurality of message segments to conceal the address of the destination during transmission of at least one encapsulated message segment to one or more trusted nodes for retransmission by the one or more trusted nodes toward the destination for reassembly of the file at the destination.

2. The apparatus of claim 1 wherein the file splitter comprises a file converter that converts the file into N message segments that enable reassembly of the file from a subset of any M of the message segments, where N and M are positive integers, and $N > M \geq 1$.

3. The apparatus of claim 1 wherein a single processor includes the file splitter and the file encapsulator.

4. The apparatus of claim 1 further comprising a file encoder that encodes the file prior to splitting of the file by the file splitter.

5. A method of secure transmission of a file from a source to a destination, comprising the steps of:
   splitting the file into a plurality of message segments, each message segment including an address of the destination;
   encapsulating at least one of the plurality of message segments to conceal the address of the destination;
   transmitting at least one encapsulated message segment to one or more trusted nodes; and

causing retransmission of the at least one of the plurality of message segments from the one or more trusted nodes toward the destination for reassembly of the file at the destination.

6. The method claim 5 wherein the step of splitting the file comprises the step of converting the file into N message segments that enable reassembly of the file from a subset of any M of the message segments, where N and M are positive integers, and $N > M \geq 1$.

7. The method of claim 6 wherein the step of causing retransmission comprises causing splitting of the at least one message segment into N_2 message segments that enable reassembly of the at least one message segment from a subset of any M_2 of the N_2 message segments, where N_2 and M_2 are positive integers and $N_2 > M_2 \geq 1$; and causing transmission of at least M_2 of the N_2 message segments toward the destination for reassembly of the at least one message segment prior to reassembly of the file.

8. The method of claim 6 wherein the step of causing retransmission comprises the step of transmitting at least M of the N message segments to the destination for reassembly of the file after at least M of the N message segments arrive at the destination.

9. The method of claim 5 wherein the step of transmitting comprises the step of transmitting more than one message segment via multiple pathways of a communications network.

10. The method of claim 5 further comprising the step of encoding the file prior to transmission.

11. The method of claim 10 wherein the step of encoding the file comprises the step of enciphering the file.

12. The method of claim 5 wherein the step of encapsulating at least one of the plurality of message segments comprises the step of enciphering the at least one of the plurality of message segments.

13. The method of claim 5 wherein the step of encapsulating at least one of the plurality of message segments comprises the step of adding forwarding instructions to at least one of the plurality of message segments to instruct a receiving one of the plurality of trusted nodes to forward at least one of the plurality of message segments toward the destination.

14. The method of claim 5 wherein the step of encapsulating at least one of the plurality of message segments comprises the step of addressing each one of the plurality of message segments to one of the plurality of trusted nodes.

15. The method of claim 5 wherein the step of causing retransmission comprises causing splitting of the at least one of the plurality of message segments into a second plurality of message segments including an address of the destination; and causing transmission of the second plurality of message segments toward the destination.

16. The method of claim 15 further comprising the steps of causing reassembly of the at least one message segment; and causing transmission of the at least one reassembled message segment toward the receiver.

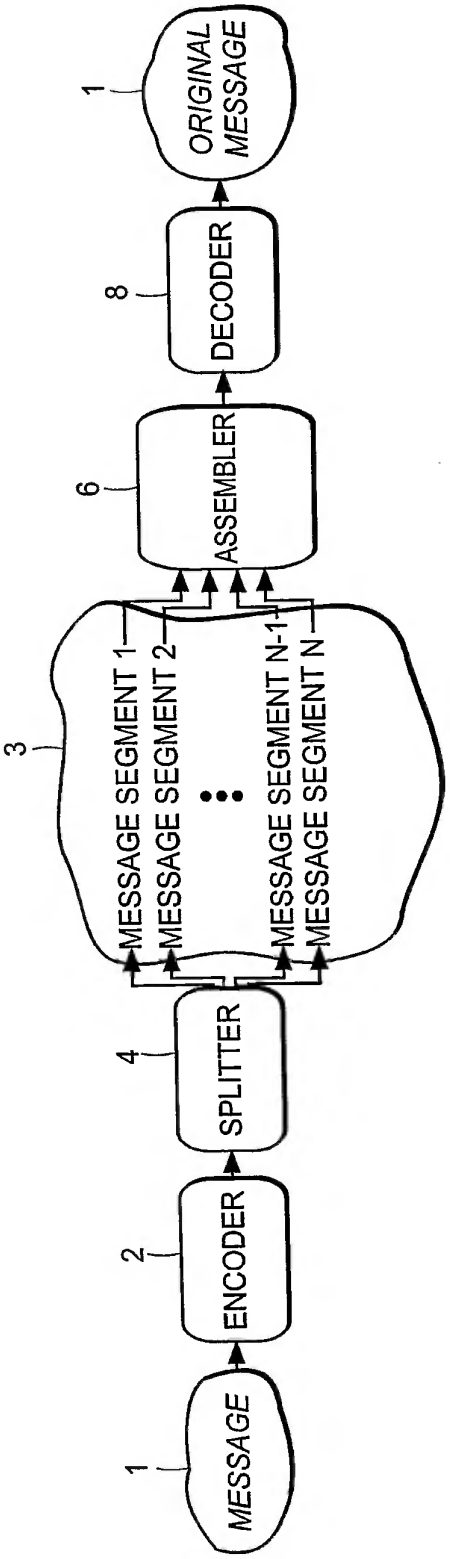

1
MESSAGE
2
ENCODER
4
SPLITTER
3
MESSAGE SEGMENT 1
MESSAGE SEGMENT 2
MESSAGE SEGMENT N-1
MESSAGE SEGMENT N
6
ASSEMBLER
8
DECODER
1
ORIGINAL MESSAGE

FIG. 1

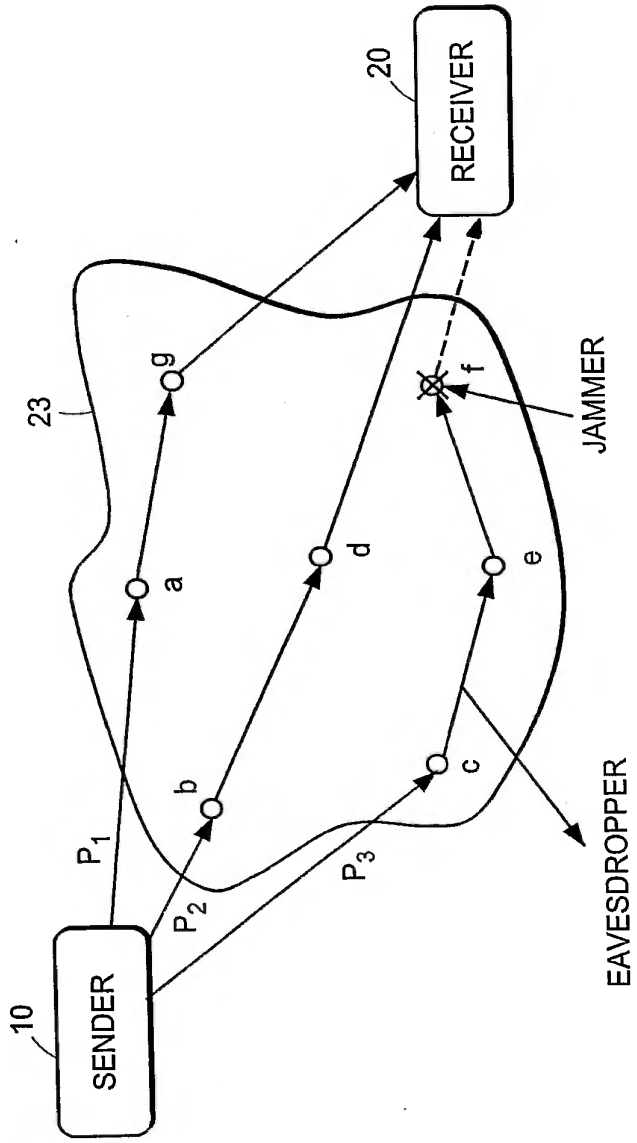

RECEIVER
20
23
g
f
JAMMER
a
d
e
b
c
P1
P2
P3
EAVESDROPPER
SENDER
10

FIG. 2

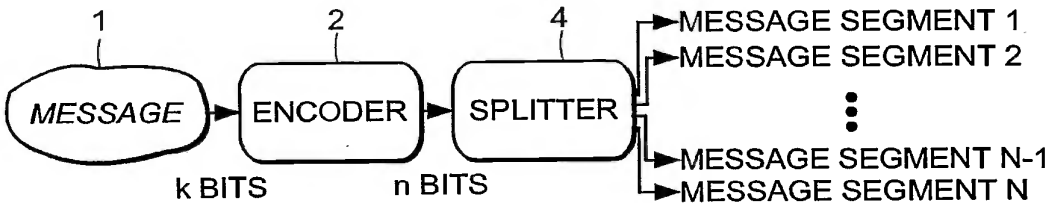

1
2
4
MESSAGE
ENCODER
SPLITTER
MESSAGE SEGMENT 1
MESSAGE SEGMENT 2
MESSAGE SEGMENT N-1
MESSAGE SEGMENT N
k BITS
n BITS

FIG. 3

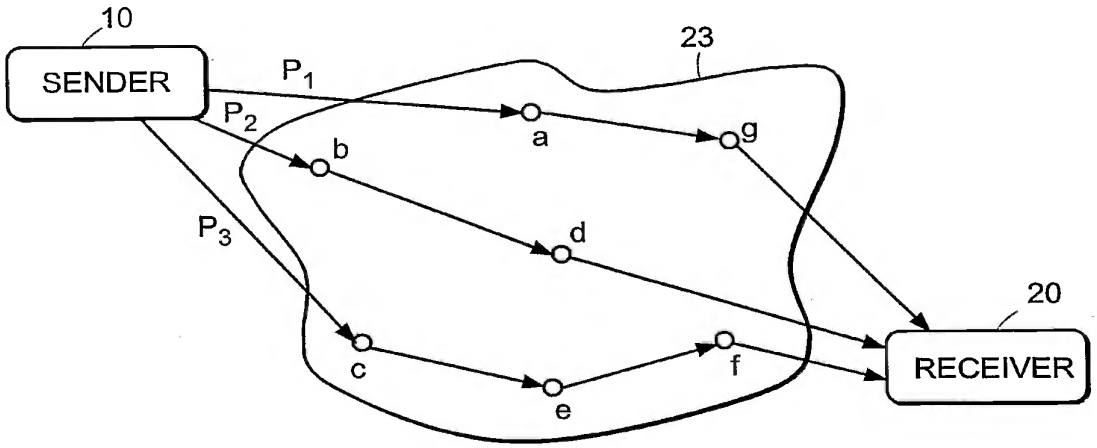

10
SENDER
P1
P2
P3
a
b
c
d
e
f
g
23
20
RECEIVER

FIG. 4

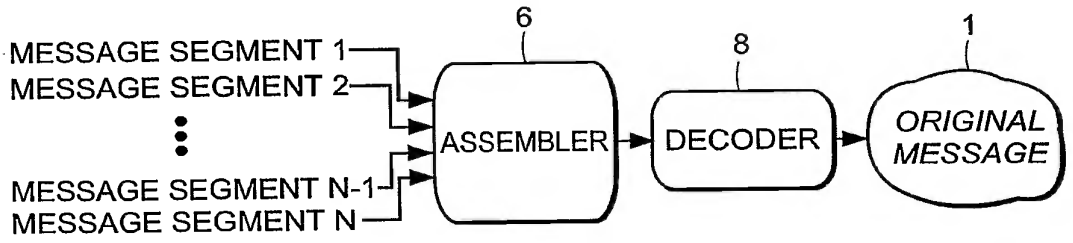

MESSAGE SEGMENT 1
MESSAGE SEGMENT 2
MESSAGE SEGMENT N-1
MESSAGE SEGMENT N
6
ASSEMBLER
8
DECODER
1
ORIGINAL MESSAGE

FIG. 5

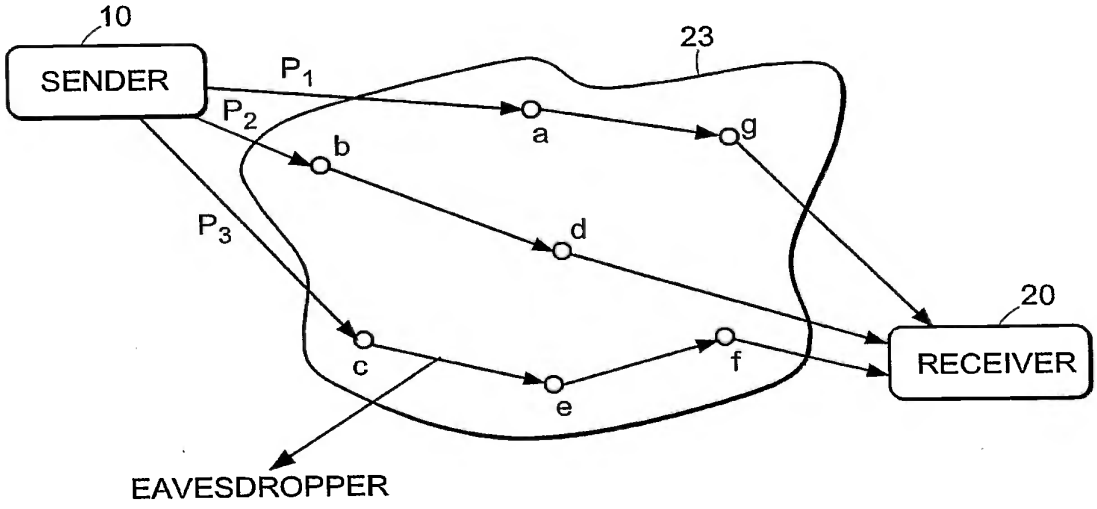

10
SENDER
P1
P2
P3
23
a
b
c
d
e
f
g
20
RECEIVER
EAVESDROPPER

FIG. 7

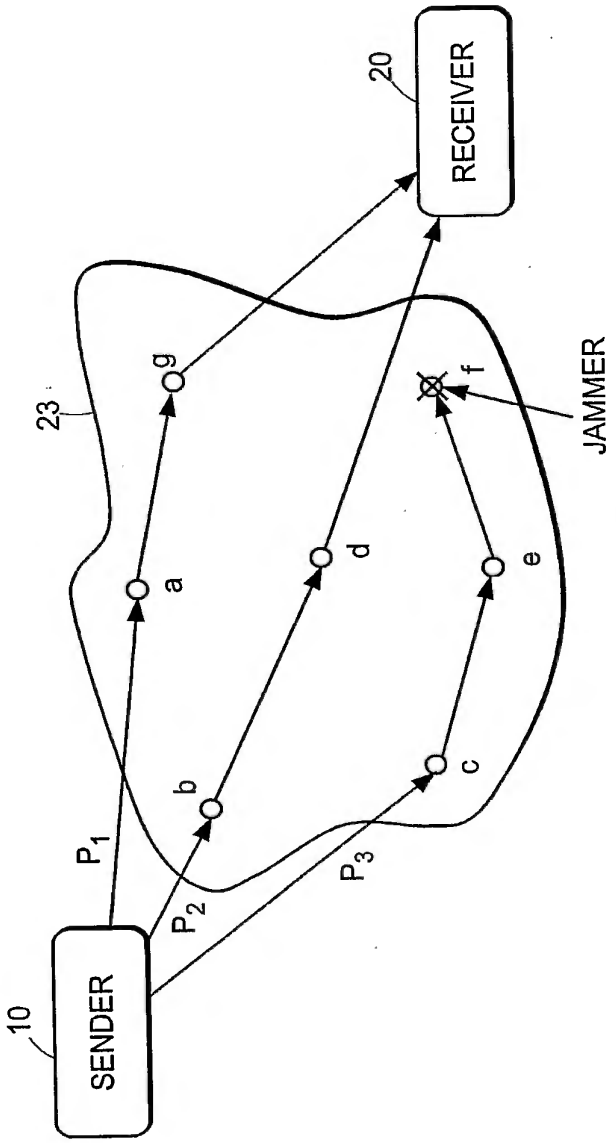


FIG. 6

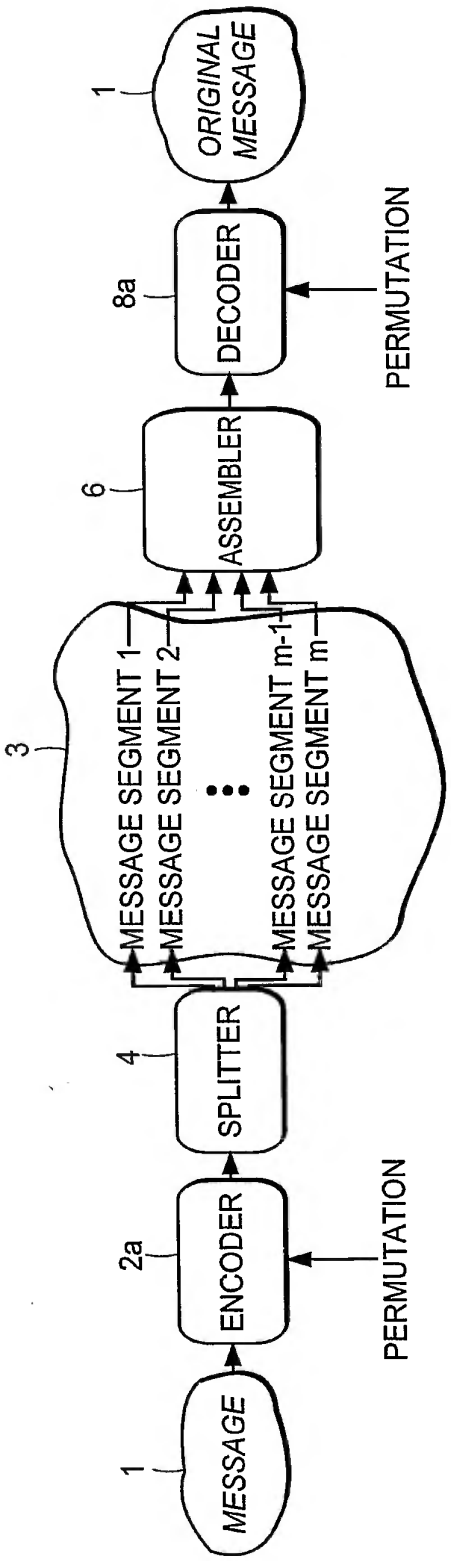

1
MESSAGE
2a
ENCODER
PERMUTATION
4
SPLITTER
3
MESSAGE SEGMENT 1
MESSAGE SEGMENT 2
MESSAGE SEGMENT m-1
MESSAGE SEGMENT m
6
ASSEMBLER
8a
DECODER
PERMUTATION
1
ORIGINAL MESSAGE

FIG. 8

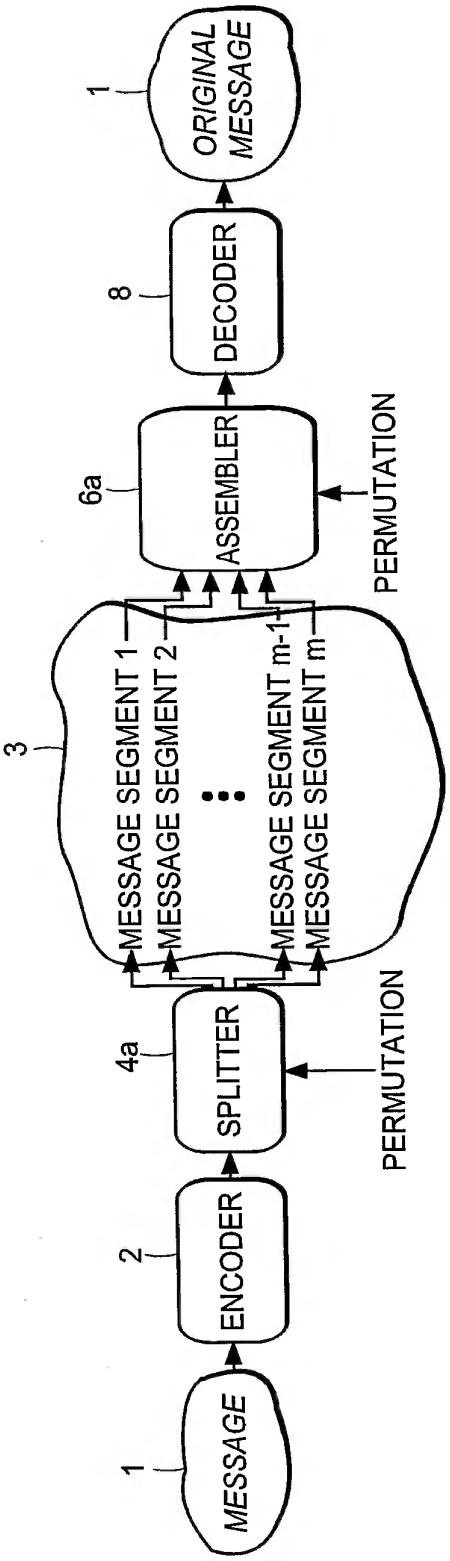

1
MESSAGE
2
ENCODER
4a
SPLITTER
PERMUTATION
3
MESSAGE SEGMENT 1
MESSAGE SEGMENT 2
MESSAGE SEGMENT m-1
MESSAGE SEGMENT m
6a
ASSEMBLER
PERMUTATION
8
DECODER
1
ORIGINAL MESSAGE

FIG. 9

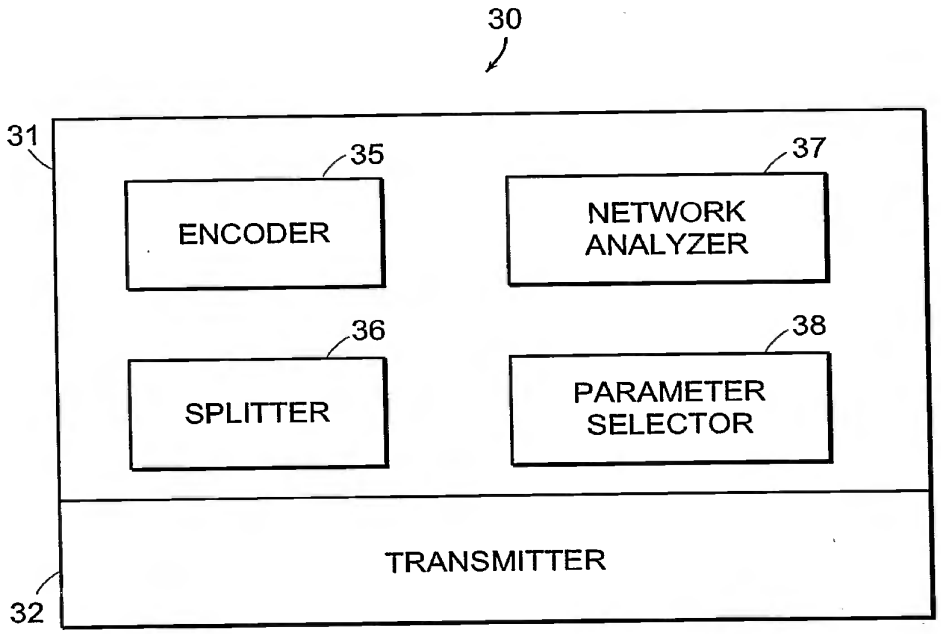

30
31
35
ENCODER
37
NETWORK ANALYZER
36
SPLITTER
38
PARAMETER SELECTOR
TRANSMITTER
32

FIG. 10

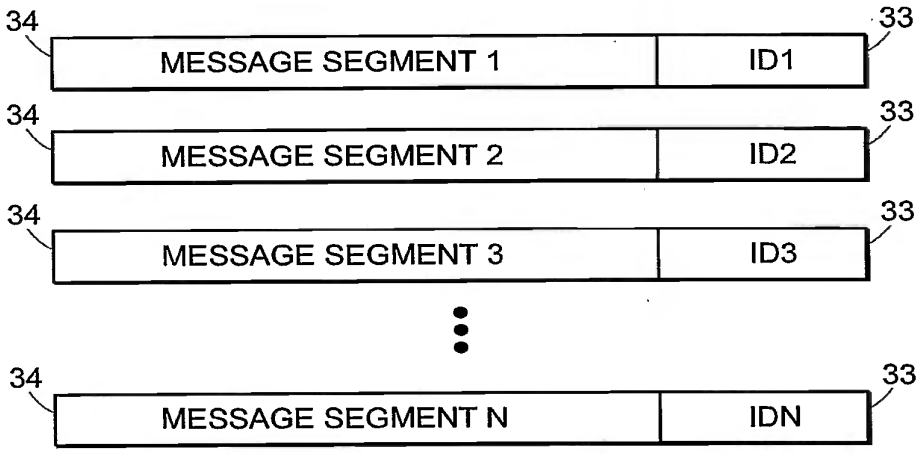

34
MESSAGE SEGMENT 1
ID1
33
34
MESSAGE SEGMENT 2
ID2
33
34
MESSAGE SEGMENT 3
ID3
33
34
MESSAGE SEGMENT N
IDN
33

FIG. 11

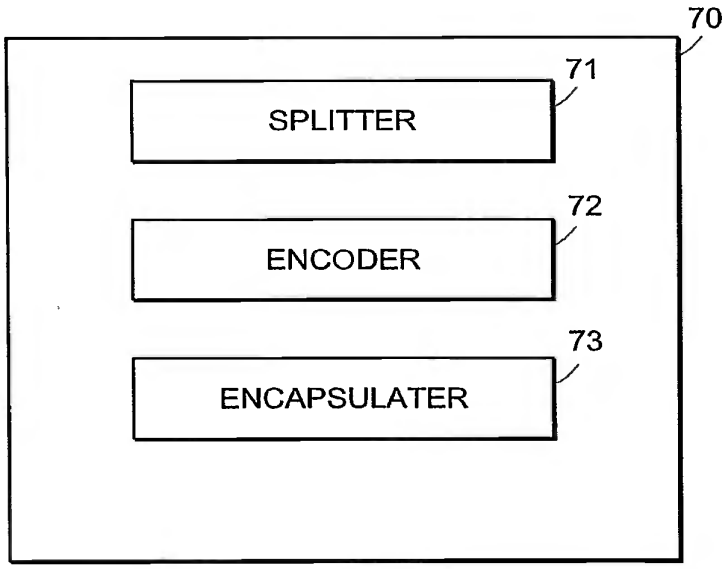


FIG. 12

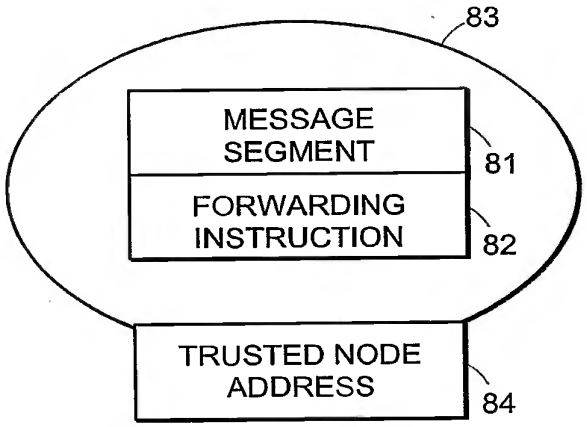

83
MESSAGE SEGMENT
81
FORWARDING INSTRUCTION
82
TRUSTED NODE ADDRESS
84

FIG. 13

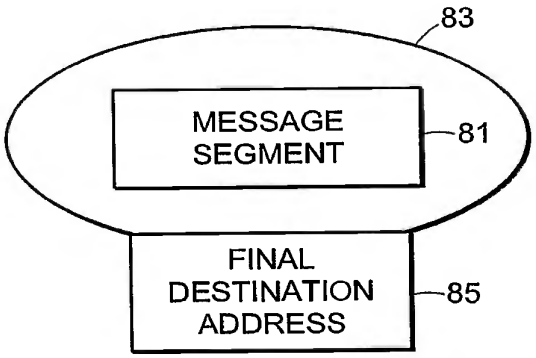

83
MESSAGE SEGMENT
81
FINAL DESTINATION ADDRESS
85

FIG. 14

INTERNATIONAL SEARCH REPORT

Int al Application No
PCT/US 01/50069

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04L29/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 00 27086 A (SCIENCE APPLICATIONS INTERNATIONAL CORPORATION) 11 May 2000 (2000-05-11)	1,3-5, 10-12
Y	claim 61	9
Y	MAXEMCHUK N F: "DISPERSITY ROUTING IN HIGH-SPEED NETWORKS" COMPUTER NETWORKS AND ISDN SYSTEMS, NORTH HOLLAND PUBLISHING. AMSTERDAM, NL, vol. 25, 1993, pages 645-661, XP000570119 ISSN: 0169-7552	9
A	page 645, left-hand column, paragraph 1 page 646, line R, paragraph 4 -page 647, left-hand column, paragraph 1	1-8, 10-16

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 November 2002	26/11/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Veen, G

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

information on patent family members

Int al Application No
PCT/US 01/50069

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0027086 A	11-05-2000	AU 1455300 A	22-05-2000
		AU 1600300 A	22-05-2000
		EP 1125414 A2	22-08-2001
		EP 1125419 A2	22-08-2001
		JP 2002529965 T	10-09-2002
		JP 2002529779 T	10-09-2002
		WO 0186911 A2	15-11-2001
		US 2002161925 A1	31-10-2002
		US 2002161884 A1	31-10-2002
		WO 0027090 A2	11-05-2000
		WO 0027086 A2	11-05-2000

Form PCT/ISA/210 (patent family annex) (July 1992)

Electronic Acknowledgement Receipt

EFS ID:	13142640
Application Number:	13371363
International Application Number:	
Confirmation Number:	7984
Title of Invention:	SECURE DATA PARSER METHOD AND SYSTEM
First Named Inventor/Applicant Name:	Rick L. Orsini
Customer Number:	1473
Filer:	Matthew Sammuel Bertenthal/Joanne Ryan
Filer Authorized By:	Matthew Sammuel Bertenthal
Attorney Docket Number:	104093-0002-105
Receipt Date:	29-JUN-2012
Filing Date:	10-FEB-2012
Time Stamp:	14:50:07
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$180
RAM confirmation Number	1566
Deposit Account	061075
Authorized User	

File Listing:

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

1		104093-0002-105_NonFinal_Response.pdf	107904 24ccf719b8c056688eb57cf2c567d7cd10742d63	yes	6

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Specification	2	2
Applicant Arguments/Remarks Made in an Amendment	3	6

Warnings:

Information:

2	Transmittal Letter	104093-0002-105_IDS.pdf	78829 19d13332c25382089fe7b601f061066afd4295b7	no	3

Warnings:

Information:

3	Information Disclosure Statement (IDS) Form (SB08)	104093-0002-105_SB08.pdf	136987 ae0a502410c6a048c522baf3ddb41a8bd72691375	no	3

Warnings:

Information:

This is not an USPTO supplied IDS fillable form

4	Foreign Reference	WO02062032.pdf	3499042 4f697a352b35360daafef94f9be0a9380b5120f5	no	87

Warnings:

Information:

5	Foreign Reference	WO2010057181.pdf	3508045 3e58f58909052163f3c2ec9198b36da5faf4c047	no	97

Warnings:

Information:

6	Non Patent Literature	Haniotakis_et_al_Security_Enhancement_Through_Multiple_Path_Transmission.pdf	297168 a15cbb2765c5f8B957ce020de3e1a619d5bb5816	no	5

Warnings:

Information:

7	Non Patent Literature	Rivest_All-Or-Nothing_Encryption.pdf	411184 3809730611a71cbc7c5f81ceb590a7b3c081431a	no	9

Warnings:

Information:

8	Non Patent Literature	12148365_OAs_Appeal_Brief_Replies.pdf	3871911 8637db23a14348fc57c02e69eed3f7400802c1bf	no	98
Warnings:					
Information:					
9	Non Patent Literature	13024791_Office_Actions_and_Replies.pdf	1585043 d1162058569caf200b4764b1d1e55ecf489f07e1	no	38
Warnings:					
Information:					
10	Non Patent Literature	13024804_NonFinal_Office_Action.pdf	1666555 f3cd9eb6839726c2267825dd77b9a87612fc695e	no	36
Warnings:					
Information:					
11	Non Patent Literature	13371361_NonFinal_Office_Action.pdf	1060443 e6ec3e51db4710749b089430c30a60836a8df784	no	23
Warnings:					
Information:					
12	Non Patent Literature	13371364_NonFinal_Office_Action.pdf	1702734 a55470b47ec874926662dbeee5d85ae4a506aab5	no	36
Warnings:					
Information:					
13	Non Patent Literature	13399923_NonFinal_Office_Action.pdf	955314 03d857ea7e1f010d1f99986b29edae9d867e7348	no	19
Warnings:					
Information:					
14	Fee Worksheet (SB06)	fee-info.pdf	30549 a24d7c1996bae2c30a40ba937268b163bd133fe8	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	18911708	

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/SB/06 (07-06)
Approved for use through 1/31/2007. 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	Filing Date	☐ To be Mailed
13/371,363	02/10/2012	

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	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT		(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 ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
	06/29/2012									
	Total (37 CFR 1.16(i))	* 27	Minus	** 27	= 0	X $ =		OR	X $60=	0
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $ =		OR	X $250=	0
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	0

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)	OR	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							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 number found in the appropriate box in column 1.

Legal Instrument Examiner:
/LINDA BADIE/

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/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 3

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

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
		US-8,151,333	04-03-2012	Zhu et al.	
		US-7,693,992	04-06-2010	Watson	
		US-7,472,105	12-30-2008	Staddon et al.	
		US-7,444,421	10-28-2008	Katayama	
		US-7,428,751	09-23-2008	Oom Temudo de Castro et al.	
		US-7,412,462	08-12-2008	Margolus et al.	
		US-7,304,990	12-04-2007	Rajwan	
		US-7,302,583	11-27-2007	Forrest	
		US-7,277,958	10-02-2007	Chung et al.	
		US-7,174,385	02-06-2007	Li	
		US-7,143,289	11-28-2006	Denning et al.	
		US-6,819,766	11-16-2004	Weidong	
		US-6,269,432	07-31-2001	Smith	
		US-6,118,874	09-12-2000	Okamoto et al.	
		US-5,937,066	08-10-1999	Gennaro et al.	
		US-5,450,099	09-12-1995	Stephenson et al.	
		US-2012/0072723	03-22-2012	Orsini et al.	
		US-20030084020	05-01-2003	Shu	
		US-6,192,472	02-20-2001	Garay et al.	

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]
		WO-02/062032	08-08-2002	The Charles Stark Draper Laboratory, Inc.		
		WO-10/057181	05-20-2010	Unisys Corp.		

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. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [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.

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 3

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

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
		US-2002/0129245	09-12-2002	Cassagnol et al.	
		US-6,363,481	03-26-2002	Hardjono	
		US-7,349,987	03-25-2008	Redlich et al.	
		US-7,546,427	06-09-2009	Gladwin et al.	
		US-7,552,482	06-23-2009	Redlich et al.	
		US-7,669,051	02-23-2010	Redlich et al.	
		US-7,721,344	05-18-2010	Redlich et al.	
		US-2011/0145573	06-16-2011	Nakai et al.	

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]

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. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [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.

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	3	of	3

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	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[2]
		Haniotakis et al., "Security Enhancement Through Multiple Path Transmission in Ad Hoc Networks," IEEE Intl. Conference on Communications, 20-24 June 2004, 5 pgs.	
		Rivest, "All-Or-Nothing Encryption and The Package Transform," Proc. Of the 4th Intl. Workshop on Fast Software Encryption (1997), 9 pgs.	

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]Applicant is to place a check mark here if English language Translation is attached.

AMENDMENTS TO THE SPECIFICATION

Please change the title of the specification to the following title:

Systems and Methods for Cryptographically Splitting and Storing Data

REMARKS

Summary of the Office Action

Claims 1-27 are pending in this application.

The title of the invention was objected to as not being descriptive.

Claims 4, 6, 13, 15, 22, and 24 were rejected under 35 U.S.C. § 112, first paragraph as allegedly failing to comply with the written description requirement.

Claims 1-3, 5-12, 14-21, and 23-27 were rejected under 35 U.S.C. § 103 as allegedly being unpatentable over Horne et al. *Escrow Services and Incentives in Peer-to-Peer Networks* ("Horne") in view of Li U.S. Patent Application Publication No. 2006/0080454 ("Li") or in the alternative in view of Hand, *Spread Spectrum Storage with Mnemosyne* ("Hand"). Claims 4, 13, and 22 were rejected under 35 U.S.C. § 103 as allegedly being unpatentable over Horne in view of Li or in the alternative Hand and Kubiatowicz *OceanStore: An Architecture for Global-Scale Persistent Storage* ("Kubiatowicz").

Applicants respectfully traverse the Examiner's rejections.

Applicants' Reply to the Objection to the Title

The title has been amended to be clearly indicative of the invention to which the claims are directed. No new matter has been added by the amendments. Accordingly, Applicant respectfully requests withdrawal of the objection to the title.

Applicants' Reply to the Rejections under 35 U.S.C. § 112

Regarding claims 4, 13, and 22, the Examiner contends that no corresponding disclosure or description could be found in the specification for the recited "causing a plurality of data units in each of the shares to be rearranged relative to one another after the separating step."[1] Applicants respectfully disagree. This limitation is at least supported by paragraphs 290 to 294 of the originally filed specification. For example, paragraph 294 recites:

[1] See Office Action pg. 3

> "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."

Therefore, claims 4, 13, and 22 are fully supported by the originally filed specification. Accordingly, Applicants respectfully request withdrawal of the Examiner's rejection under 35 U.S.C. § 112 for claims 4, 13, and 22.

Regarding claims 6, 15, and 24, the Examiner contends that Applicants' specification does not support how to use all Shamir algorithms to create data indicative of the encryption key. In particular, the Examiner alleges that Applicants' disclosure of the use of a species of Shamir algorithm does not enable the genus of all Shamir algorithms.[2] Applicants respectfully disagree. MPEP 2164.08 dictates that "the specification must teach those skilled in the art how to make and use the full scope of the claimed invention without 'undue experimentation'."[3] Furthermore, MPEP 2164.08 states that "Nevertheless, not everything necessary to practice the invention need be disclosed. In fact, what is well-known is best omitted. All that is necessary is that one skilled in the art be able to practice the claimed invention, given the level of knowledge and skill in the art."[4] Therefore, contrary to the Examiner's allegation, it is not necessary for Applicants' to support the use of all Shamir algorithms in detail, but rather, for Applicants to describe Shamir algorithms to a degree which enables one skilled in the art to practice the claimed invention.

To this point, Applicants respectfully submit that the originally filed specification fully supports the use of Shamir algorithms as claimed. For example, paragraphs 448 and 449 recite:

> "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 . . .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." – specification, par. 448-449

---

[2] See Office Action pg. 4
[3] *In re Wright*, 999 F.2d 1557, 1561, 27 USPQ2d 1510, 1513 (Fed. Cir. 1993).
[4] *In re Fisher*, 427 F.2d 833, 839, 166 USPQ 18, 24 (CCPA 1970).

Based on the portion cited above, one of ordinary skill in the art would understand that the "Shamir algorithm" as recited in claims 6, 15, and 24 may be any algorithm authored by Shamir suitable for the functionality described in these paragraphs. Therefore, in reciting "Shamir algorithm" in claims 6, 15, and 24, Applicants have not claimed the genus of all Shamir algorithms, but any and all algorithms authored by Shamir suitable for creating data indicative of an encryption key.

For at least the above reasons, Applicants respectfully submit that claims 6, 15, and 24 clearly and distinctly claim the subject matter which Applicant regards as the invention and fully satisfy the requirements of 35 U.S.C. § 112. Reconsideration and withdrawal of the Examiner's rejections for claims 6, 15, and 24 is respectfully requested.

Applicants' Reply to the Rejections under 35 U.S.C. § 103

Applicants respectfully submit that whether taken alone or in combination, Horne and Li or Horne and Hand fail to show or render obvious "including in the plurality of shares data indicative of (a) the encryption key and (b) the hash information" as recited in Applicants' claim 1. In the Office Action, the Examiner refers to section 2.2 ¶ 7, section 4.1 ¶ 3, and section 4.2 ¶ 8 of Horne to teach this feature. While the portions of Horne cited by the Examiner discuss breaking a content item into blocks and taking a hash of the overall content item, the cited portions fail to disclose including data indicative of the hash in the blocks themselves. Instead, the hash is sent separately from the content item and used to verify that a legitimate content item was received by the end user (see Horne, section 2.2 ¶ 7). Nowhere in the cited portions, nor in the reference as a whole, does Horne describe including data indicative of hash information in a plurality of data shares, as recited in claim 1. Therefore, Horne fails to show or render obvious all of the features of Applicants' claim 1.

Li and Hand which were cited as allegedly showing other features of the Applicants' claim 1, fail to remedy the deficiencies of Horne relative to the rejection. In particular, Li and Hand do not disclose creating hash information based on a hash operation using a data set and including the hash information in a plurality of shares, as claimed. Similarly, Kubiatowicz, which was cited as allegedly showing features of dependent claims 4, 13, and 22, fail to remedy the deficiencies of Horne for the same reason.

For at least the forgoing reasons, Applicants respectfully submit that independent claim 1 is allowable over the cited references. Independent claims 10 and 19 recite similar limitations as claim 1 and are therefore allowable for at least the same reasons as presented above. Claims 2-9, 11-18, and 20-27 each depend, directly or indirectly, from one of independent claims 1, 10, and 19 and add further limitations thereto. Therefore, claims 2-9, 11-18, and 20-27 are also allowable for at least the same reasons. Applicants respectfully request reconsideration and withdrawal of the rejections under 35 U.S.C. § 103 for claims 1-27.

Conclusion

For at least the reasons set forth above, Applicants submit that claims 1-27 are allowable and that this application is in condition for allowance. Reconsideration and prompt allowance of this application are respectfully requested.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 06-1075, under Order No. 104093-0002-105 from which the undersigned is authorized to draw.

Dated: June 29, 2012

Respectfully submitted,

By /Matthew S. Bertenthal/
Matthew Samuel Bertenthal
Registration No.: 61,129
ROPES & GRAY LLP
1900 University Avenue
6th Floor
Palo Alto, California 94303-2284
(650) 617-4000
(617) 235-9492 (Fax)
Attorneys/Agents For Applicant

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13371363	ORSINI ET AL.
	Examiner	Art Unit
	MICHAEL CHAO	2492

SEARCHED			
Class	Subclass	Date	Examiner
726	26	5/4/2012	mc

SEARCH NOTES		
Search Notes	Date	Examiner
Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	5/4/2012	mc
Inventor name search in EAST	5/4/2012	mc
Assignee name search in EAST	5/4/2012	mc
google scholar searched "fountain OR erasure OR tornado OR LT OR raptor OR rateless code encrypted key hash OR fingerprint OR checksum"	5/4/2012	mc
updated Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	7/16/2012	mc

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/371,363	02/10/2012	Rick L. Orsini	104093-0002-105	7984

1473 7590 07/26/2012

ROPES & GRAY LLP
PATENT DOCKETING 39/361
1211 AVENUE OF THE AMERICAS
NEW YORK, NY 10036-8704

EXAMINER	
CHAO, MICHAEL W	
ART UNIT	PAPER NUMBER
2492	

NOTIFICATION DATE	DELIVERY MODE
07/26/2012	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):

USPatentMail@ropesgray.com
USPatentMail2@ropesgray.com

Office Action Summary	Application No.	Applicant(s)	
	13/371,363	ORSINI ET AL.	
	Examiner	Art Unit	
	Michael Chao	2492	

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

Period for Reply

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

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

Status

1)☒ Responsive to communication(s) filed on *29 May 2012*.

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

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

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

Disposition of Claims

5)☒ Claim(s) *1-27* is/are pending in the application.

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

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-27* is/are rejected.

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

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

Application Papers

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

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

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

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

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

Priority under 35 U.S.C. § 119

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

a)☐ All b)☐ Some * c)☐ None of:

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

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

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

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

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *6/29/2012*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This action is in response to argument filed 6/29/2012. Application 13/371,363 claims priority to 10/25/2004. Claims 1-27 are pending and directed toward distributed data storage in an encrypted system.

Response to Arguments

Applicant's arguments, see page 3-4, filed 6/29/2012, with respect to the § 112 first paragraph rejection of claims 4, 13, and 22 have been fully considered and are persuasive. The recited portion of Applicant's specification paragraph [294] supports the claimed subject matter. The 112 first paragraph of claims 4, 13 and 22 has been withdrawn.

Applicant's arguments filed 6/29/2012 have been fully considered but they are not persuasive.

Applicant's second argument (page 4) that the 112 first and second paragraph rejections of claims 6, 15 and 24 is improper is not persuasive.

Claim 6 recites "wherein the data indicative of the encryption key comprises data created using a Shamir algorithm" and was rejected as: Shamir, as used in the art, is the name of a person. Shamir has authored several algorithms some of which are not directed toward keying. As such there does not appear to be support as to how to use all Shamir algorithms to create data indicative of the encryption key. Applicant's use of one Shamir algorithm (presumably RSA) does not disclose how to use other unrelated

algorithms for the same purpose. In other words, Applicant's disclosure of the use of a species of Shamir algorithm does not enable the genus of all Shamir algorithms.

Applicant responded by noting that paragraphs 448 and 449 recited "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 . . . 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." Applicant further responded that " one of ordinary skill in the art would understand that the "Shamir algorithm" as recited in claims 6, 15, and 24 may be any algorithm authored by Shamir suitable for the functionality described in these paragraphs."

However, Applicant's retort serves to illustrate why the written description requirement for claims 6, 15 and 24 is unfulfilled. Shamir is the name of a person, a person who has authored multiple algorithms. The claim merely recites that data indicative of an encryption key be created using a Shamir algorithm, any Shamir algorithm (See Arguments page 5). However, Applicant has not disclosed how to use any Shamir algorithm, only one which is "for securing splitting keys". Applicant's claimed scope extends beyond that which is described in the specification. Further, Applicant cannot avoid describing in his specification which Shamir algorithm is intended by alleging that one of ordinary skill in the art would understand which algorithms are "suitable for the functionality described in these paragraphs"; such would require a

person to undertake the process of invention by testing Shamir algorithms by trial and error.

Further, Applicant asserts (page 5) that they have "not claimed the genus of all Shamir algorithms, but any and all algorithms authored by Shamir suitable for creating data indicative of an encryption key". Again, Applicant's cited portions of the specification are silent with regard to what makes a Shamir algorithm suitable or capable of creating indicative data.

Applicant's third argument (page 5) that Horne in view of (Li or Hand) does not disclose "including in the plurality of shares data indicative of (a) the encryption key and (b) the hash information", is unpersuasive. Applicant furthers this argument by stating that "Nowhere in the cited portions, nor in the reference as a whole, does Horne describe including data indicative of hash information in a plurality of data shares"

In the prior action the following was cited as disclosing the limitation ("In order to obtain the key K, R computes the hash of the encrypted content H(EK(C)) and sends it to ES, together with a description of the content C it desires to obtain, and the identity of S. It also sends a payment for the content C, which will only be processed if the content is valid (step 2)." Horne § 2.2 ¶ 7). Where R is the receiver, S is the Source, and ES is the trusted third party. Thus, Horne conceives that a hash is used to reference the encrypted content and that a receiver performs the hash and sends it to the trusted third party. The receiver necessarily receives the data from a source (Horne § 2.2 ¶ 6). Because the hash of Horne is of the encrypted data itself, the encrypted data is the "data indicative of . . . (b) the hash information".

Data indicative of something is not the data itself. In addition, by definition, the original data will always be indicative of its hash. See also the other cited sections (Horne § 4.1 ¶ 3; Horne § 4.2 ¶ 8)

Although not further argued, Horne § 2.2 ¶ 7 begins "in order to obtain the key K". Thus, the process of the cited paragraph must also be indicative of the encryption key, since it is purposed to obtain the key.

In summary, Horne discloses sending the data to a recipient, who hashes the data to obtain the key. Even if Horne did not describe the step of hashing the received data itself would fairly teach "data indicative of the hash information"; since it was the data that was hashed.

Applicant's further arguments depend on those addressed and are persuasive or not persuasive for the reasons stated above.

Claim Rejections - 35 USC § 112

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

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 6, 15, 24 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter

which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claims 6, 15, 24 recite: recite wherein the data indicative of the encryption key comprises data created using a Shamir algorithm. Shamir, as used in the art, is the name of a person. Shamir has authored several algorithms some of which are not directed toward keying. As such there does not appear to be support as to how to use all Shamir algorithms to create data indicative of the encryption key. Applicant's use of one Shamir algorithm (presumably RSA) does not disclose how to use other unrelated algorithms for the same purpose. In other words, Applicant's disclosure of the use of a species of Shamir algorithm does not enable the genus of all Shamir algorithms. See In In re Wright, 999 F.2d 1557, 27 USPQ2d 1510 (Fed. Cir. 1993), In In re Vaeck, 947 F.2d 488, 495, 20 USPQ2d 1438, 1444 (Fed. Cir. 1991). See also MPEP 2164.06(b).

As to the issue of written description for the originally filed claims: "However, as discussed in paragraph I., supra, the issue of a lack of adequate written description may arise even for an original claim when an aspect of the claimed invention has not been described with sufficient particularity such that one skilled in the art would recognize that the applicant had possession of the claimed invention." See MPEP 2163 (II).

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

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

Claims 6, 15, 24 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 6, 15, 24 recite wherein the data indicative of the encryption key comprises data created using a Shamir algorithm. Shamir, as used in the art, is the name of a person. It is unclear which Shamir algorithm is intended, for the purposes of examination the claims have been interpreted to require RSA encryption.

Claim Rejections - 35 USC § 103

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

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

Claims 1-3, 5, 7-12, 14, 16-21, 23, and 25-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Horne et al. (Escrow Services and Incentives in Peer-to-Peer Networks) in view of Li (US 2006/0080454) or in the alternative in view of Hand (Spread Spectrum Storage with Mnemosyne).

With respect to claims 1, 10, 19, Horne teaches: A method for securing a data set, the method steps implemented by a programmed computer system, the method steps comprising:

encrypting the data set based on an encryption key to produce an encrypted data set; ("In the protocol that we describe, S encrypts C with a key K and sends the encryption EK(C)to R." Horne 2.2 ¶ 3)

creating hash information based on a hash operation using the data set; ("In order to take part in the protocol ES requires the correct hash of the encrypted content, H(EK(C)), and the key K that decrypts the content. . . . we assume that S sent the pair K,H(EK(C))———————————— to ES in a preprocessing stage, together with a description of C." Horne 2.2 ¶ 3; see also Horne § 4.2)

generating data splitting information, ("A Straightforward Method Based on Error Correcting Codes" Horne § 4.1) [wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;]

separating the encrypted data set into the plurality of shares based on the data splitting information; ("Distributed file storage: In this model files are not stored at a single server. Instead, a file is divided into many blocks encoded with an error correcting code, and each block is stored at a different location (this is the storage method used by Mojonation.com). The use of error correcting codes ensures that the file can be restored even if part of the peers that store parts of the file are unavailable or corrupt. The directory service might be centralized or distributed. Our ES service can cooperate with this storage system, where the use of error correcting codes we suggest in Section 4 might use (or might not use) the same error correcting code as the storage method." Horne § 5 ¶ 4)

including in the plurality of shares data indicative of (a) the encryption key and (b) the hash information; and ("In order to obtain the key K, R computes the hash of the encrypted content H(EK(C)) and sends it to ES, together with a description of the content C it desires to obtain, and the identity of S. It also sends a payment for the content C, which will only be processed if the content is valid (step 2)." Horne § 2.2 ¶ 7; "After receiving this message R picks a small random set of of the encrypted encoded blocks (where is a parameter to be defined below). It sends to ES this set of encrypted blocks, together with their indexes and the encrypted message that is directed from S to ES." Horne § 4.1 ¶ 3; "In order to verify the encrypted content that it receives from S, R should forward this signature and randomly chosen encrypted blocks to ES." Horne § 4.2 ¶ 8)

causing the plurality of shares to be stored in respective separate storage locations; (Horne § 5 ¶ 4)

wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares. ("The scheme could either use error correction codes, or use more efficient erasure codes. We first examine the use of error correction codes. The codes have the property that given n blocks, such that at least t of them are correct (although the receiver does not know which ones these are), the receiver can reconstruct the original message." Horne § 4.1 ¶ 6).

Although Horne discloses that a distributed storage system may be used (Horne § 5 ¶ 4) it does not disclose how the data is distributed among the stores, as claimed:

wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;

Li discloses a similar system directed toward peer distribution (Li [0003]) using erasure/error coding (Li [0106]). Li further discloses a method for selecting the peers for storing data ("each peer node is assigned k keys in the coded message space of n, with each key being the row index of the generator matrix G. The key assignment may be carried out by the server. Further, if the number of peers caching the media is smaller than n/k, it is possible to assign each peer a unique set of keys. As a result, it can be guaranteed that each peer holds distinctive coded messages. While this strategy provides a number of benefits, it still requires a central coordination node (such as the server)." Li [0109]; alternatively "in another embodiment, the role of the central coordination node is eliminated by allowing each peer to choose k random keys." Li [0110]). Note that, as used in Li, keys are referring to the erasure coding blocks held by a peer and are not cryptographic keys. ("the availability vector will include the media erasure coding keys assigned to serving peer, and the number of erasure blocks held by the serving peer. In addition, if the serving peer uses erasure coding and the media is also embedded coded, the availability vector will include the assigned media erasure coding keys" Li [0065])

A person of ordinary skill in the art at the time of invention would have combined Horne with Li by using the concepts of Li to implement the distribution of erasure coded blocks in Horne (Horne § 5 ¶ 4). It would have been obvious to one of ordinary skill in the art at the time of invention to combine Horne with Li in order to implement necessary

but unspecified functionality of Horne using a solution disclosed in a similar system (Li [0109-10]).

In the alternative, Hand discloses a similar system directed to distributed (Hand § 27.1 ¶ 1) erasure coded fragments for data storage (Hand § 27.1 ¶ 2). Hand additionally discloses a method for distributing the data, as claimed: wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;

("Location: Mnemosyne achieves its security properties by storing encrypted data blocks in pseudo-random (and, to an adversary, unpredictable) locations in a large virtual network store, which is then mapped onto distributed physical storage devices. The locations of the encrypted blocks making up a data set are determined by a sequence of 256-bit values obtained by successively hashing an initial value which depends ultimately on the filename and the user's key K.

Distribution: The sequence of 256-bit location identifiers from the previous step is finally mapped onto physical storage using a peer-to-peer network of storage nodes, each of which holds a fixed-size physical block store." Hand § 27.2 ¶ 6-7).

A person of ordinary skill in the art at the time of invention would have combined Horne with Hand by using the concepts of Hand to implement the distribution of erasure coded blocks in Horne (Horne § 5 ¶ 4). It would have been obvious to one of ordinary skill in the art at the time of invention to combine Horne with Hand in order to implement

necessary but unspecified functionality of Horne using a solution disclosed in a similar system Hand § 27.2 ¶ 6-7).

With respect to claims 2, 11, 20, Horne in view of Li or Hand discloses: wherein the step of separating the encrypted data set comprises using a deterministic technique. ("each peer node is assigned k keys in the coded message space of n, with each key being the row index of the generator matrix G. The key assignment may be carried out by the server. Further, if the number of peers caching the media is smaller than n/k, it is possible to assign each peer a unique set of keys. As a result, it can be guaranteed that each peer holds distinctive coded messages. While this strategy provides a number of benefits, it still requires a central coordination node (such as the server)." Li [0109]) ("The locations of the encrypted blocks making up a data set are determined by a sequence of 256-bit values obtained by successively hashing an initial value which depends ultimately on the filename and the user's key K." Hand § 27.2 ¶ 6-7).

With respect to claims 3, 12, 21, Horne in view of Li or Hand discloses: wherein the step of separating the encrypted data set comprises using a substantially random technique. ("in another embodiment, the role of the central coordination node is eliminated by allowing each peer to choose k random keys." Li [0110]) ("Location: Mnemosyne achieves its security properties by storing encrypted data blocks in pseudo-random (and, to an adversary, unpredictable) locations in a large virtual network store, which is then mapped onto distributed physical storage devices." Hand § 27.2 ¶ 6-7;

thus as disclosed by Hand, the process is 'random' despite being deterministic due to a consistent result given the same inputs)

With respect to claims 5, 14, 23, Horne in view of Li or Hand discloses: wherein the step of separating the encrypted data into the plurality of shares comprises causing the plurality of shares to have a substantially random distribution of the encrypted data set. ("in another embodiment, the role of the central coordination node is eliminated by allowing each peer to choose k random keys." Li [0110]) ("Location: Mnemosyne achieves its security properties by storing encrypted data blocks in pseudo-random (and, to an adversary, unpredictable) locations in a large virtual network store, which is then mapped onto distributed physical storage devices." Hand § 27.2 ¶ 6-7; thus as disclosed by Hand, the process is 'random' despite being deterministic due to a consistent result given the same inputs).

With respect to claims 7, 16, 25, Horne in view of Li or Hand discloses: wherein the step of including data indicative of the encryption key comprises:

Encrypting the encryption key with a second key; and. ("It then sends these blocks to R together with the key K encrypted with the public key of ES." Horne § 4.1 ¶ 2)

Including in the plurality of shares data indicative of the encrypted encryption key.("In order to obtain the key K, R computes the hash of the encrypted content H(EK(C)) and sends it to ES, together with a description of the content C it desires to

obtain, and the identity of S. It also sends a payment for the content C, which will only be processed if the content is valid (step 2)." Horne § 2.2 ¶ 7).

With respect to claims 8, 17, 26, Horne in view of Li or Hand discloses: further comprising the method step of storing the second key outside of the plurality of shares ("It then sends these blocks to R together with the key K encrypted with the public key of ES." Horne § 4.1 ¶ 2; ES is distinct from source S and receiver R), wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares, and the second key. ("The scheme could either use error correction codes, or use more efficient erasure codes. We first examine the use of error correction codes. The codes have the property that given n blocks, such that at least t of them are correct (although the receiver does not know which ones these are), the receiver can reconstruct the original message." Horne § 4.1 ¶ 6).

With respect to claims 9, 18, 27, Horne in view of Li or Hand discloses: wherein the step of storing the shares in respective separate storage locations comprises storing the shares on at least two separate storage devices. ("Distributed file storage: In this model files are not stored at a single server. Instead, a file is divided into many blocks encoded with an error correcting code, and each block is stored at a different location (this is the storage method used by Mojonation.com). The use of error correcting codes ensures that the file can be restored even if part of the peers that store parts of the file are unavailable or corrupt. The directory service might be centralized or distributed. Our

ES service can cooperate with this storage system, where the use of error correcting codes we suggest in Section 4 might use (or might not use) the same error correcting code as the storage method." Horne § 5 ¶ 4)

Claims 4, 13, 22, are rejected under 35 U.S.C. 103(a) as being unpatentable over Horne et al. (Escrow Services and Incentives in Peer-to-Peer Networks) in view of [Li (US 2006/0080454) or in the alternative Hand (Spread Spectrum Storage with Mnemosyne)] in view of Kubiatowicz (OceanStore).

With respect to claims 4, 13, and 22, Horne in view of Li or Hand does not disclose: further comprising causing a plurality of data units in each of the shares to be rearranged relative to one another after the separating step.

Kubiatowicz discloses a similar system based on distributed storage (Kubiatowicz § 2 figure 1) of erasure codes (Kubiatowicz § 4.5). Kubiatowicz further discloses a method of updating the data objects.

("Objects in the OceanStore are modified through updates. Updates contain information about what changes to make to an object and the assumed state of the object under which those changes were developed, much as in the Bayou system [13]. In principle, every update to an OceanStore object creates a new version2. Consistency based on versioning, while more expensive to implement than update-in-place consistency, provides for cleaner recovery in the face of system failures [49]. It also obviates the need for backup and supports "permanent" pointers to information." Kubiatowicz § 2 ¶ 4) ("For the user, we provide a naming syntax which explicitly

incorporates version numbers. Such names can be included in other documents as a form of permanent hyper-link. In addition, interfaces will exist to examine modification history and to set versioning policies [44]. Although in principle every version of every object is archived, clients can choose to produce versions less frequently. Archival copies are also produced when objects are idle for a long time or before objects become inactive. When generating archival fragments, the floating replicas of an object participate together: they each generate a disjoint subset of the fragments and disseminate them into the infrastructure." Kubiatowicz § 4.5 ¶4).

A person of ordinary skill in the art would have modified Horne in view of Li (or Hand) with Kubiatowicz by providing a method for versioning the files to be distributed as disclosed in Kubiatowicz. It would have been obvious to one of ordinary skill in the art at the time of invention to allow versioning of the files so that users could update the files thereby allowing for flexibility of the media storage.

Claims 6, 15, 24, are rejected under 35 U.S.C. 103(a) as being unpatentable over Horne et al. (Escrow Services and Incentives in Peer-to-Peer Networks) in view of [Li (US 2006/0080454) or in the alternative in view of Hand (Spread Spectrum Storage with Mnemosyne)] in view of official notice

With respect to claims 6, 15, and 24 Horne in view of Li or Hand discloses: wherein the data indicative of the encryption key comprises data created using a [Shamir algorithm]. ("The encryption can be done using public key cryptography" Horne § 2.1.2 ¶ 5) ("It then sends these blocks to R together with the key K encrypted with the

public key of ES." Horne § 4.1 ¶ 2). While Horne does disclose the use of a public key encryption, it does not disclose a Shamir Algorithm. Public key encryption commonly refers to the RSA algorithm by Rivest, Shamir and Adleman, Official notice is taken thereof. It would have been obvious to one of ordinary skill in the art to select RSA as the public key encryption method discussed in Horne. It would have been obvious to one of ordinary skill in the art at the time of invention to select RSA as the public key encryption in order to take advantage of a known secure algorithm that conforms to the design requirements of Horne.

Conclusion

THIS ACTION IS MADE FINAL. 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 Michael Chao whose telephone number is (571)270-5657. The examiner can normally be reached on 8-4 Monday through Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Saleh Najjar can be reached on (571)272-4006. 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.

/M. C./
Examiner, Art Unit 2492

/saleh najjar/
Supervisory Patent Examiner, Art Unit 2492

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S29	0	microsoft.asn. and erasure adj codes and @pd>"20120514" and (@ad<"20041025" or @rlad<"20041025")	US-PGPUB; USPAT	OR	OFF	2012/07/16 20:19
S30	5	(fountain OR erasure OR tornado OR LT OR raptor OR rateless) adj2 cod$3 encrypted key (hash OR fingerprint OR checksum) and @pd>"20120514" and (@ad<"20041025" or @rlad<"20041025")	US-PGPUB; USPAT; EPO; IBM_TDB	AND	OFF	2012/07/16 20:19
S31	1	(fountain OR erasure OR tornado OR raptor OR rateless) adj (coding or codes) encrypted key (hash OR fingerprint OR checksum) and @pd>"20120514" and (@ad<"20041025" or @rlad<"20041025")	US-PGPUB; USPAT; EPO; IBM_TDB	AND	OFF	2012/07/16 20:19
S32	7	(fountain OR erasure OR tornado OR LT OR raptor OR rateless) adj2 cod$3 and distribution and @pd>"20120514" and (@ad<"20041025" or @rlad<"20041025")	US-PGPUB; USPAT; EPO; IBM_TDB	AND	OFF	2012/07/16 20:19
S33	3	(fountain OR erasure OR tornado OR LT OR raptor OR rateless) adj cod$3 and distribution and @pd>"20120514" and (@ad<"20041025" or @rlad<"20041025")	US-PGPUB; USPAT; EPO; IBM_TDB	AND	OFF	2012/07/16 20:19
S34	7	713/153.ccls. and @pd>"20120514" and (@ad<"20041025" or @rlad<"20041025")	US-PGPUB; USPAT; EPO; IBM_TDB	AND	OFF	2012/07/16 20:19
S35	20	726/27.ccls. and @pd>"20120514" and (@ad<"20041025" or @rlad<"20041025")	US-PGPUB; USPAT; EPO; IBM_TDB	AND	OFF	2012/07/16 20:20
S36	7	(security adj first).asn. and @pd>"20120514"	US-PGPUB; USPAT; EPO; IBM_TDB	OR	OFF	2012/07/16 20:20
S37	1	(orsini and rick or hare and mark or davenport and rojer or winick and steven).in. and @pd>"20120514" and (@ad<"20041025" or @rlad<"20041025")	US-PGPUB; USPAT; EPO; IBM_TDB	OR	OFF	2012/07/16 20:20
S38	25	US-8151333-$.DID. OR US-7693992-$.DID. OR US-7472105-$.DID. OR US-7444421-$.DID. OR US-7428751-$.DID. OR US-7412462-$.DID. OR US-7304990-$.DID. OR US-7302583-$.DID. OR US-7277958-$.DID. OR US-7174385-$.DID. OR US-7143289-$.DID. OR US-6819766-$.DID. OR US-	US-PGPUB; USPAT; USOCR	OR	OFF	2012/07/16 20:22

		6269432-$.DID. OR US-6118874-$.DID. OR US-5937066-$.DID. OR US-5450099-$.DID. OR US-20030084020-$.DID. OR US-6192472-$.DID. OR WO-02062032-$.DID. OR US-20020129245-$.DID. OR US-6363481-$.DID. OR US-7349987-$.DID. OR US-7546427-$.DID. OR US-7552482-$.DID. OR US-7669051-$.DID. OR US-7721344-$.DID.				

7/ 17/ 2012 9:32:28 AM
C:\ Users\ mchao\ Documents\ EAST\ Workspaces\ 13371363.wsp

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13371363	ORSINI ET AL.
	Examiner	**Art Unit**
	MICHAEL CHAO	2492

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

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

CLAIM		DATE								
Final	Original	05/02/2012	07/16/2012							
	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	✓	✓							
	26	✓	✓							
	27	✓	✓							

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 3

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

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
/M.C./		US-8,151,333	04-03-2012	Zhu et al.	
/M.C./		US-7,693,992	04-06-2010	Watson	
/M.C./		US-7,472,105	12-30-2008	Staddon et al.	
/M.C./		US-7,444,421	10-28-2008	Katayama	
/M.C./		US-7,428,751	09-23-2008	Oom Temudo de Castro et al.	
/M.C./		US-7,412,462	08-12-2008	Margolus et al.	
/M.C./		US-7,304,990	12-04-2007	Rajwan	
/M.C./		US-7,302,583	11-27-2007	Forrest	
/M.C./		US-7,277,958	10-02-2007	Chung et al.	
/M.C./		US-7,174,385	02-06-2007	Li	
/M.C./		US-7,143,289	11-28-2006	Denning et al.	
/M.C./		US-6,819,766	11-16-2004	Weidong	
/M.C./		US-6,269,432	07-31-2001	Smith	
/M.C./		US-6,118,874	09-12-2000	Okamoto et al.	
/M.C./		US-5,937,066	08-10-1999	Gennaro et al.	
/M.C./		US-5,450,099	09-12-1995	Stephenson et al.	
/M.C./		US-2012/0072723	03-22-2012	Orsini et al.	
/M.C./		US-20030084020	05-01-2003	Shu	
/M.C./		US-6,192,472	02-20-2001	Garay et al.	

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]
/M.C./		WO-02/062032	08-08-2002	The Charles Stark Draper Laboratory, Inc.		
/M.C./		WO-10/057181	05-20-2010	Unisys Corp.		

Examiner Signature	/Michael Chao/	Date Considered	07/16/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [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.

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 3

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

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
/M.C./		US-2002/0129245	09-12-2002	Cassagnol et al.	
/M.C./		US-6,363,481	03-26-2002	Hardjono	
/M.C./		US-7,349,987	03-25-2008	Redlich et al.	
/M.C./		US-7,546,427	06-09-2009	Gladwin et al.	
/M.C./		US-7,552,482	06-23-2009	Redlich et al.	
/M.C./		US-7,669,051	02-23-2010	Redlich et al.	
/M.C./		US-7,721,344	05-18-2010	Redlich et al.	
/M.C./		US-2011/0145573	06-16-2011	Nakai et al.	
/M.C./					

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]

Examiner Signature	/Michael Chao/	Date Considered	07/16/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [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.

31155180_1

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 3 of 3

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	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[2]
/M.C./		Haniotakis et al., "Security Enhancement Through Multiple Path Transmission in Ad Hoc Networks," IEEE Intl. Conference on Communications, 20-24 June 2004, 5 pgs.	
/M.C./		Rivest, "All-Or-Nothing Encryption and The Package Transform," Proc. Of the 4th Intl. Workshop on Fast Software Encryption (1997), 9 pgs.	

Examiner Signature	/Michael Chao/	Date Considered	07/16/2012

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

[1]Applicant's unique citation designation number (optional). [2]Applicant is to place a check mark here if English language Translation is attached.

Docket No.: 104093-0002-105
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Orsini et al.

Application No.: 13/371,363 | Confirmation No.: 7984

Filed: February 10, 2012 | Art Unit: 2492

For: SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA | Examiner: M. W. Chao

REPLY ACCOMPANYING REQUEST FOR CONTINUED EXAMINATION (RCE)

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

Dear Madam:

INTRODUCTORY COMMENTS

In response to the Office Action dated July 26, 2012, please amend the above-identified U.S. patent application as follows. A Request for Continued Examination (RCE) is filed concurrently herewith.

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this Reply.

Remarks/Arguments begin on page 8 of this Reply.

PTO/SB/30 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Request for Continued Examination (RCE) Transmittal

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

Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

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. [x] Enclosed
      i. [x] Amendment/Reply
      ii. [ ] Affidavit(s)/Declaration(s)
      iii. [x] 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. [x] 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. [x] 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)

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	/Matthew S. Bertenthal/	Date	September 20, 2012
Name (Print/Type)	Matthew Samuel Bertenthal	Registration No.	61,129

32004246_1

REMARKS

Summary of the Office Action

Claims 1-27 were pending in this application.

Claims 6, 15, and 24 were rejected under 35 U.S.C. § 112 as allegedly failing to comply with the written description requirement.

Claims 1-3, 5, 7-12, 14, 16-21, 23, and 25-27 were rejected under 35 U.S.C. § 103 as allegedly being obvious from Horne et al. *Escrow Services and Incentives in Peer-to-Peer Networks* ("Horne") in view of Li U.S. Patent Application Publication No. 2006/0080454 ("Li") or in the alternative Hand *Spread Spectrum Storage with Mnemosyne* ("Hand"). Claims 4, 13, and 22 were rejected under 35 U.S.C. § 103 as allegedly being obvious from Horne in view of Li or in the alternative Hand and Kubiatowicz *Oceanstore: An Architecture for Global-Scale Persistent Storage* ("Kubiatowicz"). Claims 6, 15, and 24 were rejected under 35 U.S.C. § 103 as allegedly being obvious from Horne in view of Li, Hand, and official notice.

Summary of Applicants' Reply

Applicants have amended claims 1, 6, 10, 15, 19, and 24. No new matter has been added, and the amendments are fully supported by the originally filed application.

Applicants respectfully traverse the Examiner's rejections.

Applicants' Reply to the 35 U.S.C. § 112 Rejection

The Examiner rejected claims 6, 15, and 24 as allegedly failing to comply with the written description requirement. In particular, the Examiner contends that the Applicants' use of one Shamir algorithm does not disclose how to use other unrelated algorithms for the same purpose (see Office Action pg. 6).

Applicants have amended claims 6, 15, and 24 to recite a Shamir secret sharing algorithm. Support for amendment can be found in U.S. Provisional Application No. 60/718,185, to which the present application claims priority and incorporates by reference. See e.g., pages 178, 256, 264, 270, 275, and 277 of U.S. Provisional Application No. 60/718,185, portions of which are reproduced below.

> "Key Secure: the above transform key or split session key is securely divided into key-shares using a "split knowledge" key splitting technique such as the Shamir algorithm. Each key-share is distributed to one data share." – pg. 178
>
> "The security of the constructions is based on the strength of standard cryptographic algorithms such as AES, HMAC-SHA1 and Shamir secret sharing" – pg. 264
>
> "The technique of 'secret sharing', sometimes referred to as 'split knowledge', allows parties to divide some piece of secret data into shares such that the secret can only be recovered by re-combining all, or some preset number, of the shares . . . The technique developed by Shamir in 1979 allows for *threshold* splitting, in which the number of shares required to recover the secret (t) may be smaller than the total number of shares (n)." – pg. 270
>
> "The SecureParser incorporates the technique of secret sharing of Shamir (Adi Shamir, 1979) for encryption key security . . . This key is subsequently 'split' into N shares using the Shamir technique, such that any M shares are required in order to re-construct the original key." – pg. 275

The above cited portions make clear both which Shamir algorithm is used (i.e., a Shamir secret-sharing algorithm), as well as how to use the Shamir algorithms to create data indicative of an encryption key, as recited in claims 6, 15, and 24. In view of the amendment and above support from the specification, Applicants respectfully submit that claims 6, 15, and 24 clearly and distinctly claim the subject matter which Applicant regards as the invention and fully satisfy the requirements of 35 U.S.C. § 112. Reconsideration and withdrawal of the Examiner's rejection under 35 U.S.C. § 112 for claims 6, 15, and 24 is respectfully requested.

Applicants' Reply to the 35 U.S.C. § 103 Rejection

Applicants' amended independent claims 1, 10, and 19 recite, *inter alia*, encrypting a data set based on an encryption key, creating hash information based on a hash operation using the data set, separating the encrypted data set into a plurality of shares based on data splitting information,

and including in the plurality of shares (a) data indicative of the encryption key and (b) the hash information.

Applicants respectfully submit that Horne, Li, and Hand, either alone or in combination, fail to show or render obvious at least the claimed limitation of including the hash information in the plurality of shares. In the Office Action, the Examiner refers to Horne § 2.2 ¶ 7, § 4.1 ¶ 3, and § 4.2 ¶ 8 as allegedly teaching this limitation, reproduced below.

> "In order to obtain the key K, R computes the hash of the encrypted content $H(E_K(C))$ and sends it to ES, together with a description of the content C it desires to obtain, and the identity of S. It also sends a payment for the content C, which will only be processed if the content is valid (step 2)" - Horne § 2.2 ¶ 7
>
> "After receiving this message R picks a small random set of *l* of the encrypted encoded blocks (where *l* is a parameter to be defined below). It sends to ES this set of encrypted blocks, together with their indexes and the encrypted message that is directed from S to ES." - Horne § 4.1 ¶ 3
>
> "In order to verify the encrypted content that it receives from S, R should forward this signature and *l* randomly chosen encrypted blocks to ES. ES can decrypt the blocks, generate the nodes in the paths from the corresponding leafs to the root, and verify that they match the signed value of the root node." - Horne § 4.2 ¶ 8

The above cited portions discuss a recipient R, which computes the hash information of an encrypted content C and sends the hash information to an escrow server ES. However, nowhere in the cited portions, nor in the reference as a whole, does Horne include the hash information within a plurality of data shares. Indeed, according to Horne, the hash information is sent separately from content C and encrypted encoded blocks *l*. To the extent that the encrypted encoded blocks *l* can even correspond to the claimed plurality of shares, Horne fails to discuss including the hash information within the encrypted blocks. Therefore, Horne fails to show or suggest at least the claimed limitation of including hash information in a plurality of shares

Li and Hand, which were cited as allegedly showing other features of the Applicants' independent claims, fail to remedy the deficiencies of Horne. In particular, Li and Hand fail to disclose creating hash information based on a hash operation using a data set, much less including the hash information in a plurality of shares, as claimed. Similarly, Kubiatowicz, which was cited as allegedly showing features of dependent claims 4, 13, and 22, fail to remedy the deficiencies of Horne for the same reasons.

For at least the forgoing reasons, Applicants respectfully submit that independent claims 1, 10, and 19 are allowable over the cited references. Claims 2-9, 11-18, and 20-27 each depend, directly or indirectly, from one of allowable independent claims 1, 10, and 19 and add further limitations thereto. Therefore, these claims are also allowable for at least the same reasons. Applicants respectfully request reconsideration and withdrawal of the rejections under 35 U.S.C. § 103 for claims 1-27.

Conclusion

For at least the reasons set forth above, Applicants respectfully submit that claims 1-27 are allowable and that this application is in condition for allowance. Reconsideration and prompt allowance of this application are respectfully requested.

Applicants believe no fee is due with this response other than as reflected on the enclosed Transmittal. However, if a fee is due, please charge our Deposit Account No. 06-1075, under Order No. 104093-0002-105 from which the undersigned is authorized to draw.

Dated: September 20, 2012

Respectfully submitted,

Electronic signature: /Matthew S. Bertenthal/
Matthew Samuel Bertenthal
Registration No.: 61,129
ROPES & GRAY LLP
1900 University Avenue
6th Floor
Palo Alto, California 94303-2284
(650) 617-4000
(617) 235-9492 (Fax)
Attorneys/Agents For Applicant

Electronic Patent Application Fee Transmittal

Application Number:	13371363
Filing Date:	10-Feb-2012
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Rick L. Orsini
Filer:	Matthew Sammuel Bertenthal/Joanne Ryan
Attorney Docket Number:	104093-0002-105

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

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

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Request for continued examination	1801	1	930	930
		Total in USD ($)		**930**

Electronic Acknowledgement Receipt

EFS ID:	13795220
Application Number:	13371363
International Application Number:	
Confirmation Number:	7984
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Rick L. Orsini
Customer Number:	1473
Filer:	Matthew Sammuel Bertenthal/Joanne Ryan
Filer Authorized By:	Matthew Sammuel Bertenthal
Attorney Docket Number:	104093-0002-105
Receipt Date:	20-SEP-2012
Filing Date:	10-FEB-2012
Time Stamp:	15:57:18
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$930
RAM confirmation Number	2717
Deposit Account	061075
Authorized User	

File Listing:

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

1	Request for Continued Examination (RCE)	104093-0002-105_RCE_Transmittal.pdf	96318 c1c39468d610620192ac719f975a8cfe95d9abd5	no	1
Warnings:					
This is not a USPTO supplied RCE SB30 form.					
Information:					
2		104093-0002-105_Final_Response.pdf	127306 a2d562a8a6789acd7ec92c5964299ee2b92c6208	yes	11
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Amendment Submitted/Entered with Filing of CPA/RCE		1	1	
	Claims		2	7	
	Applicant Arguments/Remarks Made in an Amendment		8	11	
Warnings:					
Information:					
3	Transmittal Letter	104093-0002-105_IDS.pdf	77620 def775bfe83ea6fc4d95ef53bdee379ac368dab8	no	3
Warnings:					
Information:					
4	Information Disclosure Statement (IDS) Form (SB08)	104093-0002-105_SB08.pdf	136625 37d7f6122e8bea939dc5c5eaaa6a617bc60fcf3b	no	2
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
5	Non Patent Literature	13371364_NonFinal_Reply_070312_and_Final_Office_Action_dated_082812.pdf	24976732 d68733d5129046ecb7643cbb16211aa2cc1dca05	no	49
Warnings:					
Information:					
6	Non Patent Literature	13399923_NonFinal_OA_052512_and_Reply_.pdf	21992897 c65fc4a660dd4106f2ee6ab2b257d5815005e05a	no	33
Warnings:					
Information:					
7	Non Patent Literature	13399923_Notice_of_Allowance_dated_091912.pdf	4723931 e243769e869172e5f15b9fdbbc40574654454ff9	no	13

Warnings:					
Information:					
8	Non Patent Literature	13024791_NonFinal_Office_Action_dated_070512.pdf	8238184 14deb4d4d142e7a439a318a031f9f1cd9d766347	no	28
Warnings:					
Information:					
9	Fee Worksheet (SB06)	fee-info.pdf	30781 01742c618104d156bc2679e5fdd0f04750abdc98	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	60400394		

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.

AMENDMENTS TO THE CLAIMS

The following listing of claims will replace all prior versions, and listings, of claims in this application.

Listing of Claims

1. (Currently Amended) A method for securing a data set, the method steps implemented by a programmed computer system, the method steps comprising:

encrypting the data set based on an encryption key to produce an encrypted data set;

creating hash information based on a hash operation using the data set;

generating data splitting information, wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;

separating the encrypted data set into the plurality of shares based on the data splitting information;

including in the plurality of shares (a) data indicative of [[(a)]] the encryption key and (b) the hash information; and

causing the plurality of shares to be stored in respective separate storage locations;

wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares.

2. (Original) The method of claim 1, wherein the step of separating the encrypted data set comprises using a deterministic technique.

3. (Original) The method of claim 1, wherein the step of separating the encrypted data set comprises using a substantially random technique.

4. (Original) The method of claim 1, further comprising causing a plurality of data units in each of the shares to be rearranged relative to one another after the separating step.

5. (Original) The method of claim 1, wherein the step of separating the encrypted data into the plurality of shares comprises causing the plurality of shares to have a substantially randomly distribution of the encrypted data set.

6. (Currently Amended) The method of claim 1, wherein the data indicative of the encryption key comprises data created using a Shamir secret sharing algorithm.

7. (Original) The method of claim 1, wherein the step of including data indicative of the encryption key comprises:

encrypting the encryption key with a second key; and

including in the plurality of shares data indicative of the encrypted encryption key.

8. (Original) The method of claim 7 further comprising the method step of storing the second key outside of the plurality of shares, wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares, and the second key.

9. (Original) The method of claim 1, wherein the step of storing the shares in respective separate storage locations comprises storing the shares on at least two separate storage devices.

10. (Currently Amended) A non-transitory computer readable medium storing computer executable instructions that, when executed by at least one processor, cause a computer system to carry out a method for securing a data set, the method comprising the steps of:

encrypting the data set based on an encryption key to produce an encrypted data set;

creating hash information based on a hash operation using the data set;

generating data splitting information, wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;

separating the encrypted data set into the plurality of shares based on the data splitting information;

including in the plurality of shares (a) data indicative of [[(a)]] the encryption key and (b) the hash information; and

causing the plurality of shares to be stored in respective separate storage locations;

wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares.

11. (Original) The non-transitory computer readable medium of claim 10, wherein the step of separating the encrypted data set comprises using a deterministic technique.

12. (Original) The non-transitory computer readable medium of claim 10, wherein the step of separating the encrypted data set comprises using a substantially random technique.

13. (Original) The non-transitory computer readable medium of claim 10, wherein the method further comprises causing a plurality of data units of the encrypted data set to be rearranged relative to one another after the separating step.

14. (Original) The non-transitory computer readable medium of claim 10, wherein the step of separating the encrypted data into the plurality of shares comprises causing the plurality of shares to have a substantially randomly distribution of the encrypted data set.

15. (Currently Amended) The non-transitory computer readable medium of claim 10, wherein the data indicative of the encryption key comprises data created using a Shamir secret sharing algorithm.

16. (Original) The non-transitory computer readable medium of claim 11, wherein the step of including data indicative of the encryption key comprises:

encrypting the encryption key with a second key; and

including in the plurality of shares data indicative of the encrypted encryption key.

17. (Original) The non-transitory computer readable medium of claim 16 wherein the method further comprises storing the second key outside of the plurality of shares, wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares, and the second key.

18. (Original) The non-transitory computer readable medium of claim 10, wherein the step of storing the shares in respective separate storage locations comprises storing the shares on at least two separate storage devices.

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

at least one processor;

a non-transitory computer readable medium storing computer executable instructions that, when executed by the at least one processor, cause the computer system to carry out the following steps:

encrypting the data set based on an encryption key to produce an encrypted data set;

creating hash information based on a hash operation using the data set;

generating data splitting information, wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;

separating the encrypted data set into the plurality of shares based on the data splitting information;

including in the plurality of shares (a) data indicative of [[(a)]] the encryption key and (b) the hash information; and

causing the plurality of shares to be stored in respective separate storage locations;

wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares.

20. (Original) The system of claim 19, wherein the step of separating the encrypted data set comprises using a deterministic technique.

21. (Original) The system of claim 19, wherein the step of separating the encrypted data set comprises using a substantially random technique.

22. (Original) The system of claim 19, wherein the method further comprises causing a plurality of data units of the encrypted data set to be rearranged relative to one another after the separating step.

23. (Original) The system of claim 19, wherein the step of separating the encrypted data into the plurality of shares comprises causing the plurality of shares to have a substantially randomly distribution of the encrypted data set.

24. (Currently Amended) The system of claim 19, wherein data indicative of the encryption key comprises data that was created using a Shamir secret sharing algorithm.

25. (Original) The system of claim 19, wherein the step of including data indicative of the encryption key comprises:

encrypting the encryption key with a second key; and

including in the plurality of shares data indicative of the encrypted encryption key.

26. (Original) The system of claim 25 wherein the method further comprises storing the second key outside of the plurality of shares, wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares, and the second key.

27. (Original) The system of claim 19, wherein the separate storage locations are located on at least two separate storage devices.

Docket No.: 104093-0002-105
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Orsini et al.

Application No.: 13/371,363 | Confirmation No.: 7984

Filed: February 10, 2012 | Art Unit: 2492

For: SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA | Examiner: M. W. Chao

INFORMATION DISCLOSURE STATEMENT (IDS)

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

Dear Madam:

Pursuant to 37 CFR 1.56, 1.97 and 1.98, the attention of the Patent and Trademark Office is hereby directed to the references listed on the attached PTO/SB/08. It is respectfully requested that the information be expressly considered during the prosecution of this application, and that the references be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Information Disclosure Statement, pursuant to 37 CFR 1.114(c), accompanies the Request for Continued Examination (37 CFR 1.114) submitted herewith.

In accordance with 37 CFR 1.98(a)(2)(ii), Applicants have not submitted copies of U.S. patents and U.S. patent applications.

In accordance with 37 CFR 1.97(g), the filing of this Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 CFR 1.56(a) exists. In accordance with 37 CFR 1.97(h), the filing of this Information Disclosure Statement shall not be construed to be an admission that any patent, publication or other information referred to therein is "prior art" for this invention unless specifically designated as such.

Notice of Related Patent Applications

The Examiner is advised that the following patent applications contain subject matter that may be related to the pending claims in the present application. In particular, applicants would like to draw the Examiner's attention to the fact that substantive examination may have occurred in these cases. For these cases, copies of any Office Actions that have issued and Replies that have been filed in these cases since the last information disclosure statement are submitted herewith. Applicants invite the Examiner to review these documents or any future substantive documents that will issue or be filed in any of the below cases. By bringing the following applications to the Examiner's attention, applicants do not waive any applicable confidentiality provisions of 35 U.S.C. 122.

Application No.	**Publication No.**	**Attorney Docket No.**	**Filing Date**	**Status**
12/148,365	US 2008-0244277	104093-0001-102	4/18/2008	Pending
13/024,791	US 2011-0179287	104093-0001-103	2/10/2011	Pending
13/024,804	US 2011-0179271	104093-0001-104	2/10/2011	Pending
13/399,923	Not published	104093-0001-105	2/17/2012	Allowed
13/371,361	Not published	104093-0002-104	2/10/2012	Issued
13/371,364	Not published	104093-0002-106	2/10/2012	Pending

It is submitted that the Information Disclosure Statement is in compliance with 37 CFR 1.98 and the Examiner is respectfully requested to consider the listed references.

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, under Order No. 104093-0002-105.

Dated: September 20, 2012

Respectfully submitted,

Electronic signature: /Matthew S. Bertenthal/
Matthew Samuel Bertenthal
Registration No.: 61,129
ROPES & GRAY LLP
1900 University Avenue
6th Floor
Palo Alto, California 94303-2284
(650) 617-4000
(617) 235-9492 (Fax)
Attorneys/Agents For Applicant

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. 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	Filing Date	☐ To be Mailed
13/371,363	02/10/2012	

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	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT		(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 ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
	09/20/2012									
	Total (37 CFR 1.16(i))	* 27	Minus	** 27	= 0	X $ =		OR	X $60=	0
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $ =		OR	X $250=	0
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	0

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)	OR	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							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 number found in the appropriate box in column 1.

Legal Instrument Examiner:
/BRENDA J. DENNY/

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/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

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
		US-8,271,802	09-18-2012	Orsini et al.	
		US-2012/0166818	06-28-2012	Orsini et al.	
		US-2012/0166576	06-28-2012	Orsini et al.	
		US-2012/0179916	07-12-2012	Staker et al.	
		US-2012/0221854	08-30-2012	Orsini et al.	
		US-2012/0222134	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-2012/0226904	09-06-2012	Orsini et al.	

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]
						√

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. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. ** CITE NO.: Those document(s) which are marked with an double asterisk (**) next to the Cite No. are not supplied because they were previously cited by or submitted to the Office in a prior application relied upon in this application for an earlier filing date under 35 U.S.C. 120. [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.

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	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[2]

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]Applicant is to place a check mark here if English language Translation is attached.

Electronic Patent Application Fee Transmittal

Application Number:	13371363
Filing Date:	10-Feb-2012
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Rick L. Orsini
Filer:	Christopher Jinhyun Han/Joanne Ryan
Attorney Docket Number:	104093-0002-105

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Request for Prioritized Examination	1817	1	4800	4800
Pages:				
Claims:				
Miscellaneous-Filing:				
Processing Fee, except for Provis. apps	1808	1	130	130
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**4930**

Doc Code: TRACK1.REQ
Document Description: TrackOne Request

PTO/SB/424 (09-12)

CERTIFICATION AND REQUEST FOR PRIORITIZED EXAMINATION UNDER 37 CFR 1.102(e) (Page 1 of 1)

First Named Inventor:	Rick L. Orsini	Nonprovisional Application Number (if known):	13/371,363
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA		

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS PRIORITIZED EXAMINATION FOR THE ABOVE-IDENTIFIED APPLICATION.

1. The processing fee set forth in 37 CFR 1.17(i), the prioritized examination fee set forth in 37 CFR 1.17(c), and if not already paid, the publication fee set forth in 37 CFR 1.18(d) have been filed with the request. The basic filing fee, search fee, examination fee, and any required excess claims and application size fees are filed with the request or have been already been paid.
2. The application contains or is amended to contain no more than four independent claims and no more than thirty total claims, and no multiple dependent claims.
3. The applicable box is checked below:

I. [ ] **Original Application (Track One) - Prioritized Examination under § 1.102(e)(1)**

i (a) The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a). This certification and request is being filed with the utility application via EFS-Web.

---OR---

(b) The application is an original nonprovisional plant application filed under 35 U.S.C. 111(a). This certification and request is being filed with the plant application in paper.

ii The executed inventor's oath or declaration is filed with the application. (37 CFR 1.63 and 1.64)

II. [X] **Request for Continued Examination - Prioritized Examination under § 1.102(e)(2)**

i. A request for continued examination has been filed with, or prior to, this form.
ii. If the application is a utility application, this certification and request is being filed via EFS-Web.
iii. The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a), or is a national stage entry under 35 U.S.C. 371.
iv. This certification and request is being filed prior to the mailing of a first Office action responsive to the request for continued examination.
v. No prior request for continued examination has been granted prioritized examination status under 37 CFR 1.102(e)(2).

Signature	/Christopher J. Han/	Date	November 19, 2012
Name (Print/Typed)	Christopher J. Han	Practitioner Registration Number	70,069

Note: *Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required in accordance with 37 CFR 1.33 and 11.18. Please see 37 CFR 1.4(d) for the form of the signature. If necessary, submit multiple forms for more than one signature, see below**

[X] *Total of 1 forms are submitted.

32561969_1

Electronic Acknowledgement Receipt

EFS ID:	14268149
Application Number:	13371363
International Application Number:	
Confirmation Number:	7984
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Rick L. Orsini
Customer Number:	1473
Filer:	Christopher Jinhyun Han/Joanne Ryan
Filer Authorized By:	Christopher Jinhyun Han
Attorney Docket Number:	104093-0002-105
Receipt Date:	19-NOV-2012
Filing Date:	10-FEB-2012
Time Stamp:	17:52:15
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$4930
RAM confirmation Number	6358
Deposit Account	061075
Authorized User	

File Listing:

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

1	TrackOne Request	104093-0002-105_Priority_Exam_Request_after_RCE.pdf	120523 02aeb4971c84c67906e6ebbbcbc18bd73a6feb18	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	32453 ffa41cf883327cde3f605861bd755a749b3f0910	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	152976		

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

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

ROPES & GRAY LLP
PATENT DOCKETING 39/361
1211 AVENUE OF THE AMERICAS
NEW YORK NY 10036-8704

MAILED
FEB 27 2013
OFFICE OF PETITIONS

Doc Code: TRACK1.GRANT

Decision Granting Request for Prioritized Examination (Track I or After RCE)	Application No.: 13/371,363

1. THE REQUEST FILED November 19, 2012 IS **GRANTED.**

The above-identified application has met the requirements for prioritized examination

A. ☐ for an original nonprovisional application (Track I).

B. ☒ for an application undergoing continued examination (RCE).

2. **The above-identified application will undergo prioritized examination.** The application will be accorded special status throughout its entire course of prosecution until one of the following occurs:

A. filing a **petition for extension of time** to extend the time period for filing a reply;

B. filing an **amendment to amend the application to contain more than four independent claims, more than thirty total claims**, or a multiple dependent claim;

C. filing a **request for continued examination**;

D. filing a notice of appeal;

E. filing a request for suspension of action;

F. mailing of a notice of allowance;

G. mailing of a final Office action;

H. completion of examination as defined in 37 CFR 41.102; or

I. abandonment of the application.

Telephone inquiries with regard to this decision should be directed to Brian W. Brown at 571-272-5338.

/Brian W. Brown/
[*Signature*]

Petitions Examiner, Office of Petitions
(Title)

Notice of References Cited	Application/Control No. 13/371,363	Applicant(s)/Patent Under Reexamination ORSINI ET AL.	
	Examiner Michael Chao	Art Unit 2492	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-			
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	SSMS, Krawczyk, 1994, Secret Sharing Made Short, Retrieved from the Internet <URL: link.springer.com/chapter/10.1007%2F3-540-48329-2_12>, pp 1-11 as printed.
	V	DFSID, Krawczyk, 1993, Distributed Fingerprints and Secure Information Dispersal, Retrieved from the internet <URL: dl.acm.org/citation.cfm?id=164075>, pp 1-12 as printed.
	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.

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

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
/M.C./		US-8,271,802	09-18-2012	Orsini et al.	
/M.C./		US-2012/0166818	06-28-2012	Orsini et al.	
/M.C./		US-2012/0166576	06-28-2012	Orsini et al.	
/M.C./		US-2012/0179916	07-12-2012	Staker et al.	
/M.C./		US-2012/0221854	08-30-2012	Orsini et al.	
/M.C./		US-2012/0222134	08-30-2012	Orsini et al.	
/M.C./		US-2012/0221855	08-30-2012	Orsini et al.	
/M.C./		US-2012/0221856	08-30-2012	Orsini et al.	
/M.C./		US-2012/0226904	09-06-2012	Orsini et al.	

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]
						√

Examiner Signature	/Michael Chao/	Date Considered	03/12/2013

*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. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. ** CITE NO.: Those document(s) which are marked with an double asterisk (**) next to the Cite No. are not supplied because they were previously cited by or submitted to the Office in a prior application relied upon in this application for an earlier filing date under 35 U.S.C. 120. [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.

31606313_1

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13371363	ORSINI ET AL.
	Examiner	**Art Unit**
	MICHAEL CHAO	2492

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

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

CLAIM		DATE								
Final	Original	05/02/2012	07/16/2012	03/12/2013						
	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	✓	✓	✓						
	26	✓	✓	✓						
	27	✓	✓	✓						

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13371363	ORSINI ET AL.
	Examiner	Art Unit
	MICHAEL CHAO	2492

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	26	5/4/2012	mc

SEARCH NOTES		
Search Notes	Date	Examiner
Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	5/4/2012	mc
Inventor name search in EAST	5/4/2012	mc
Assignee name search in EAST	5/4/2012	mc
google scholar searched "fountain OR erasure OR tornado OR LT OR raptor OR rateless code encrypted key hash OR fingerprint OR checksum"	5/4/2012	mc
updated Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	7/16/2012	mc
google searched "shamir secret sharing"	3/12/2013	mc
updated Text search of USPAT, US PGPUB, EPO, IBM TDB. See Search History Printout.	3/12/2013	mc

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/371,363	02/10/2012	Rick L. Orsini	104093-0002-105	7984

1473 7590 04/11/2013

ROPES & GRAY LLP
PATENT DOCKETING 39/361
1211 AVENUE OF THE AMERICAS
NEW YORK, NY 10036-8704

EXAMINER	
CHAO, MICHAEL W	
ART UNIT	**PAPER NUMBER**
2492	

NOTIFICATION DATE	DELIVERY MODE
04/11/2013	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):

USPatentMail@ropesgray.com
USPatentMail2@ropesgray.com

Office Action Summary	Application No.	Applicant(s)	
	13/371,363	ORSINI ET AL.	
	Examiner	Art Unit	
	Michael Chao	2492	

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

Period for Reply

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

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

Status

1)☒ Responsive to communication(s) filed on *20 September 2012*.

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

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

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

Disposition of Claims

5)☒ Claim(s) *1-27* is/are pending in the application.

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

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-27* 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 _____ 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).

a)☐ All b)☐ Some * c)☐ None of:

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

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

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

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

Attachment(s)

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

2) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *9/20/2012*.

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

4) ☐ Other: _____.

DETAILED ACTION

This action is in response to argument filed 9/20/2012. Application 13/371,363 claims priority to 10/25/2004. Claims 1-27 are pending and directed toward distributed data storage in an encrypted system.

Information Disclosure Statement

The information disclosure statement filed 9/20/2012 fails to comply with the provisions of 37 CFR 1.97, 1.98 and MPEP § 609 because it does not provide (B) a column that provides a space next to each document listed to permit the examiner's initials. It has been placed in the application file, but the information referred to therein has not been considered as to the merits. Applicant is advised that the date of any re-submission of any item of information contained in this information disclosure statement or the submission of any missing element(s) will be the date of submission for purposes of determining compliance with the requirements based on the time of filing the statement, including all certification requirements for statements under 37 CFR 1.97(e). See MPEP § 609.05(a).

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory

obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

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

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1-27 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-27 of U.S. Patent No. 8,271,802. Although the conflicting claims are not identical, they are not patentably distinct from each other because the claims sole distinguishing factor is that the claims of '802 substitute "integrity information" for the presently claimed "hash information". Integrity

information includes in its scope hash information as disclosed by Applicant in ¶¶ 394, 395.

Response to Arguments

Regarding Applicant's statement with respect to the amendment of claim 6 to include "secret sharing", such is not in compliance with the MPEP despite being incorporated by reference from a provisional application, see below.

Applicant's argument with regard to a hash "in the plurality of shares" (p. 10) is not persuasive. The claim itself requires "data indicative of [] the hash information" rather than the hash information itself. The data that is hashed is indicative of hash information. This is generated by the recipient of the data, thereby indicating the shares possession of "data indicative of hash information" "The recipient receives this message and forwards to ES the hash H(EK(C))" (Horne § 3). Horne in view of Li or, in the alternative Hand therefore discloses the required scope of the claim.

Applicant's further arguments are dependent upon those addressed and are unpersuasive for the reasons stated above.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-9 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

The claimed invention is not directed to patent eligible subject matter. Based upon consideration of all of the relevant factors with respect to the claim as a whole, claim(s) 1-9 is/are determined to be directed to an abstract idea. The rationale for this determination is explained below: The claim sets forth a method comprising a plurality of steps and the performance of mathematical algorithms. Taking into consideration the relevant factors the claim does not appear to require a machine. Even if such a machine were interpreted to be required the steps need not be performed by such a machine. Since it is unclear that a machine performs any of the steps, the claims are directed toward an abstract idea that is performable by a human operator. See MPEP 2106(1)(a).

Claim Rejections - 35 USC § 112

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

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 6, 15, 24 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The entirety of Applicant's support for a Shamir algorithm has been included below:

[0448] 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.

[0449] 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.

[0450] . . . The transformed encryption key may then be distributed among the data shares according to, for example, the Shamir algorithm or any other suitable algorithm.

While Applicant mentions that the support for the amended "Shamir secret sharing" may be found in provisional application 60/718,185; Applicant may not rely on a provisional for "essential material". "An application for a patent when filed may incorporate "essential material" by reference to (1) a U.S. patent, or (2) a U.S. patent application publication, which patent or patent application publication does not itself incorporate such essential material by reference. . . . "Essential material" is defined in 37 CFR 1.57(c) as that which is necessary to (1) provide a written description of the claimed invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and set forth the best mode contemplated by the inventor of carrying out the invention as required by the first paragraph of 35 U.S.C. 112" MPEP 608.01(p)(A). In other words, only published documents; provisional applications are not published but they do

provide sufficient support for Applicant to amend the specification without implicating the new matter concern.

Claim Rejections - 35 USC § 103

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

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

Claims 1-3, 5-12, 14-21, and 23-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Krawczyk (Secret Sharing Made Short) hereafter referred to as SSMS, in view of Krawczyk (Distributed Fingerprints and Secure Information Dispersal) hereafter referred to as DFSID, in view of Li (US 2006/0080454) or in the alternative in view of Hand (Spread Spectrum Storage with Mnemosyne).

With respect to claims 1, 10, 19, SSMS teaches: A method for securing a data set, the method steps implemented by a programmed computer system, the method steps comprising:

encrypting the data set based on an encryption key to produce an encrypted data set; ("1. Choose a random encryption key K. Encrypt the secret S using the encryption function ENC under the key K, let E = $ENC_K(S)$" SSMS p. 6).

[creating hash information based on a hash operation using the data set;

generating data splitting information, wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;]

separating the encrypted data set into the plurality of shares [based on the data splitting information;] ("2. Using IDA partition the encryption file E into n fragments, E_1, E_2, . . . , E_n." SSMS p. 6)("3. Using PSS generate n shares for the key K" SSMS p. 6)

including in the plurality of shares (a) data indicative of the encryption key and (b) the hash information; and ("4. Send to each participant P_i, I = 1, 2, . . . , n the share S_i = (E_i, K_i). The portion Ki is privately transmitted to Pi (e.g. using encryption or any other secure way)." SSMS p. 7)

causing the plurality of shares to be stored in respective separate storage locations; (to each participant. SSMS p. 7. "The distribution process gets ~ 1 sin put the secret S (and the values of n and m) and generates n shares Sl, Sz, . . , , Sn, which are privately delivered to the system participants." SSMS p. 3) (where the system is a set of distributed servers "These constructions have many applications, especially in distributed scenarios where secrecy and integrity of information are to be protected. For example, consider a group of five servers sharing a data base of confidential information such that no pair of servers is allowed to learn about the information without the collaboration of a third one. (That is, the system tolerates up to two corrupted servers without compromising the information)." SSMS p. 2)

wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares. (“The reconstruction process reconstructs the correct secret when input with any subset of m shares.” SSMS p. 3)

SSMS does not disclose:

creating hash information based on a hash operation using the data set;

generating data splitting information, wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;

DFSID discloses an analogous algorithm purposed for use with SSMS (DFSID § 5 referencing the SSMS disclosure as system architecture "[6]"). DFSID further discloses including the hash information in the plurality of shares: "

1. Use IDA to distribute the file among the n processors. Denote by F_i the piece distributed to processor p_i.

2. Fingerprint each piece F_i, i = 1, . . , n, by the DFP method (as described in Section 3). That is, for each i, compute $H(F_i)$ and then distribute this value among all processors using the coding function C. (Each processor p_j gets a share s_{ij} corresponding to $H(F_i)$)." (DFSID § 4.1, see also § 4.1 generally)

A fingerprint is a hash, see DFSID § 3.

A person of ordinary skill in the art at the time of invention would have modified SSMS by including the fingerprint of DFSID. It would have been obvious to one of ordinary skill in the art at the time of invention to modify SSMS with DFSID since it was

suggested explicitly by DFSID (DFSID § 5 referencing the SSMS disclosure as system architecture "[6]") and to solve the information integrity problem (DFSID Abstract).

SSMS in view of DFSID does not disclose:

generating data splitting information, wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;

(1) Li discloses a similar system directed toward peer distribution (Li [0003]) using erasure/error coding (Li [0106]). Li further discloses a method for selecting the peers for storing data ("each peer node is assigned k keys in the coded message space of n, with each key being the row index of the generator matrix G. The key assignment may be carried out by the server. Further, if the number of peers caching the media is smaller than n/k, it is possible to assign each peer a unique set of keys. As a result, it can be guaranteed that each peer holds distinctive coded messages. While this strategy provides a number of benefits, it still requires a central coordination node (such as the server)." Li [0109]; alternatively "in another embodiment, the role of the central coordination node is eliminated by allowing each peer to choose k random keys." Li [0110]). Note that, as used in Li, keys are referring to the erasure coding blocks held by a peer and are not cryptographic keys. ("the availability vector will include the media erasure coding keys assigned to serving peer, and the number of erasure blocks held by the serving peer. In addition, if the serving peer uses erasure coding and the media is also embedded coded, the availability vector will include the assigned media erasure coding keys" Li [0065])

A person of ordinary skill in the art at the time of invention would have combined SSMS in view of DFSID with Li by using the concepts of Li to implement the distribution of shares (SSMS p. 2). It would have been obvious to one of ordinary skill in the art at the time of invention to combine SSMS in view of DFSID with Li in order to implement necessary but unspecified functionality of Horne using a solution disclosed in a similar system (Li [0109-10]).

(2) In the alternative, Hand discloses a similar system directed to distributed (Hand § 27.1 ¶ 1) erasure coded fragments for data storage (Hand § 27.1 ¶ 2). Hand additionally discloses a method for distributing the data, as claimed: wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;

("Location: Mnemosyne achieves its security properties by storing encrypted data blocks in pseudo-random (and, to an adversary, unpredictable) locations in a large virtual network store, which is then mapped onto distributed physical storage devices. The locations of the encrypted blocks making up a data set are determined by a sequence of 256-bit values obtained by successively hashing an initial value which depends ultimately on the filename and the user's key K.

Distribution: The sequence of 256-bit location identifiers from the previous step is finally mapped onto physical storage using a peer-to-peer network of storage nodes, each of which holds a fixed-size physical block store." Hand § 27.2 ¶ 6-7).

A person of ordinary skill in the art at the time of invention would have combined SSMS in view of DFSID with Hand by using the concepts of Hand to implement the distribution of shares (SSMS p. 2). It would have been obvious to one of ordinary skill in the art at the time of invention to combine Horne with Hand in order to implement necessary but unspecified functionality of SSMS in view of DFSID using a solution disclosed in a similar system Hand § 27.2 ¶ 6-7).

With respect to claims 2, 11, 20, SSMS in view of DFSID in view of {Li or, in the alternative, Hand} discloses: wherein the step of separating the encrypted data set comprises using a deterministic technique. (determinism is a necessary feature of any system that will retrieve obfuscated data)

With respect to claims 3, 12, 21, SSMS in view of DFSID in view of {Li or, in the alternative, Hand} discloses: wherein the step of separating the encrypted data set comprises using a substantially random technique. ("An (n,m)-secret sharing scheme is a randomized protocol for the distribution of a secret S among n parties such that the recovery of the secret is possible out of m shares for a fixed value m, 1 <= m <= n, while m - 1 shares give no information on the secret S" SSMS § 2)

With respect to claims 5, 14, 23, SSMS in view of DFSID in view of {Li or, in the alternative, Hand} discloses: wherein the step of separating the encrypted data into the plurality of shares comprises causing the plurality of shares to have a substantially

randomly distribution of the encrypted data set. (“An (n,m)-secret sharing scheme is a randomized protocol for the distribution of a secret S among n parties such that the recovery of the secret is possible out of m shares for a fixed value m, 1 <= m <= n, while m - 1 shares give no information on the secret S” SSMS § 2)

With respect to claims 6, 15, 24, SSMS in view of DFSID in view of {Li or, in the alternative, Hand} discloses: wherein the data indicative of the encryption key comprises data created using a Shamir secret sharing algorithm. (“In order to achieve a space efficient secret sharing scheme we combine an information dispersal scheme with a secure encryption scheme and a perfect (e.g. Shamir’s) secret sharing scheme.” SSMS § 3)

With respect to claims 7, 16, 25, SSMS in view of DFSID in view of {Li or, in the alternative, Hand} discloses: wherein the step of including data indicative of the encryption key comprises:
encrypting the encryption key with a second key; and
including in the plurality of shares data indicative of the encrypted encryption key. (“The portion Ki is privately transmitted to Pi (e.g. using encryption or any other secure way).” SSMS p. 7. Encryption requires a key of some kind.)

With respect to claims 8, 17, 26, SSMS in view of DFSID in view of {Li or, in the alternative, Hand} discloses: further comprising the method step of storing the second

key outside of the plurality of shares, wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares, and the second key. ("An (n,m)-secret sharing scheme is a randomized protocol for the distribution of a secret S among n parties such that the recovery of the secret is possible out of m shares for a fixed value m, 1 <= m <= n, while m - 1 shares give no information on the secret S" SSMS § 2).

With respect to claims 9, 18, 27, SSMS in view of DFSID in view of {Li or, in the alternative, Hand} discloses: wherein the step of storing the shares in respective separate storage locations comprises storing the shares on at least two separate storage devices.

Claims 4, 13, 22, are rejected under 35 U.S.C. 103(a) as being unpatentable over SSMS in view of DFSID in view of [Li (US 2006/0080454) or in the alternative Hand (Spread Spectrum Storage with Mnemosyne)] in view of Kubiatowicz (OceanStore).

With respect to claims 4, 13, and 22, SSMS in view of DFSID in view of Li or Hand does not disclose: further comprising causing a plurality of data units in each of the shares to be rearranged relative to one another after the separating step.

Kubiatowicz discloses a similar system based on distributed storage (Kubiatowicz § 2 figure 1) of erasure codes (Kubiatowicz § 4.5). Kubiatowicz further discloses a method of updating the data objects.

("Objects in the OceanStore are modified through updates. Updates contain information about what changes to make to an object and the assumed state of the object under which those changes were developed, much as in the Bayou system [13]. In principle, every update to an OceanStore object creates a new version2. Consistency based on versioning, while more expensive to implement than update-in-place consistency, provides for cleaner recovery in the face of system failures [49]. It also obviates the need for backup and supports "permanent" pointers to information." Kubiatowicz § 2 ¶ 4) ("For the user, we provide a naming syntax which explicitly incorporates version numbers. Such names can be included in other documents as a form of permanent hyper-link. In addition, interfaces will exist to examine modification history and to set versioning policies [44]. Although in principle every version of every object is archived, clients can choose to produce versions less frequently. Archival copies are also produced when objects are idle for a long time or before objects become inactive. When generating archival fragments, the floating replicas of an object participate together: they each generate a disjoint subset of the fragments and disseminate them into the infrastructure." Kubiatowicz § 4.5 ¶4).

A person of ordinary skill in the art would have modified SSMS in view of DFSID in view of Li (or Hand) with Kubiatowicz by providing a method for versioning the files to be distributed as disclosed in Kubiatowicz. It would have been obvious to one of ordinary skill in the art at the time of invention to allow versioning of the files so that users could update the files thereby allowing for flexibility of the media storage.

In the alternative, Claims 1-3, 5, 7-12, 14, 16-21, 23, and 25-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Horne et al. (Escrow Services and Incentives in Peer-to-Peer Networks) in view of Li (US 2006/0080454) or in the alternative in view of Hand (Spread Spectrum Storage with Mnemosyne).

With respect to claims 1, 10, 19, Horne teaches: A method for securing a data set, the method steps implemented by a programmed computer system, the method steps comprising:

encrypting the data set based on an encryption key to produce an encrypted data set; ("In the protocol that we describe, S encrypts C with a key K and sends the encryption EK(C)to R." Horne 2.2 ¶ 3)

creating hash information based on a hash operation using the data set; ("In order to take part in the protocol ES requires the correct hash of the encrypted content, H(EK(C)), and the key K that decrypts the content. . . . we assume that S sent the pair K,H(EK(C))———————————— to ES in a preprocessing stage, together with a description of C." Horne 2.2 ¶ 3; see also Horne § 4.2)

generating data splitting information, ("A Straightforward Method Based on Error Correcting Codes" Horne § 4.1) [wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;]

separating the encrypted data set into the plurality of shares based on the data splitting information; ("Distributed file storage: In this model files are not stored at a single server. Instead, a file is divided into many blocks encoded with an error correcting code, and each block is stored at a different location (this is the storage method used by Mojonation.com). The use of error correcting codes ensures that the file can be restored even if part of the peers that store parts of the file are unavailable or corrupt. The directory service might be centralized or distributed. Our ES service can cooperate with this storage system, where the use of error correcting codes we suggest in Section 4 might use (or might not use) the same error correcting code as the storage method." Horne § 5 ¶ 4)

including in the plurality of shares data indicative of (a) the encryption key and (b) the hash information; and ("In order to obtain the key K, R computes the hash of the encrypted content H(EK(C)) and sends it to ES, together with a description of the content C it desires to obtain, and the identity of S. It also sends a payment for the content C, which will only be processed if the content is valid (step 2)." Horne § 2.2 ¶ 7; "After receiving this message R picks a small random set of of the encrypted encoded blocks (where is a parameter to be defined below). It sends to ES this set of encrypted blocks, together with their indexes and the encrypted message that is directed from S to ES." Horne § 4.1 ¶ 3; "In order to verify the encrypted content that it receives from S, R should forward this signature and randomly chosen encrypted blocks to ES." Horne § 4.2 ¶ 8)

causing the plurality of shares to be stored in respective separate storage locations; (Horne § 5 ¶ 4)

wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares. ("The scheme could either use error correction codes, or use more efficient erasure codes. We first examine the use of error correction codes. The codes have the property that given n blocks, such that at least t of them are correct (although the receiver does not know which ones these are), the receiver can reconstruct the original message." Horne § 4.1 ¶ 6).

Although Horne discloses that a distributed storage system may be used (Horne § 5 ¶ 4) it does not disclose how the data is distributed among the stores, as claimed:

wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;

Li discloses a similar system directed toward peer distribution (Li [0003]) using erasure/error coding (Li [0106]). Li further discloses a method for selecting the peers for storing data ("each peer node is assigned k keys in the coded message space of n, with each key being the row index of the generator matrix G. The key assignment may be carried out by the server. Further, if the number of peers caching the media is smaller than n/k, it is possible to assign each peer a unique set of keys. As a result, it can be guaranteed that each peer holds distinctive coded messages. While this strategy provides a number of benefits, it still requires a central coordination node (such as the server)." Li [0109]; alternatively "in another embodiment, the role of the central coordination node is eliminated by allowing each peer to choose k random keys." Li

[0110]). Note that, as used in Li, keys are referring to the erasure coding blocks held by a peer and are not cryptographic keys. ("the availability vector will include the media erasure coding keys assigned to serving peer, and the number of erasure blocks held by the serving peer. In addition, if the serving peer uses erasure coding and the media is also embedded coded, the availability vector will include the assigned media erasure coding keys" Li [0065])

A person of ordinary skill in the art at the time of invention would have combined Horne with Li by using the concepts of Li to implement the distribution of erasure coded blocks in Horne (Horne § 5 ¶ 4). It would have been obvious to one of ordinary skill in the art at the time of invention to combine Horne with Li in order to implement necessary but unspecified functionality of Horne using a solution disclosed in a similar system (Li [0109-10]).

In the alternative, Hand discloses a similar system directed to distributed (Hand § 27.1 ¶ 1) erasure coded fragments for data storage (Hand § 27.1 ¶ 2). Hand additionally discloses a method for distributing the data, as claimed: wherein the data splitting information is usable to determine into which of a plurality of shares of data a unit of data of the encrypted data set will be placed;

("Location: Mnemosyne achieves its security properties by storing encrypted data blocks in pseudo-random (and, to an adversary, unpredictable) locations in a large virtual network store, which is then mapped onto distributed physical storage devices. The locations of the encrypted blocks making up a data set are determined by a

sequence of 256-bit values obtained by successively hashing an initial value which depends ultimately on the filename and the user's key K.

Distribution: The sequence of 256-bit location identifiers from the previous step is finally mapped onto physical storage using a peer-to-peer network of storage nodes, each of which holds a fixed-size physical block store." Hand § 27.2 ¶ 6-7).

A person of ordinary skill in the art at the time of invention would have combined Horne with Hand by using the concepts of Hand to implement the distribution of erasure coded blocks in Horne (Horne § 5 ¶ 4). It would have been obvious to one of ordinary skill in the art at the time of invention to combine Horne with Hand in order to implement necessary but unspecified functionality of Horne using a solution disclosed in a similar system Hand § 27.2 ¶ 6-7).

With respect to claims 2, 11, 20, Horne in view of Li or Hand discloses: wherein the step of separating the encrypted data set comprises using a deterministic technique. ("each peer node is assigned k keys in the coded message space of n, with each key being the row index of the generator matrix G. The key assignment may be carried out by the server. Further, if the number of peers caching the media is smaller than n/k, it is possible to assign each peer a unique set of keys. As a result, it can be guaranteed that each peer holds distinctive coded messages. While this strategy provides a number of benefits, it still requires a central coordination node (such as the server)." Li [0109]) ("The locations of the encrypted blocks making up a data set are determined by a

sequence of 256-bit values obtained by successively hashing an initial value which depends ultimately on the filename and the user's key K." Hand § 27.2 ¶ 6-7).

With respect to claims 3, 12, 21, Horne in view of Li or Hand discloses: wherein the step of separating the encrypted data set comprises using a substantially random technique. ("in another embodiment, the role of the central coordination node is eliminated by allowing each peer to choose k random keys." Li [0110]) ("Location: Mnemosyne achieves its security properties by storing encrypted data blocks in pseudo-random (and, to an adversary, unpredictable) locations in a large virtual network store, which is then mapped onto distributed physical storage devices." Hand § 27.2 ¶ 6-7; thus as disclosed by Hand, the process is 'random' despite being deterministic due to a consistent result given the same inputs)

With respect to claims 5, 14, 23, Horne in view of Li or Hand discloses: wherein the step of separating the encrypted data into the plurality of shares comprises causing the plurality of shares to have a substantially random distribution of the encrypted data set. ("in another embodiment, the role of the central coordination node is eliminated by allowing each peer to choose k random keys." Li [0110]) ("Location: Mnemosyne achieves its security properties by storing encrypted data blocks in pseudo-random (and, to an adversary, unpredictable) locations in a large virtual network store, which is then mapped onto distributed physical storage devices." Hand § 27.2 ¶ 6-7; thus as

disclosed by Hand, the process is 'random' despite being deterministic due to a consistent result given the same inputs).

With respect to claims 7, 16, 25, Horne in view of Li or Hand discloses: wherein the step of including data indicative of the encryption key comprises:

Encrypting the encryption key with a second key; and. ("It then sends these blocks to R together with the key K encrypted with the public key of ES." Horne § 4.1 ¶ 2)

Including in the plurality of shares data indicative of the encrypted encryption key.("In order to obtain the key K, R computes the hash of the encrypted content H(EK(C)) and sends it to ES, together with a description of the content C it desires to obtain, and the identity of S. It also sends a payment for the content C, which will only be processed if the content is valid (step 2)." Horne § 2.2 ¶ 7).

With respect to claims 8, 17, 26, Horne in view of Li or Hand discloses: further comprising the method step of storing the second key outside of the plurality of shares ("It then sends these blocks to R together with the key K encrypted with the public key of ES." Horne § 4.1 ¶ 2; ES is distinct from source S and receiver R), wherein the data set is restorable by accessing less than all, but at least a threshold number of, the plurality of shares, and the second key. ("The scheme could either use error correction codes, or use more efficient erasure codes. We first examine the use of error correction codes. The codes have the property that given n blocks, such that at least t of them are

correct (although the receiver does not know which ones these are), the receiver can reconstruct the original message." Horne § 4.1 ¶ 6).

With respect to claims 9, 18, 27, Horne in view of Li or Hand discloses: wherein the step of storing the shares in respective separate storage locations comprises storing the shares on at least two separate storage devices. ("Distributed file storage: In this model files are not stored at a single server. Instead, a file is divided into many blocks encoded with an error correcting code, and each block is stored at a different location (this is the storage method used by Mojonation.com). The use of error correcting codes ensures that the file can be restored even if part of the peers that store parts of the file are unavailable or corrupt. The directory service might be centralized or distributed. Our ES service can cooperate with this storage system, where the use of error correcting codes we suggest in Section 4 might use (or might not use) the same error correcting code as the storage method." Horne § 5 ¶ 4)

Claims 4, 13, 22, are rejected under 35 U.S.C. 103(a) as being unpatentable over Horne et al. (Escrow Services and Incentives in Peer-to-Peer Networks) in view of [Li (US 2006/0080454) or in the alternative Hand (Spread Spectrum Storage with Mnemosyne)] in view of Kubiatowicz (OceanStore).

With respect to claims 4, 13, and 22, Horne in view of Li or Hand does not disclose: further comprising causing a plurality of data units in each of the shares to be rearranged relative to one another after the separating step.

Kubiatowicz discloses a similar system based on distributed storage (Kubiatowicz § 2 figure 1) of erasure codes (Kubiatowicz § 4.5). Kubiatowicz further discloses a method of updating the data objects.

("Objects in the OceanStore are modified through updates. Updates contain information about what changes to make to an object and the assumed state of the object under which those changes were developed, much as in the Bayou system [13]. In principle, every update to an OceanStore object creates a new version2. Consistency based on versioning, while more expensive to implement than update-in-place consistency, provides for cleaner recovery in the face of system failures [49]. It also obviates the need for backup and supports "permanent" pointers to information." Kubiatowicz § 2 ¶ 4) ("For the user, we provide a naming syntax which explicitly incorporates version numbers. Such names can be included in other documents as a form of permanent hyper-link. In addition, interfaces will exist to examine modification history and to set versioning policies [44]. Although in principle every version of every object is archived, clients can choose to produce versions less frequently. Archival copies are also produced when objects are idle for a long time or before objects become inactive. When generating archival fragments, the floating replicas of an object participate together: they each generate a disjoint subset of the fragments and disseminate them into the infrastructure." Kubiatowicz § 4.5 ¶4).

A person of ordinary skill in the art would have modified Horne in view of Li (or Hand) with Kubiatowicz by providing a method for versioning the files to be distributed as disclosed in Kubiatowicz. It would have been obvious to one of ordinary skill in the

art at the time of invention to allow versioning of the files so that users could update the files thereby allowing for flexibility of the media storage.

Claims 6, 15, 24, are rejected under 35 U.S.C. 103(a) as being unpatentable over Horne et al. (Escrow Services and Incentives in Peer-to-Peer Networks) in view of [Li (US 2006/0080454) or in the alternative in view of Hand (Spread Spectrum Storage with Mnemosyne)] in view of SSMS.

With respect to claims 6, 15, and 24 Horne in view of Li or Hand discloses: wherein the data indicative of the encryption key comprises data created using a [Shamir secret sharing algorithm]. ("The encryption can be done using public key cryptography" Horne § 2.1.2 ¶ 5) ("It then sends these blocks to R together with the key K encrypted with the public key of ES." Horne § 4.1 ¶ 2). While Horne does disclose the use of a public key encryption, it does not disclose a Shamir Algorithm. SSMS discloses a Shamir secret sharing algorithms use with coded data ("In order to achieve a space efficient secret sharing scheme we combine an information dispersal scheme with a secure encryption scheme and a perfect (e.g. Shamir's) secret sharing scheme." SSMS § 3). A person of ordinary skill in the art at the time of invention would have modified Horne in view of {Li or, in the alternative, Hand} with SSMS by utilizing the key splitting mechanism of SSMS with the combination. It would have been obvious to one of ordinary skill in the art at the time of invention to use the key splitting of SSMS in order to create space efficient secured secret shares (SSMS § 1).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Chao whose telephone number is (571)270-5657. The examiner can normally be reached on 8-4 Monday through Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Saleh Najjar can be reached on (571)272-4006. 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.

/Michael Chao/
Examiner, Art Unit 2492

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/371,363	02/10/2012	Rick L. Orsini	104093-0002-105	7984

1473 7590 06/03/2013

ROPES & GRAY LLP
PATENT DOCKETING 39/361
1211 AVENUE OF THE AMERICAS
NEW YORK, NY 10036-8704

EXAMINER	
CHAO, MICHAEL W	
ART UNIT	**PAPER NUMBER**
2492	

NOTIFICATION DATE	DELIVERY MODE
06/03/2013	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):

USPatentMail@ropesgray.com
USPatentMail2@ropesgray.com

Applicant-Initiated Interview Summary	Application No.	Applicant(s)	
	13/371,363	ORSINI ET AL.	
	Examiner	Art Unit	
	Michael Chao	2492	

All participants (applicant, applicant's representative, PTO personnel):

(1) *Michael Chao*.

(2) *Christopher Han (Reg. No. 70,069)*.

(3) *Regina Sam (Reg. No. 67,362)*.

(4)_____.

Date of Interview: *21 May 2013*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☐ No.
If Yes, brief description: _____.

Issues Discussed ☒101 ☒112 ☐102 ☒103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1*.

Identification of prior art discussed: *Krawczyk references (Short Secret Sharing) and (Distributed Fingerprints and Secure Information Dispersal)*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Applicant's representatives and Examiner discussed the rationals of the 112 and 101 rejections. Applicant's representatives pointed out that the shares include (b) hash information as well as (a) information indicative of the encryption key. Examiner agreed with Applicant's interpretation of the claim and that the response to arguments in the last office action (4/11/2013) was incorrect in view thereof. Examiner expressed his belief that the Krawczyk references disclosed the argued limitations (a) and (b). No agreement was reached..

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

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

☐ Attachment

/Michael Chao/ Examiner, Art Unit 2492	/saleh najjar/ Supervisory Patent Examiner, Art Unit 2492

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

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

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

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

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

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

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

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

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

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

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

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

Examiner to Check for Accuracy

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

Docket No.: 104093-0002-105
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Orsini et al.

Application No.: 13/371,363 | Confirmation No.: 7984

Filed: February 10, 2012 | Art Unit: 2492

For: SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA | Examiner: M. W. Chao

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT (IDS)

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

Dear Madam:

Pursuant to 37 C.F.R. § 1.56, 1.97 and 1.98, the attention of the Patent and Trademark Office is hereby directed to the references listed on the attached PTO/SB/08. It is respectfully requested that the information be expressly considered during the prosecution of this application, and that the references be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Supplemental Information Disclosure Statement is filed more than three months after the U.S. filing date, OR more than three months after the date of entry of the national stage of a PCT application, AND after the mailing date of the first Office Action on the merits, whichever occurs first, but before the mailing date of any of a Final Office Action, a Notice of Allowance (37 C.F.R. § 1.97(c)) or an action that otherwise closes prosecution in the application.

In accordance with 37 C.F.R. § 1.98(a)(2)(ii), Applicant has not submitted copies of U.S. patents and U.S. patent applications. Applicant submits herewith copies of foreign patents and non-patent literature in accordance with 37 C.F.R. § 1.98(a)(2).

In accordance with 37 C.F.R. § 1.97(g), the filing of this Supplemental Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 C.F.R. § 1.56(a) exists. In accordance with 37 C.F.R. § 1.97(h), the filing of this Supplemental Information Disclosure Statement shall not be construed to be an admission that any patent, publication or other information referred to therein is "prior art" for this invention unless specifically designated as such.

Notice of Related Patent Applications

The Examiner is advised that the following patent applications contain subject matter that may be related to the pending claims in the present application. In particular, Applicants would like to draw the Examiner's attention to the fact that substantive examination may have occurred in these cases. For these cases, copies of any Office Actions that have issued and Replies that have been filed in these cases that have not been previously submitted are submitted herewith, and a corresponding entry for the Examiner's initials has been added on the form PTO/SB/08b filed concurrently herewith. Applicants invite the Examiner to review these documents or any future substantive documents that will issue or be filed in any of the below cases. By bringing the following applications to the Examiner's attention, applicants do not waive any applicable confidentiality provisions of 35 U.S.C. 122.

Application No.	**Publication No.**	**Attorney Docket No.**	**Filing Date**	**Status**
12/148,365	US 2008-0244277	104093-0001-102	4/18/2008	Pending
13/024,791	US 2011-0179287	104093-0001-103	2/10/2011	Pending
13/024,804	US 2011-0179271	104093-0001-104	2/10/2011	Pending
13/371,364	US 2012-0159197	104093-0002-106	2/10/2012	Pending

It is submitted that the Supplemental Information Disclosure Statement is in compliance with 37 C.F.R. § 1.98 and the Examiner is respectfully requested to consider the listed references.

Please charge our Deposit Account No. 06-1075 in the amount of $180.00 covering the fee set forth in 37 C.F.R. § 1.17(p). 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, under Order No. 104093-0002-105.

Dated: July 11, 2013

Respectfully submitted,

Electronic signature: /Christopher J. Han/
Christopher J. Han
Registration No.: 70,069
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, Massachusetts 02199
(617) 951-7000
(617) 235-9492 (Fax)
Attorneys/Agents 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.
13/371,363	02/10/2012	Rick L. Orsini	104093-0002-105	7984

1473 7590 07/11/2013

ROPES & GRAY LLP
PATENT DOCKETING 39/361
1211 AVENUE OF THE AMERICAS
NEW YORK, NY 10036-8704

EXAMINER	
CHAO, MICHAEL W	
ART UNIT	**PAPER NUMBER**
2492	

NOTIFICATION DATE	DELIVERY MODE
07/11/2013	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):

USPatentMail@ropesgray.com
USPatentMail2@ropesgray.com

Applicant-Initiated Interview Summary	Application No.	Applicant(s)	
	13/371,363	ORSINI ET AL.	
	Examiner	Art Unit	
	Michael Chao	2492	

All participants (applicant, applicant's representative, PTO personnel):

(1) *Michael Chao*.

(2) *Christopher Han (Reg. No. 70,069)*.

(3) *Regina Sam (Reg. No. 67,362)*.

(4) _____.

Date of Interview: *26 June 2013*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☒103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1*.

Identification of prior art discussed: *Krawczyk references {Secret Sharing Made Short; Distributed Fingerprints and Secure Information Dispersal}, Li (US 2006/0080454), Hand (Spread Spectrum Storage with Mnemosyne)*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Applicant's representatives and Examiner discussed the limitations dealing with "data splitting information" and potential interpretations with respect to the prior art. No agreement was reached.

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

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

☐ Attachment

/Michael Chao/ Examiner, Art Unit 2492	/saleh najjar/ Supervisory Patent Examiner, Art Unit 2492

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

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

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

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

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

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

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

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

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

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

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

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

Examiner to Check for Accuracy

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

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 5

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

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
		US-8,307,443	11-06-2012	Wang et al.	
		US-8,261,265	09-04-2012	Chen et al.	
		US-8,250,643	08-21-2012	Enomoto et al.	
		US-8,195,976	06-05-2012	Rao et al.	
		US-8,060,088	11-15-2011	Ihattula	
		US-7,926,090	04-12-2011	Blevins et al.	
		US-7,921,288	04-05-2011	Hildebrand	
		US-7,865,741	01-04-2011	Wood et al.	
		US-7,801,781	09-21-2010	Olin et al.	
		US-7,756,792	07-13-2010	Hughes	
		US-7,752,482	07-06-2010	Gredone et al.	
		US-7,721,150	05-18-2010	Belyakov et al.	
		US-7,623,809	11-24-2009	Nakano et al.	
		US-7,535,905	05-19-2009	Narayanan et al.	
		US-7,478,427	01-13-2009	Mukherjee et al.	
		US-7,428,754	09-23-2008	Neumann et al.	
		US-7,363,361	04-22-2008	Tewari et al.	
		US-7,346,925	03-18-2008	Marcjan	
		US-7,140,044	11-21-2006	Redlich et al.	

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]
		JP-2006-174152-A	06-29-2006	Matsushita Electric Works Ltd.		√

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. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [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.

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 5

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

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
		US-7,107,385	09-12-2006	Rajan et al.	
		US-7,085,854	08-01-2006	Corente	
		US-7,003,668	02-21-2006	Berson et al.	
		US-6,915,436	07-05-2005	Booth, III et al.	
		US-6,785,768	08-31-2004	Peters et al.	
		US-6,505,216	01-07-2003	Schutzman et al.	
		US-6,415,373	07-02-2002	Peters et al.	
		US-5,666,514	09-09-1997	Cheriton	
		US-5,623,549	04-22-1997	Ritter	
		US-5,603,003	02-11-1997	Akizawa et al.	
		US-2013/0042105	02-14-2013	Orsini et al.	
		US-2012/0266231	10-18-2012	Spiers et al.	
		US-2012/0255035	10-04-2012	Orsini et al.	
		US-2012/0255034	10-04-2012	Orsini et al.	
		US-2011/0145413	06-16-2011	Dawson et al.	
		US-2011/0093113	04-21-2011	Sager et al.	
		US-2010/0332617	12-30-2010	Goodwin et al.	
		US-2010/0318812	12-16-2010	Auradkar et al.	
		US-2010/0283734	11-11-2010	Hallbauer et al.	

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]

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. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [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.

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 3 of 5

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

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
		US-2010/0223613	09-02-2010	Schneider	
		US-2010/0125730	05-20-2010	Dodgson et al.	
		US-2010/0005028	01-07-2010	Hartley et al.	
		US-2009/0305900	12-10-2009	Belouchi et al.	
		US-2009/0300284	12-03-2009	Murotani et al.	
		US-2009/0292919	11-26-2009	England	
		US-2009/0209232	08-20-2009	Cha et al.	
		US-2009/0113203	04-30-2009	Tsuge et al.	
		US-2009/0097657	04-16-2009	Scheidt et al.	
		US-2009/0092252	04-09-2009	Noll et al.	
		US-2008/0240441	10-02-2008	Kawakami	
		US-2008/0232592	09-25-2008	Lee et al.	
		US-2008/0155252	06-26-2008	Nambiar	
		US-2008/0126614	05-29-2008	Ooi et al.	
		US-2008/0072035	03-20-2008	Johnson et al.	
		US-2008/0046752	02-21-2008	Berger et al.	
		US-2008/0016334	01-17-2008	Kurapati et al.	
		US-2007/0097885	05-03-2007	Traversat et al.	
		US-2006/0165060	07-27-2006	Dua	

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]

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. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [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.

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 4 of 5

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

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
		US-2006/0078127	04-13-2006	Cacayorin	
		US-2006/0046728	03-02-2006	Jung et al.	
		US-2005/0198306	09-08-2005	Palojarvi et al.	
		US-2005/0160290	07-21-2005	Moon et al.	
		US-2005/0132060	06-16-2005	Mo et al.	
		US-2005/0071631	03-31-2005	Langer	
		US-2004/0122960	06-24-2004	Hall et al.	
		US-2003/0084290	05-01-2003	Murty et al.	
		US-2003/0061481	03-27-2003	Levine et al.	
		US-2003/0023958	01-30-2003	Patel et al.	
		US-2003/0005094	01-02-2003	YUAN et al.	
		US-2002/0184444	12-05-2002	Shandony	
		US-2002/0178361	11-28-2002	Genty et al.	
		US-2002/0141590	10-03-2002	Montgomery	
		US-2002/0023210	02-21-2002	Tuomenoksa et al.	
		US-2002/0016926	02-07-2002	Nguyen et al.	
		US-2007/157025	07-05-2007	Sastry et al.	
		US-2010/0077252	03-25-2010	Siewert et al.	
		US-2010/0306578	12-02-2010	THORNTON et al.	
		US-8,397,288	03-12-3013	Melvin, Jr. et al.	
		US-8,341,115	12-25-2012	Natanzon et al.	
		US-8,261,084	09-04-2012	Nonaka et al.	
		US-7,743,261	06-22-2010	Nonaka et al.	
		US-7,596,741	09-29-2009	LaVigne et al.	
		US-7,549,061	06-16-2009	Nonaka et al.	

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]

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. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. [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.

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 5 of 5

Complete if Known	
Application Number	13/371,363
Filing Date	February 10, 2012
First Named Inventor	Rick L. Orsini
Art Unit	2492
Examiner Name	M. W. Chao
Attorney Docket Number	104093-0002-105

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	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[2]
		Dierks, "The Transport Layer Security Protocol," RFC 4346m Version 1.1, April 2006, 86 pages	
		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.	
		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	
		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	
		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)	
		Copies of Office Actions and Replies for U.S. Application No. 12/148,365 (104093-0001-102)	
		Copies of Office Actions and replies for U.S. Application No. 13/024,791 (104093-0001-103)	
		Copies of Office Actions and replies for U.S. Application No. 13/024,804 (104093-000-104)	
		Copies of Office Actions and Replies for U.S. Application No. 13/371,364 (104093-0002-106)	

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]Applicant is to place a check mark here if English language Translation is attached.

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 13/371,363	Filing Date 02/10/2012	☐ 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 $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $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	07/11/2013	(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))	* 27	Minus	** 27	= 0	X $80 =	0
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $420 =	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 $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
	☐ 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.
** 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 number found in the appropriate box in column 1.

LIE
/RENEE HAWKINS/

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.

Electronic Acknowledgement Receipt

EFS ID:	16284612
Application Number:	13371363
International Application Number:	
Confirmation Number:	7984
Title of Invention:	SYSTEMS AND METHODS FOR CRYPTOGRAPHICALLY SPLITTING AND STORING DATA
First Named Inventor/Applicant Name:	Rick L. Orsini
Customer Number:	1473
Filer:	Christopher Jinhyun Han/Joanne Ryan
Filer Authorized By:	Christopher Jinhyun Han
Attorney Docket Number:	104093-0002-105
Receipt Date:	11-JUL-2013
Filing Date:	10-FEB-2012
Time Stamp:	14:13:40
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$340
RAM confirmation Number	449
Deposit Account	061075
Authorized User	

File Listing:

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

1	Terminal Disclaimer Filed	104093-0002-105_Terminal_Disclaimer.pdf	78939 94a584824de0bc7029401c4ae67a65dd80a5fb20	no	1
Warnings:					
Information:					
2		104093-0002-105_NonFinal_Response.pdf	159031 966d40cec093e33ab36b89a6bd6265fde9336f7c	yes	12
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Amendment/Req. Reconsideration-After Non-Final Reject		1	1	
	Specification		2	2	
	Claims		3	8	
	Applicant Arguments/Remarks Made in an Amendment		9	12	
Warnings:					
Information:					
3	Information Disclosure Statement (IDS) Form (SB08)	104093-0002-105_SB08.pdf	167381 b20419a45f4f272c3ad358b21a596f8a0ed73189	no	5
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
4	Foreign Reference	JP2006174152_with_English_Translation.pdf	9563668 a1ed8a75580b9470957fc12ccc5a44b99ad293d9	no	137
Warnings:					
Information:					
5	Non Patent Literature	Dierks_Transport_Layer_Security_Protocol.pdf	3053557 13c8de19039198ae07ee6cc99be115f6fbad05c5	no	87
Warnings:					
Information:					
6	Non Patent Literature	Johnson_MLS_Net.pdf	652266 f82576ad06e4bdcade2bc68cdf2e71e8e470509d	no	8
Warnings:					
Information:					
7	Non Patent Literature	Kent_Security_Architecture_for_the_Internet_Protocol.pdf	2711704 f3173ad1607c6917c873063b7549911ffa27b691	no	67

Warnings:					
Information:					
8	Non Patent Literature	Kroc_Access_Control.pdf	20660511 ea5db491d62dbbf6446a305778b8a8a6353 42bd1	no	155
Warnings:					
Information:					
9	Non Patent Literature	Pattam_Enhancing_Security_in_802.pdf	5108596 b43bd2dcae6797aed0dab34ff05c602bca9 a5598	no	111
Warnings:					
Information:					
10	Non Patent Literature	Sengar_et_al_MTPSec_Customizable_Secure_MTP3_Tunnels.pdf	721387 9dc12cede78fcd19d67c4ca5193d38d94dc 393b9	no	8
Warnings:					
Information:					
11	Non Patent Literature	12148365_OAs_and_Replies.pdf	12198392 ede765004bf8bd02d206a863eaad4c2192b 26a7a	no	249
Warnings:					
Information:					
12	Non Patent Literature	13024791_OAs_and_Replies.pdf	3451820 82d4ee5f4424390b0662c1623718c5d982f 29f0b	no	92
Warnings:					
Information:					
13	Non Patent Literature	13024804_OAs_and_Replies.pdf	3886588 bed4afa2ca56b9680980481ae971cb13af3e d124	no	95
Warnings:					
Information:					
14	Non Patent Literature	13371364_OAs_and_Replies.pdf	3916353 aa0cd8dca13e62d41b3421b81e4a8c12ea9 7a087	no	93
Warnings:					
Information:					
15	Transmittal Letter	104093-0002-105_Supp_IDS.pdf	79210 75b96b9e06ff23e08716bff8c1ecff88c87c9 30e	no	3
Warnings:					
Information:					
16	Fee Worksheet (SB06)	fee-info.pdf	31896 d699aebb1d24e6cb493b87dd41eb82f49f1 08d34	no	2

Warnings:	
Information:	
Total Files Size (in bytes):	66441299

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.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2006-174152**
(43)Date of publication of application : **29.06.2006**

(51)Int.Cl. *H04L 9/32 (2006.01)*
H04Q 7/38 (2006.01)
H04L 9/08 (2006.01)

(21)Application number : **2004-364591**
(22)Date of filing : **16.12.2004**

(71)Applicant : **MATSUSHITA ELECTRIC WORKS LTD**
INTERNET RESEARCH INSTITUTE INC
(72)Inventor : **KURAMAE KENJI**
TAKAZOE TOMOKI
MATSUDA KAZUHIRO
KUROKI HIDEKAZU
MIZUSHIMA TOMOAKI
OGINO TSUKASA

(54) AUTOMATIC TUNNEL SETTING APPARATUS, AUTOMATIC TUNNEL SETTING METHOD AND AUTOMATIC TUNNEL SETTING PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an automatic tunnel setting apparatus, automatic tunnel setting method and automatic tunnel setting program for automatically constructing a tunnel, while improving security, by performing inter-authentication via a third party institution.
SOLUTION: An automatic tunnel setting apparatus 11, according to the present invention, for automatically setting a 6o4 tunnel 5 to a network comprises a tunnel setting section for setting the 6o4 tunnel 5, after performing inter-authentication using a public key certificate, with an automatic tunnel setting apparatus 11 that is a connection destination in the 6o4 tunnel 5.

* NOTICES *

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1]
In tunnel automatic setting equipment which sets a tunnel to a network automatically,
It has a tunnel set part which sets up the aforementioned tunnel after performing mutual recognition using a public key certification between tunnel automatic setting equipment of a connection destination in the aforementioned tunnel.
Tunnel automatic setting equipment by which it is characterized.
[Claim 2]
It has further an input part which inputs IPsec setup information showing setting out of whether to apply IPsec into the aforementioned tunnel,
The aforementioned tunnel set part sets up the aforementioned tunnel according to the aforementioned IPsec setup information.
The tunnel automatic setting equipment according to claim 1 by which it is characterized.
[Claim 3]
It has further a tunnel cutout which deletes the aforementioned tunnel after performing mutual recognition using tunnel automatic setting equipment and a public key certification of the aforementioned connection destination.
The tunnel automatic setting equipment according to claim 1 by which it is characterized.
[Claim 4]
It has further a clock part which times the date and time,
It judges whether based on the date and time which were acquired from a lapse list and the aforementioned clock part of a public key certification before using the aforementioned public key certification, the aforementioned public key certification of the aforementioned tunnel set part is effective, and when not effective, update the aforementioned public key certification.
The tunnel automatic setting equipment according to claim 1 by which it is characterized.
[Claim 5]
It has further a clock part which times the date and time,
It judges whether based on the date and time which were acquired from a lapse list and the aforementioned clock part of a public key certification before using the aforementioned public key certification, the aforementioned public key certification of the aforementioned tunnel cutout is effective, and when not effective, update the aforementioned public key certification.
The tunnel automatic setting equipment according to claim 3 by which it is characterized.
[Claim 6]
The aforementioned clock part acquires a present date and time from an NTP server in a network, and a date and time which acquired [aforementioned], and a synchronization are taken.
The tunnel automatic setting equipment according to claim 4 or 5 by which it is characterized.
[Claim 7]
The aforementioned tunnel set part updates a public key certification at the time of starting.
The tunnel automatic setting equipment according to claim 1 by which it is characterized.
[Claim 8]
The aforementioned tunnel cutout should delete the aforementioned tunnel, when an obstacle occurs to the aforementioned tunnel.
The tunnel automatic setting equipment according to claim 3 by which it is characterized.
[Claim 9]

After the aforementioned tunnel cutout deletes the aforementioned tunnel, the aforementioned tunnel set part is made to reset the aforementioned tunnel.
The tunnel automatic setting equipment according to claim 8 by which it is characterized.
[Claim 10]
The aforementioned tunnel set part can set up two or more tunnels.
The tunnel automatic setting equipment according to claim 1 by which it is characterized.
[Claim 11]
Tunnel automatic setting equipment. In a tunnel automatic setting method with which tunnel automatic setting equipment which memorizes an automatic setting device identifier of self to identify, an automatic setting device identifier in tunnel automatic setting equipment of a connection destination of a tunnel, and a tunnel internal address of self sets the aforementioned tunnel to a network automatically,
A step which acquires an IP address assigned with connection with the aforementioned network as a tunnel external IP address of the aforementioned tunnel connection origin,
A step which transmits said assigned IP address and the aforementioned automatic setting device identifier of self to an information server which matches a tunnel external IP address with an automatic setting device identifier, and manages it,
A step which transmits an automatic setting device identifier in tunnel automatic setting equipment of a connection destination of the aforementioned tunnel to the aforementioned information server, and acquires a tunnel external IP address of a connection destination of the aforementioned tunnel,
To an authentication server which matches a public key certification of tunnel automatic setting equipment with an automatic setting device identifier, manages it, and publishes a public key certification of tunnel automatic setting equipment, A step which transmits an automatic setting device identifier in tunnel automatic setting equipment of a connection destination of the aforementioned tunnel, and acquires a public key certification in tunnel automatic setting equipment of a connection destination of the aforementioned tunnel,
A step which receives a challenge character string of the 1st kind which tunnel automatic setting equipment of a connection destination of the aforementioned tunnel generated from tunnel automatic setting equipment of a connection destination of the aforementioned tunnel,
A response character string of the 1st kind is generated by enciphering the result of an operation which calculated said CHIERENJI character string of the 1st kind with a predetermined arithmetic method with a public key of a self public key certification, and a secret key which constitutes a cryptographic key pair, A step which transmits a response character string of the 1st kind which generated [aforementioned] to tunnel automatic setting equipment of a connection destination of the aforementioned tunnel,
A step which generates a challenge character string of the 2nd kind and transmits a challenge character string of the 2nd kind which generated [aforementioned] to tunnel automatic setting equipment of a connection destination of the aforementioned tunnel,
Tunnel automatic setting equipment of a connection destination of the aforementioned tunnel a public key and a cryptographic key pair of a public key certification of tunnel automatic setting equipment. [in / for the result of an operation which calculated said challenge character string of the 2nd kind with a predetermined arithmetic method / tunnel automatic setting equipment of a connection destination of the aforementioned tunnel] A step which generates a response character string of the 2nd kind and receives a response character string of the 2nd kind which generated [aforementioned] from tunnel automatic setting equipment of a connection

destination of the aforementioned tunnel by enciphering with a secret key to constitute,
A decoding result which decoded a response character string of the 2nd kind received from tunnel automatic setting equipment of a connection destination of the aforementioned tunnel by a public key of a public key certification of tunnel automatic setting equipment in tunnel automatic setting equipment of a connection destination of the aforementioned tunnel, A step which judges whether the result of an operation which calculated said challenge character string of the 2nd kind with the aforementioned predetermined arithmetic method corresponds,
It has a step which exchanges setup information of a tunnel internal address required [when corresponding] in order to set the aforementioned tunnel to tunnel automatic setting equipment of a connection destination of the aforementioned tunnel, and others, and sets up the aforementioned tunnel using the aforementioned setup information.
A tunnel automatic setting method by which it is characterized.
[Claim 12]
In order to perform tunnel automatic setting equipment which memorizes an automatic setting device identifier of self which identifies tunnel automatic setting equipment, an automatic setting device identifier in tunnel automatic setting equipment of a connection destination of a tunnel, and a tunnel internal address of self, In a tunnel automatic setting program which sets the aforementioned tunnel to a network automatically,
A step which acquires an IP address assigned with connection with the aforementioned network as a tunnel external IP address of the aforementioned tunnel connection origin,
A step which transmits said assigned IP address and the aforementioned automatic setting device identifier of self to an information server which matches a tunnel external IP address with an automatic setting device identifier, and manages it,
A step which transmits an automatic setting device identifier in tunnel automatic setting equipment of a connection destination of the aforementioned tunnel to the aforementioned information server, and acquires a tunnel external IP address of a connection destination of the aforementioned tunnel,
To an authentication server which matches a public key certification of tunnel automatic setting equipment with an automatic setting device identifier, manages it, and publishes a public key certification of tunnel automatic setting equipment, A step which transmits an automatic setting device identifier in tunnel automatic setting equipment of a connection destination of the aforementioned tunnel, and acquires a public key certification in tunnel automatic setting equipment of a connection destination of the aforementioned tunnel,
A step which receives a challenge character string of the 1st kind which tunnel automatic setting equipment of a connection destination of the aforementioned tunnel generated from tunnel automatic setting equipment of a connection destination of the aforementioned tunnel,
A response character string of the 1st kind is generated by enciphering the result of an operation which calculated said CHIERENJI character string of the 1st kind with a predetermined arithmetic method with a public key of a self public key certification, and a secret key which constitutes a cryptographic key pair, A step which transmits a response character string of the 1st kind which generated [aforementioned] to tunnel automatic setting equipment of a connection destination of the aforementioned tunnel,
A step which generates a challenge character string of the 2nd kind and transmits a challenge character string of the 2nd kind which generated [aforementioned] to tunnel automatic setting equipment of a connection destination of the aforementioned tunnel,
Tunnel automatic setting equipment of a connection destination of the aforementioned tunnel a

public key and a cryptographic key pair of a public key certification of tunnel automatic setting equipment. [in / for the result of an operation which calculated said challenge character string of the 2nd kind with a predetermined arithmetic method / tunnel automatic setting equipment of a connection destination of the aforementioned tunnel] A step which generates a response character string of the 2nd kind and receives a response character string of the 2nd kind which generated [aforementioned] from tunnel automatic setting equipment of a connection destination of the aforementioned tunnel by enciphering with a secret key to constitute,
A decoding result which decoded a response character string of the 2nd kind received from tunnel automatic setting equipment of a connection destination of the aforementioned tunnel by a public key of a public key certification of tunnel automatic setting equipment in tunnel automatic setting equipment of a connection destination of the aforementioned tunnel, A step which judges whether the result of an operation which calculated said challenge character string of the 2nd kind with the aforementioned predetermined arithmetic method corresponds,
It has a step which exchanges setup information of a tunnel internal address required [when corresponding] in order to set the aforementioned tunnel to tunnel automatic setting equipment of a connection destination of the aforementioned tunnel, and others, and sets up the aforementioned tunnel using the aforementioned setup information.
A tunnel automatic setting program by which it is characterized.

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[Field of the Invention]
[0001]
The present invention relates to the tunnel automatic setting equipment and the tunnel automatic setting method which set up a virtual link (tunnel) automatically between nodes.
[Background of the Invention]
[0002]

The Internet which began from U.S. ARPANET (Advanced Research Projects Agency Network) in 1969, TCP/IP (Transmission Control Protocol/Internet Protocol) which is the essential technology of the Internet is developed and introduced from the 1970s to the 1980s, Use was explosively expanded taking advantage of the start of the commercial services of the 1990s, and development of WWW (World Wide Web) technology. Although IPv4 (Internet Protocol Version 4) is mainly used as a protocol of a network layer on the Internet now, Since the IP address (Internet Protocol Address) (it is hereafter written as the "IPv four address".) of IPv4 comprised 32 bits, drain of the IP address became one problem as a result of the expansion of use. In order to solve this problem, IPv6 (Internet Protocol Version 6) which expands an IP address to 128 bits is developed. Compared with IPv4, IPv6 it not only expanded the IP address to 128 bits, but, It has the characteristics, such as address solution by standard equipment of the hierarchical addressing architecture which can be collected, a multicast function, a mobility function, a security function, etc., and NDP (Neighbor Discovery Protocol, neighboring discovery protocol), and convenience is improving.

Although shift to the Internet of IPv6 which has such characteristics is desired, it is difficult to shift at IPv6 each node which uses IPv4 [diffused now], such as a vast quantity of host computers and server computers, and a router device, at a stretch. For this reason, in the transition period from IPv4 to IPv6, the network of IPv4 and the network of IPv6 will live together. In this coexistence environment, the technology which communicates via the network of other protocols in the networks of the same protocol is needed. There is a thing adapting tunneling as one of them.

[0003]

This tunneling encapsulates transmit information by the frame of another protocol, or Paquette by the node in the exit of the network which the equipment of a transmitting agency connects, and passes the network of another protocol, It is the technology which undoes a capsule by the node in the entrance of the network which the equipment of an address connects, and is returned to the original transmit information. There are 6to4, ISATAP, DTCP, etc. in the technology of such tunneling, for example (for example, the nonpatent literature 1 and two references).

[Nonpatent literature 1] "RFC2473 Generic Packet Tunnelingin IPv6 Specification", [online], JP-NIC, [Heisei 15(2003) January 22 search], Internet <http://rfc-jp.nic.ad.jp/rfc/rfc2473.txt>

[Nonpatent literature 2] ********, "a 6to4 open-relay router employment experiment", KDDI R&D Laboratories, [Heisei 16(2004) March 3 search], the Internet <URL;http://www.6to4.jp/>

[Description of the Invention]

[Problem to be solved by the invention]

[0004]

by the way, the person himself/herself who used the independent organization in communication using an open network -- it cannot be said that the technology of tunneling mentioned above has sufficient security although it is necessary to secure advanced security, such as authentication, data integrity, and the confidentiality (confidentiality, privacy) of data. That is, above-mentioned 6to4 and ISATAP are not equipped with the means itself which secures security. Since APOP (Authenticated Post Office Protocol) is used when building a tunnel, DTCP is only performing personal identification using a password, the strict person himself/herself using an independent organization -- it is not necessarily authenticating, and when especially a password is leaked, what is called spoofing may arise.

[0005]

Even if all the nodes shift to IPv6, or the end node is not provided in particular with the security

function by all nodes from a point of cost or performance, the case where it has a part of security function may arise. Even in such a case, secure communication may be desired.
[0006]
The present invention is invention in which it succeeded in view of the above-mentioned situation, and an object of the present invention is to provide the tunnel automatic setting equipment which builds a tunnel automatically performing mutual recognition through an independent organization and improving security. And it aims at providing the tunnel automatic setting method applied to such tunnel automatic setting equipment. It aims at providing the tunnel automatic setting program of such a tunnel automatic setting method.
[Means for solving problem]
[0007]
In order to attain the above-mentioned purpose, the tunnel automatic setting equipment concerning one mode of the present invention which sets a tunnel to a network automatically, After performing mutual recognition using a public key certification between the tunnel automatic setting equipment of the connection destination in the aforementioned tunnel, it has a tunnel set part which sets up the aforementioned tunnel.
[0008]
And in above-mentioned tunnel automatic setting equipment, it has further an input part which inputs the IPsec setup information showing setting out of whether to apply IPsec to the aforementioned tunnel, and the aforementioned tunnel set part sets up the aforementioned tunnel according to the aforementioned IPsec setup information.
[0009]
In above-mentioned tunnel automatic setting equipment, after performing mutual recognition using the tunnel automatic setting equipment and the public key certification of the aforementioned connection destination, it has further a tunnel cutout which deletes the aforementioned tunnel.
[0010]
In above-mentioned tunnel automatic setting equipment, have further a clock part which times the date and time, and the aforementioned tunnel set part, Before using the aforementioned public key certification, based on the date and time which were acquired from the lapse list and the aforementioned clock part of the public key certification, it judges whether the aforementioned public key certification is effective, and when not effective, the aforementioned public key certification is updated.
[0011]
And in above-mentioned tunnel automatic setting equipment, have further a clock part which times the date and time, and the aforementioned tunnel cutout, Before using the aforementioned public key certification, based on the date and time which were acquired from the lapse list and the aforementioned clock part of the public key certification, it judges whether the aforementioned public key certification is effective, and when not effective, the aforementioned public key certification is updated.
[0012]
In above-mentioned tunnel automatic setting equipment, the aforementioned clock part acquires a present date and time from the NTP server in a network, and takes this the date and time which were acquired, and synchronization.
[0013]
In above-mentioned tunnel automatic setting equipment, the aforementioned tunnel set part

updates a public key certification at the time of starting.
[0014]
And in above-mentioned tunnel automatic setting equipment, the aforementioned tunnel cutout deletes the aforementioned tunnel, when an obstacle occurs to the aforementioned tunnel.
[0015]
The aforementioned tunnel cutout makes the aforementioned tunnel set part reset the aforementioned tunnel in above-mentioned tunnel automatic setting equipment, after deleting the aforementioned tunnel.
[0016]
In above-mentioned tunnel automatic setting equipment, the aforementioned tunnel set part is characterized by the ability to set up two or more tunnels.
[0017]
One mode is started in order to attain the present invention and the above-mentioned purpose, Tunnel automatic setting equipment. Tunnel automatic setting equipment which memorizes an automatic setting device identifier of self to identify, an automatic setting device identifier in tunnel automatic setting equipment of a connection destination of a tunnel, and a tunnel internal address of self to a tunnel automatic setting method which sets the aforementioned tunnel to a network automatically the following. It is characterized by providing.
A step which acquires an IP address assigned with connection with the aforementioned network as a tunnel external IP address of the aforementioned tunnel connection origin.
A step which transmits assigned above-mentioned IP address and the aforementioned automatic setting device identifier of self to an information server which matches a tunnel external IP address with an automatic setting device identifier, and manages it.
A step which transmits an automatic setting device identifier in tunnel automatic setting equipment of a connection destination of the aforementioned tunnel to the aforementioned information server, and acquires a tunnel external IP address of a connection destination of the aforementioned tunnel.
To the authentication server which matches the public key certification of tunnel automatic setting equipment with an automatic setting device identifier, manages it, and publishes the public key certification of tunnel automatic setting equipment, A step which transmits an automatic setting device identifier in tunnel automatic setting equipment of a connection destination of the aforementioned tunnel, and acquires a public key certification in tunnel automatic setting equipment of a connection destination of the aforementioned tunnel, A step which receives a challenge character string of the 1st kind which tunnel automatic setting equipment of a connection destination of the aforementioned tunnel generated from tunnel automatic setting equipment of a connection destination of the aforementioned tunnel, A response character string of the 1st kind is generated by enciphering the result of an operation which calculated above-mentioned CHIERENJI character string of the 1st kind with a predetermined arithmetic method with a public key of a self public key certification, and a secret key which constitutes a cryptographic key pair, A step which transmits a response character string of the 1st kind which generated [aforementioned] to tunnel automatic setting equipment of a connection destination of the aforementioned tunnel, and a step which generates a challenge character string of the 2nd kind and transmits a challenge character string of the 2nd kind which generated [aforementioned] to tunnel automatic setting equipment of a connection destination of the aforementioned tunnel, The tunnel automatic setting equipment of the connection destination of the aforementioned tunnel the public key and cryptographic key pair of a public

key certification of tunnel automatic setting equipment. [in / for the result of an operation which calculated the above-mentioned challenge character string of the 2nd kind with the predetermined arithmetic method / the tunnel automatic setting equipment of the connection destination of the aforementioned tunnel] A step which generates a response character string of the 2nd kind and receives a response character string of the 2nd kind which generated [aforementioned] from tunnel automatic setting equipment of a connection destination of the aforementioned tunnel by enciphering with a secret key to constitute, A decoding result which decoded a response character string of the 2nd kind received from tunnel automatic setting equipment of a connection destination of the aforementioned tunnel by a public key of a public key certification of tunnel automatic setting equipment in tunnel automatic setting equipment of a connection destination of the aforementioned tunnel, A step which judges whether the result of an operation which calculated above-mentioned challenge character string of the 2nd kind with the aforementioned predetermined arithmetic method corresponds, A step which exchanges setup information of a tunnel internal address required [when corresponding] in order to set the aforementioned tunnel to tunnel automatic setting equipment of a connection destination of the aforementioned tunnel, and others, and sets up the aforementioned tunnel using the aforementioned setup information.

[0018]
The present invention relates to one mode again, in order to attain the above-mentioned purpose, In order to perform tunnel automatic setting equipment which memorizes an automatic setting device identifier of self which identifies tunnel automatic setting equipment, an automatic setting device identifier in tunnel automatic setting equipment of a connection destination of a tunnel, and a tunnel internal address of self, It is characterized by a tunnel automatic setting program which sets the aforementioned tunnel to a network automatically comprising the following.
A step which acquires an IP address assigned with connection with the aforementioned network as a tunnel external IP address of the aforementioned tunnel connection origin.
A step which transmits assigned above-mentioned IP address and the aforementioned automatic setting device identifier of self to an information server which matches a tunnel external IP address with an automatic setting device identifier, and manages it.
A step which transmits an automatic setting device identifier in tunnel automatic setting equipment of a connection destination of the aforementioned tunnel to the aforementioned information server, and acquires a tunnel external IP address of a connection destination of the aforementioned tunnel.
To the authentication server which matches the public key certification of tunnel automatic setting equipment with an automatic setting device identifier, manages it, and publishes the public key certification of tunnel automatic setting equipment, A step which transmits an automatic setting device identifier in tunnel automatic setting equipment of a connection destination of the aforementioned tunnel, and acquires a public key certification in tunnel automatic setting equipment of a connection destination of the aforementioned tunnel, A step which receives a challenge character string of the 1st kind which tunnel automatic setting equipment of a connection destination of the aforementioned tunnel generated from tunnel automatic setting equipment of a connection destination of the aforementioned tunnel, A response character string of the 1st kind is generated by enciphering the result of an operation which calculated above-mentioned CHIERENJI character string of the 1st kind with a predetermined arithmetic method with a public key of a self public key certification, and a secret

key which constitutes a cryptographic key pair, A step which transmits a response character string of the 1st kind which generated [aforementioned] to tunnel automatic setting equipment of a connection destination of the aforementioned tunnel, and a step which generates a challenge character string of the 2nd kind and transmits a challenge character string of the 2nd kind which generated [aforementioned] to tunnel automatic setting equipment of a connection destination of the aforementioned tunnel, The tunnel automatic setting equipment of the connection destination of the aforementioned tunnel the public key and cryptographic key pair of a public key certification of tunnel automatic setting equipment. [in / for the result of an operation which calculated the above-mentioned challenge character string of the 2nd kind with the predetermined arithmetic method / the tunnel automatic setting equipment of the connection destination of the aforementioned tunnel] A step which generates a response character string of the 2nd kind and receives a response character string of the 2nd kind which generated [aforementioned] from tunnel automatic setting equipment of a connection destination of the aforementioned tunnel by enciphering with a secret key to constitute, A decoding result which decoded a response character string of the 2nd kind received from tunnel automatic setting equipment of a connection destination of the aforementioned tunnel by a public key of a public key certification of tunnel automatic setting equipment in tunnel automatic setting equipment of a connection destination of the aforementioned tunnel, A step which judges whether the result of an operation which calculated above-mentioned challenge character string of the 2nd kind with the aforementioned predetermined arithmetic method corresponds, A step which exchanges setup information of a tunnel internal address required [when corresponding] in order to set the aforementioned tunnel to tunnel automatic setting equipment of a connection destination of the aforementioned tunnel, and others, and sets up the aforementioned tunnel using the aforementioned setup information.

[Effect of the Invention]
[0019]
The tunnel automatic setting equipment, tunnel automatic setting method, and tunnel automatic setting program concerning the present invention, Since mutual recognition is performed using the public key certification which the certificate authority of the public key infrastructure which is an independent organization publishes for the tunnel automatic setting equipment of the connection origin which sets up a tunnel, and a connection destination, a tunnel can be set up between the genuine tunnel automatic setting equipment meant in order to set up a tunnel.
[Best Mode of Carrying Out the Invention]
[0020]
Hereafter, the embodiment concerning the present invention is described based on Drawings. The composition which attached the same code in each figure shows that it is the same composition, and omits the description. When the reference agreement which omitted the subscript of the alphabet shows in naming generically, and individual composition is shown, the reference agreement which attached the subscript of the alphabet shows.
(Composition of an embodiment)
This embodiment is an embodiment of tunnel automatic setting equipment which can set up the tunnel on IPv4 network between [in two networks of IPv6] tunnel automatic setting equipment automatically. Thus, in order to enable communication between the nodes of IPv6, the tunnel set as the network of IPv4 is called IPv6overIPv4 tunnel (Tunnel) (it is hereafter written as "6o4 tunnel".).

[0021]
Fig.1 is a figure showing the entire configuration of the network in an embodiment. Fig.2 is a block diagram showing the composition of the network containing tunnel automatic setting equipment. Fig.3 is a figure showing the composition of the setting-out tunnel-pipes Osamu information table in tunnel automatic setting equipment. Fig.4 is a figure showing the composition of the offer tunnel setting information table in an information server. Fig.5 is a figure showing the composition of the login certification information registration table in a registration server. Fig.6 is a figure showing the composition of the automatic setting device book humanity news registration table in a registration server. Fig.7 is a figure showing the composition of the repository in an authentication server.
[0022]
In Fig.1, the network 1 is a communications network with which the network of two or more IPv6 and the network of two or more IPv4 live together.
[0023]
The network 2 of IPv6 containing the tunnel automatic setting equipment (it is hereafter written as "automatic setting equipment".) 11 which performs mutual recognition using an independent organization and sets up 6o4 tunnel automatically is in the network of IPv6 which constitutes the network 1. The networks 2 of IPv6 are the local area network (Local Area Network, LAN) where 1 or two or more apparatus were connected by the communication wire, LAN containing the remote-supervisory-control equipment which supervises and controls these apparatus to remoteness, etc., for example. In Fig.1, network 2-A of three IPv6, 2-B, and 2-C are shown, and network 2-A of each IPv6, 2-B, and 2-C contain each automatic setting equipment 11-A, 11-B, and 11-C, respectively.
[0024]
ISP networks 3 which the Internet Service Provider (it is hereafter written as "ISP".) which the automatic setting equipment 11 should connect builds, and the network 4 which ISP networks 3 connect are in the network of IPv4 which constitutes the network 1. In Fig.1, ISP-networks 3-A of three IPv4, 3-B, and 3-C are shown by ISP networks 3, and each ISP-networks 3-A, 3-B, and 3-C, The service connected to the Internet to each automatic setting equipment 11-A, 11-B, and 11-C is provided, respectively. To each ISP-networks 3-A, 3-B, and 3-C, DHCP (Dynamic Host Configuration Protocol) server 26-A, 26-B which assign an unassigned IP address automatically to the client which requires connection in order to receive service linked to the Internet, 26-C is contained, respectively and the computer (an ISP computer, un-illustrating) which provides service linked to the Internet and which can be communicated is contained, respectively. The network 4 is a network which comprises nodes which use IPv4, such as a router device, a gateway unit, a server computer, and a host computer.
[0025]
And the network 1 is provided with the following.
The information server 21 which provides information required for setting out of 6o4 tunnel when the automatic setting equipment 11 sets up 6o4 tunnel automatically.
being related with issue of a public key certification to a public key of the automatic setting equipment 11 -- the person himself/herself -- the registration server 22 which it authenticates, and registers and manages information about the person himself/herself (automatic setting equipment 11).
the registration server 22 -- the person himself/herself -- the authentication server 23 which publishes a public key certification to a public key of the automatic setting equipment 11

authenticated and it was accepted that was genuine.
The NTP (Network Time Protocol) server 24 which replies time according to a demand from a client (the automatic setting equipment 11 and the authentication server 23 are included).

[0026]
The registration server 22 and the authentication server 23 are what is called public key infrastructure (). [Public Key Infrastructur and] A role of the registration authority (Registration Authority) and certificate authority (Certification Authority) in PKI is played, respectively. Thus, by dividing the registration server 22 and the authentication server 23, the authentication server 23 can concentrate hardware resources and a software resource on issue of a public key certification, and can ease a burden. The same computer may realize the registration server 22 and the authentication server 23.
[0027]
The networks 1 are a telephone network, a digital communication network, a wireless communication network, etc., for example, and the signal transmission which accommodated information using the predetermined communications protocol is transmitted. In this embodiment, the network 1 to a communications protocol HTTP (Hyper Text Transfer Protocol), FTP (File Transfer Protocol), POP3 (Post Office Protocol ver.3), SMTP (Simple Mail Transfer Protocol), Telnet, TCP (Transmission Control Protocol), Internet protocol suites, such as UDP (User Datagram Protocol) and IP (Internet Protocol), are used, and the Internet is constituted. As for IP, the version 4 and the version 6 are used in two or more versions and this embodiment.
[0028]
The automatic setting equipment 11 contained in the network 2 of IPv6, It is included in the router device arranged in this embodiment on the boundary of the network 2 of IPv6, and other networks which constitute the network 1, for example, The communication packet transmitted from other networks which constitute the network 1, Carry out routing (channel selection) of the communication packet transmitted from the network 2 of IPv6 with which the automatic setting equipment 11 concerned belongs, the communication packet which the automatic setting equipment 11 self concerned transmits, etc., and. 6o4 tunnel is automatically set up between the automatic setting equipment 11 in the network of other IPv6. In the example shown in Fig.1, automatic setting equipment 11-A in network 2-A of IPv6, IPv6overIPv4 tunnel 5-AB and 5-AC are automatically set up, respectively between automatic setting equipment 11-C between automatic setting equipment 11-B in network 2-B of IPv6, and in network 2-C of IPv6.
[0029]
For example, the automatic setting equipment 11 is built into the router device of the network 2 of IPv6 installed in buildings, such as a single-family house, collective housing, a public facility, and an office building, in the example shown in Fig.2. 1 or two or more apparatus 12 (12-A --) which are automatic setting equipped with the network 2 of IPv6 11, and work considering the electrical and electric equipment as an energy source It has 12-B, ..., the communication wire 13 that connects the automatic setting equipment 11 and the apparatus 12, for example, Ethernet, (Ethernet, registered trademark), and intranet is constituted.
[0030]
The communications department 81 where the apparatus 12 communicates via the automatic setting equipment 11 and the communication wire 13, Have, and the function part 82 which performs the function of the apparatus 12 is constituted, and The state of the function part 82. Transmit (for example, ON/OFF of a power supply, a working state, a failed state, etc.) to the

remote-supervisory-control equipment in other networks, etc. using the communications department 81 via the communication wire 13 and the automatic setting equipment 11, and. The control instruction which controls the state of the function part 82 is received using the communications department 81 via the automatic setting equipment 11 and the communication wire 13 from the remote-supervisory-control equipment in other networks, etc., and it controls as control instruction. Control instruction is transmitted from terminal units which access remote-supervisory-control equipment etc., such as a cellular phone, PDA (Personal Digital Assistants), and a personal computer, for example. The function part 82 is a measurement function which measures the amount of the gas used, when the apparatus 12 is a gas meter which measures the amount of the gas used, for example. The electrical meter with which the apparatus 12 measures the amount of electric [used] other than a gas meter, for example, And equipment which adjusts dwelling unit environment, office environment, etc., such as measuring meter, such as a water meter which measures the amount of the waterworks used, a light, and an air-conditioner, Dwelling unit equipment of sensors, such as a smoke sensor, a temperature sensor, and a humidity sensor, an electronic lock device, etc., They are medical equipment, such as communication equipment, such as information processing equipments, such as home electronics, such as a television, a videotape recorder, a DVD recorder, and a washing machine, and a computer, telephone, and a facsimile machine, and pulsometer, a thermometer, a blood-oxygen-levels meter, and an electrocardiogram meter, etc.

[0031]

As shown in Fig.2, the automatic setting equipment 11 The local area network side interface part (it is hereafter written as the "LAN side interface part".) 51, It has the control part 52, the storage part 53, the input part 54, and the wide area network side interface part (it is hereafter written as the "WAN side interface part".) 55, and is constituted.

[0032]

The LAN side interface part 51 is an interface circuit which transmits and receives signal transmission via the communication wire 13 between the apparatus 12 in the network 2 of IPv6 to which the automatic setting equipment 11 concerned belongs, for example, are network cards, such as an Ethernet card. The IPsec (IP security) setup information showing setting out of whether the input part 54 applies IPsec to 6o4 tunnel, It is equipment which inputs into the automatic setting equipment 11 concerned varieties of information, such as an automatic setting device identifier in the automatic setting equipment 11 of the connection destination which sets up 6o4 tunnel, for example, they are a DIP switch, a jumper switch, a ten keypad, etc. When the input parts 54 are input devices, such as a ten keypad and a keyboard, in order to check an entry content, it is preferable to have display parts, such as a liquid crystal display, further. The WAN side interface part 55 is an interface circuit which transmits and receives signal transmission among other networks which constitute the network 1, for example, are modems, such as 56K modem, a terminal adopter, and ADSL Modem.

[0033]

The storage part 53 is provided with the setting-out tunnel-pipes Osamu information storage part 73 which memorizes the information storage part 71 for tunnel setting out which memorizes the information for tunnel setting out, the security information storage part 72 which memorizes security information, and setting-out tunnel-pipes Osamu information, A tunnel automatic setting program for setting up a tunnel automatically, a program for using the Internet, Varieties of information, such as various programs, such as a routing program which performs routing of a communication packet, and information concerning setting out of a tunnel, and information

produced during execution of various programs, are memorized. The storage part 53 The memory of volatility for example, such as RAM (Random Access Memory), And it has nonvolatile memories, such as ROM (Read Only Memory) and rewritable EEPROM (Electrically Erasable Programmable Read Only Memory), and is constituted.
[0034]
The information for tunnel setting out is information required in order to set up a tunnel automatically memorized previously, and in this embodiment, in order to identify the IP address and the automatic setting equipment 11 of the information server 21, it is the peculiar (it is unique) identifier (automatic setting device identifier) assigned previously. An automatic setting device identifier is a symbol string which consists of 1 or two or more signs, and is used also as the creation information (a prefix etc. are included.) of the IPv6 address of the automatic setting equipment 11 concerned by this embodiment, for example. For this reason, since the creation information of the IPv6 address of the automatic setting equipment 11 is memorized in a manufacturing stage, a shipping stage, etc., the manufacturing enterprise can manage the creation information of the IPv6 address of the automatic setting equipment 11.
[0035]
The inside IP address of a tunnel of the connection origin which sets up 6o4 tunnel in setting up 6o4 tunnel automatically (in the case of a network including two or more IP addresses, it is the attendant information about networks, such as an IP address and prefix length.) Hereafter, also in a network, it will be called the inside IP address of a tunnel. And a tunnel external IP address, the inside IP address of a tunnel of a connection destination, and a tunnel external IP address are required. The IP address of the IP header in the communication packet by which the inside IP address of a tunnel is encapsulated (capsuling), That is, the IP address of the IP header in the communication packet accommodated in the pay load in the communication packet after capsuling corresponds, and the IP address of an IP header [in / in a tunnel external IP address / the communication packet after capsuling] corresponds. In this embodiment, since IPv6overIPv4 tunnel is set up automatically, The IPv6 address (it corresponds to the inside IP address of a tunnel) of a connecting agency and the IPv four address (it corresponds to a tunnel external IP address), the IPv6 address (it corresponds to the inside IP address of a tunnel) of a connection destination, and the IPv four address (it corresponds to a tunnel external IP address) are required. The IPv6 address of a connecting agency is generated from the automatic setting device identifier of a connecting agency, and as for the IPv four address of a connecting agency, the automatic setting equipment of a connecting agency is assigned by the DHCP server in ISP networks 3 at the time connected to ISP networks 3 so that it may mention later. Similarly, the IPv6 address of a connection destination is generated from the automatic setting device identifier of a connection destination, and as for the IPv four address of a connection destination, the automatic setting equipment of a connection destination is assigned by the DHCP server in ISP networks 3 at the time connected to ISP networks 3 so that it may mention later. And the automatic setting equipment of a connecting agency acquires the IPv four address of a connection destination from the information server 21.
[0036]
the person himself/herself for whom security information used the independent organization -- it is information required in order to authenticate, and there are information memorized previously and information memorized by the below-mentioned operation. Previously the information memorized The IP address of the registration server 22, the IP address of the authentication server 23, it being the IPsec pertinent information which is needed when the group of ID for

logging in to the IP address of NTP server 24 and the registration server 22 and a password and IPsec are set up, and, The information memorized by the below-mentioned operation is a cryptographic key pair of the automatic setting equipment 11, a public key certification of the automatic setting equipment 11, a public key certification of the authentication server 23, and a public key certification of the automatic setting equipment 11 of a connection destination. IPsec pertinent information is a transmission origin port number, a destination port number, a transport layer protocol, action, a security protocol, encapsulation mode, an encryption algorithm, and an authentication algorithm in this embodiment, as mentioned later.

[0037]

Setting-out tunnel-pipes Osamu information is information about the 6o4 tunnel set up between the automatic setting equipment 11 of the connection destination which opposes, The inside IP address of a tunnel of a connecting agency and a tunnel external IP address, the inside IP address of a tunnel of a connection destination, and a tunnel external IP address are included at least.

[0038]

A tunnel name for setting-out tunnel-pipes Osamu information to identify 6o4 tunnel in this embodiment, The inside IP address of a tunnel in the automatic setting equipment 11 and tunnel external IP address of a connecting agency, It is with the automatic setting device identifier in the automatic setting equipment 11 of a connection destination, the inside IP address of a tunnel and a tunnel external IP address, IPsec setup information, and the tunnel established-state information that shows the established state of that 6o4 tunnel which 6o4 tunnel is ending with setting out, or is under deletion. The setting-out tunnel-pipes Osamu information table 101 which these setting-out tunnel-pipes Osamu information is memorized by table format, for example as shown in Fig.3, and registers setting-out tunnel-pipes Osamu information, The management number field 110 which registers the management number which identifies each record, The tunnel name field 111 which registers a tunnel name, and the connecting agency tunnel external IP address field 113 which registers the tunnel external IP address in the automatic setting equipment 11 of a connecting agency, The inside IP address field 114 of a connecting agency tunnel which registers the inside IP address of a tunnel in the automatic setting equipment 11 of a connecting agency, The connection destination automatic setting device identifier field 115 which registers the automatic setting device identifier in the automatic setting equipment 11 of a connection destination, The connection destination tunnel external IP address field 116 which registers the tunnel external IP address in the automatic setting equipment 11 of a connection destination, The inside IP address field 117 of a connecting agency tunnel which registers the inside IP address of a tunnel in the automatic setting equipment 11 of a connection destination, Have the IPsec setup information field 118 which registers IPsec setup information, and the tunnel established-state information field 119 which registers tunnel established-state information, and it is constituted, A record is created every tunnel name of every, i.e., 6o4 set up tunnel.

[0039]

Thus, two or more 6o4 tunnels can be simultaneously set to two or more of other automatic setting equipment 11, respectively by providing the automatic setting equipment 11 with the setting-out tunnel-pipes Osamu information table 101, and managing every 6o4 tunnel. And the control part 52 employs two or more 6o4 tunnels set up simultaneously by time sharing. By equipping the setting-out tunnel-pipes Osamu information table 101 with the tunnel established-state information field 119, It can be known by referring to the information on this tunnel established-state information field 119 via the network 1 from a terminal unit whether 6o4 tunnel

is ending with setting out, or it is under deletion.
[0040]
When neither a variety of information nor various programs are memorized by the storage part 53, These varieties of information and various programs these using recorded recording media, such as CD-ROM and DVD-ROM, install via a drive device not shown, or, It may install by downloading via the network 1 from the server which manages these varieties of information and various programs.
[0041]
The control part 52 is what performs routing of a communication packet, an automatic setup of 6o4 tunnel, etc., and controls the automatic setting equipment 11 whole by executing various programs, Functionally, Routing of a communication packet. The routing parts 61 and 1 or two or more 6o4 tunnels to perform. the tunnel set part 62 to set up, the inside IP address generation part 63 of a connection destination tunnel which generates the inside IP address of a tunnel in the automatic setting equipment 11 of a connection destination, the public key certification Management Department 64 which manages a public key certification, and the tunnel cutout 65 which deletes the 6o4 set-up tunnel -- and, It has the clock part 66 which times the date and time. The control part 52 is provided with a microprocessor etc., for example, and is constituted.
[0042]
The information server 21 is a server computer which provides information required for setting out of a tunnel when the automatic setting equipment 11 sets up 6o4 tunnel automatically and which can be communicated, It has an offer tunnel setting information storage part which matches with an automatic setting device identifier information (offer tunnel setup information) required for setting out of the 6o4 tunnel with which the storage part is provided, and memorizes it.
[0043]
Offer tunnel setup information is a tunnel external address at least. For example, the offer tunnel setting information table 102 which is memorized by table format and registers offer tunnel setup information as shown in Fig.4, The management number field 121 which registers the management number which identifies each record, It has the automatic setting device identifier field 123 which registers an automatic setting device identifier, and the tunnel external IP address field 124 which registers a tunnel external IP address, and is constituted, and a record is created for every automatic setting device identifier.
[0044]
the registration server 22 is related with issue of the public key certification to the public key of the automatic setting equipment 11 -- the person himself/herself -- it authenticating, and being a server computer which registers and manages the information about the person himself/herself (automatic setting equipment 11) and which can be communicated, and, The storage part is equipped with the login certification information registration table storage part which memorizes a login certification information registration table previously, and the automatic setting device book humanity news registration table storage part which memorizes an automatic setting device book humanity news registration table.
[0045]
A login certification information registration table registers previously ID and the password of the automatic setting equipment 11 which are set as the automatic setting equipment 11 which permits login to the registration server 22 concerned. As shown in Fig.5, the login certification information registration table 103, for example. the management number field 131 which

registers the management number for managing each record, and ID field 132 which registers ID (Identification) which specifies the automatic setting equipment 11 -- and, It has each field of the password field 133 which registers the password which is combined with ID and used for discernment of whether to be a regular user, and is constituted, and a record is created for every ID.

[0046]

automatic setting equipment -- in order that, as for a person-himself/herself information registration table, the authentication server 23 may publish a public key certification -- the registration server 22 -- the person himself/herself -- it being a table which registers the information (automatic setting equipment the person himself/herself information) about the authenticated automatic setting equipment 11, and, In this embodiment, it is the information (automatic setting equipment the person himself/herself information) about the public key (public key of the automatic setting equipment 11) and the automatic setting equipment 11 for verifying the digital signature of the automatic setting equipment 11. Automatic setting equipment book humanity news is an automatic setting device identifier of the automatic setting equipment 11, an address of a setting position, a handling person's in charge name, and a person's in charge contact in this embodiment, for example. For this reason, as shown in Fig.6, in this embodiment, for example the automatic setting device book humanity news registration table 104, the management **** field 141 which registers the management number for managing each record, and the public key field 142 which registers the public key of the automatic setting equipment 11 -- and, It has each field of the automatic setting equipment this humanity news field 143 which registers automatic setting equipment book humanity news, and is constituted, and a record is created for every public key of the automatic setting equipment 11. And the automatic setting equipment book humanity news field 143, The automatic setting device identifier of the automatic setting equipment 11. the automatic setting device identifier field 1431 to register, the setting position address field 1432 which registers the address of the setting position of the automatic setting equipment 11, and the person-in-charge name field 1433 which registers the name (the company name of a management company is included) of the person in charge who treats the automatic setting equipment 11 -- and, It has each subfield of the contact field 1434 which registers the contact of the person in charge concerned, and is constituted. Here, a contact is an address using the networks 1, such as a telephone number, a facsimile number, and an e-mail address, of a means of communication.

[0047]

the authentication server 23 -- the registration server 22 -- the person himself/herself -- it being a server computer which publishes a public key certification to the public key of the automatic setting equipment 11 authenticated and it was accepted that was genuine and which can be communicated, and, the information concerning the public key certification of the authentication server 23 to the storage part -- that is, The authentication server public key certification storage part which memorizes the public key certification and the term of validity of the authentication server 23, It has a repository storage part which memorizes a repository, a certificate cancellation list storage section which memorizes a certificate cancellation list, and a cryptographic key pair storage part for a self signature which memorizes the cryptographic key pair for the below-mentioned self signature. And the authentication server 23 is provided with the clock part which acquires the present time from NTP server 24, and sets an internal clock at this time.

[0048]

A repository is a table which matches the public key certification of the automatic setting

equipment 11 with the automatic setting device identifier of the automatic setting equipment 11 concerned, and registers it. Although the form of a public key certification has variously PKCS#6 (Extended-Certificate Syntax Standard), X.509 of ITU (International Telecommunication Union, International Telecommunications Union), etc., For example, in following the standard of X.509, as shown in Fig.7, for example the repository 105, the management number field 151 which registers the management number for managing each record, and the automatic setting device identifier field 152 which registers an automatic setting device identifier (it corresponds to the owner of a public key) -- and, It has the public key certification field 153 which registers the public key certification of the automatic setting equipment 11, and a record is created every automatic setting equipment 11. To the public key certification according to X.509 here, The serial number of a public key certification, the algorithm of a digital certificate, the algorithm in a public key, The start period of the shelf-life denoted by a date time second, the end time of the shelf-life denoted by a date time second, a public key, the version of the standard of a public key certification, the publisher of a certificate, the owner of a certificate, and the signature depended authentication server 23 are included.

[0049]

A certificate cancellation list (a lapse list, Certificate Revocation List, CRL), It is a list of the public key certification canceled (lapse), and, more specifically, the certificate authority which published the canceled public key certification concerned attaches a digital signature to the list of the serial numbers of the canceled public key certification.

[0050]

Although the public key certification which performed the digital signature to the public key of the automatic setting equipment 11 is published, the authentication server 23, In order to perform the digital signature, the secret key of the authentication server 23 is required, and it is necessary to distribute the secret key of the authentication server 23 concerned, and the public key of the authentication server 23 which constitutes a cryptographic key pair to the automatic setting equipment 11. This is because a certain automatic setting equipment 11 verifies the public key certification of other automatic setting equipment 11, so it is needed. Although it is necessary to judge whether the automatic setting equipment 11 has a genuine public key of the distributed authentication server 23 in the case of distribution of the public key of this authentication server 23, By this embodiment, authentication server 23 self has adopted as this genuine check of things the self signature (self-signature) which performs a digital signature to the public key of the authentication server 23. The public key certification in which this authentication server 23 self performed the digital signature to the public key of the authentication server 23 is a public key certification of the authentication server 23. Here, it supposes that the cryptographic key pair for performing a self signature is called the cryptographic key pair for a self signature, and suppose that the secret key and public key are called the secret key for a self signature, and the public key for a self signature, respectively. This public key for a self signature turns into a public key for verifying the public key certification of the authentication server 23. Although the self signature is adopted in this embodiment, It may constitute so that the public key of the authentication server 23 may be authenticated by the certificate authority of other public key infrastructure, for example, the certificate authority of government public key infrastructure (Government Public Key Infrastructure, GPKI).

[0051]

NTP server 24 is a server computer which replies time according to the demand from a client and which can be communicated. Generally NTP has a layered structure from which an NTP server,

and other host computers and NTP servers serve as the top, When the NTP server which is the top acquires the standard time from exact clocks, such as an atomic clock and GPS, and a low-ranking host computer (a low-ranking NTP server is included) doubles the time in a self clock at the time with reference to it, A synchronization is taken between the nodes in a network. The automatic setting equipment 11 and the authentication server 23 can take a synchronization by acquiring the date and time from NTP server 24, and setting the clock with which a self inside is equipped at this date and time that were acquired, for example, a software clock.

[0052]

Next, it describes about operation of this embodiment.

(Operation of an embodiment)

First, it describes about public key certification acquisition processing for the automatic setting equipment 11 to get the authentication server 23 to publish a public key certification. This public key certification acquisition processing is processing performed a priori, before the automatic setting equipment 11 sets up 6o4 tunnel automatically. A public key certification is data which the authentication server 23 publishes, and is data proving the public key of the automatic setting equipment 11 for digital signature verification being genuine.

[0053]

Fig.8 is a sequence diagram showing operation of public key certification acquisition processing. Fig.9 is a flow chart which shows the operation in the issue processing of the public key certification of automatic setting equipment. Fig.10 is a flow chart which shows the operation in the memory processing of the public key certification of automatic setting equipment.

[0054]

In Fig.8, the public key certification Management Department 64 in the control part 52 of the automatic setting equipment 11 generates the cryptographic key pair of the public key (public key of the automatic setting equipment 11) and secret key (secret key of the automatic setting equipment 11) in public key encryption (S11).

[0055]

The data enciphered with the secret key can decode public key encryption (unsymmetrical key code) only by a corresponding public key (a secret key and the public key which constitutes a cryptographic key pair), The data enciphered by the public key is a cipher system which can be decoded only with a corresponding secret key (a public key and the secret key which constitutes a cryptographic key pair). Usually, a public key is a key widely exhibited among cryptographic key pairs, and a secret key is a key which is managed severely and kept secret so that only the person himself/herself may understand among cryptographic key pairs. Since the public key encryption does not need to transport a key in a safe course, compared with the common key encryptosystem (a symmetrical code, a secret key cryptosystem) which performs encryption and a decoding with the same key, management of a key is easy for it, and its safety is high.

[0056]

Although public key encryption has the various systems by various algorithms, there are a RSA (Rivest-Shamir-Adleman) system, an ElGamal system, a Rabin system, an elliptic curve cryptosystem, etc., for example. In public key encryption, in order to secure the confidentiality of data, by the case where data is enciphered, a sending person will encipher data by a public key, and an addressee will decrypt with a secret key, but. A signer enciphers data with a secret key (equivalent to creation of a signature), and, in the case of the digital signature for performing person-himself/herself authentication, it becomes what (equivalent to verification of a signature) a verification person decrypts by a public key. and the equipment side which received the public

key with a public key certification by authenticating by the certificate authority which can trust a signer's public key (issue of a public key certification) -- the public key concerned -- a genuine signer -- it is reliable in it being a public key of the person himself/herself.
[0057]
Next, the public key certification Management Department 64 of the automatic setting equipment 11, the registration server 22 -- the person himself/herself -- the public key of the automatic setting equipment 11 created by the processing S11 in order to make it authenticate and to make the authentication server 23 publish a public key certification, and the automatic setting equipment of the automatic setting equipment 11 concerned -- the person himself/herself -- the signal transmission (public key certification issue requesting signal) which accommodates information is created (S12).
[0058]
And the public key certification Management Department 64 of the automatic setting equipment 11, Connect with ISP networks 3 and an Internet access service is received, The registration server 22 is accessed using the IP address of the registration server 22 of the security information storage part 72, ID and the password which are set up previously and memorized are transmitted to the registration server 22, and it logs in to the registration server 22 (S13). The registration server 22 refers to the login certification information registration table 103, In judging whether the group of ID and the password which were transmitted from the automatic setting equipment 11 is registered into the login certification information registration table 103, being registered and being, it admits being the proper automatic setting equipment 11, and login of the automatic setting equipment 11 is permitted. Login is refused and cut when not registered.
[0059]
Next, if the automatic setting equipment 11 succeeds in login, it will transmit a public key certification issue requesting signal to the registration server 22 so that it may obtain the public key certification to the public key of the automatic setting equipment 11 (S14). If a public key certification issue requesting signal is received, the registration server 22 will give a new management number to the automatic setting device book humanity news registration table 104, and will add a new record, the public key of the automatic setting equipment 11 accommodated in the public key certification issue requesting signal, and automatic setting equipment -- the public key field 142 in the record to which person-himself/herself information was newly added, and automatic setting equipment -- it resembles the person-himself/herself information field 143, respectively, and registers with it (S15).
[0060]
According to this embodiment, it has judged as mentioned above that the automatic setting equipment 11 which requires issue of a digital signature is the genuine automatic setting equipment 11 (what is called personal identification) by the ability of the automatic setting equipment 11 concerned to log in to the registration server 22. Although the reliability of personal identification becomes important depending on the reliability of the authentication server 23, especially the reliability of a public key certification, The reliability of this personal identification is secured with constituting from this embodiment so that the manufacturing enterprise and selling enterprise of the automatic setting equipment 11 may include in the automatic setting equipment 11 previously before selling ID of the automatic setting equipment 11, and the group of a password, or they may supply a purchaser widely by mailing or telephone. When based on mailing or a telephone, ID and a password are memorized by the automatic setting equipment 11 from the input part 54.

[0061]
One-time password (One-Time Password) technology may be used for processing of the processing S13 from a viewpoint [prevent leakage of a password and] of improving the reliability of personal identification further. First, a server (this embodiment registration server 22) generates the random character string (challenge character string) which serves as a "kind" of an authentication character string at a client (this embodiment automatic setting equipment 11), and this one-time password technology transmits this challenge character string, A client calculates according to a predetermined procedure using a challenge character string and a password, They are whether it is a regular client and the technology to distinguish by verifying the response character string which replied the result of an operation (an authentication character string, a response character string) to the server, and was replied from the client using the password remembered to be the challenge character string which the server generated. From a viewpoint of furthermore improving the reliability of personal identification, match the IP address of the automatic setting equipment 11 with ID, and it is further registered into the login certification information registration table 103, When a public key certification issue requesting signal is received, the IP address corresponding to ID which permitted login by the processing S13 is searched from the login certification information registration table 103, Personal identification may be performed by receiving the reply of the purport that transmitted the signal transmission (personal identification signal) which asks whether the public key certification issue requesting signal which made the address the searched IP address was transmitted, and the public key certification issue requesting signal was transmitted.
[0062]
Next, the information on the purport that it is required for the authentication server 23 that the registration server 22 should publish a public key certification to the automatic setting equipment 11 which transmitted the public key certification issue requesting signal, The signal transmission (issue requesting signal) which accommodated the automatic setting device identifier of the automatic setting equipment 11 concerned and the public key of the automatic setting equipment 11 concerned is created, and it transmits to the authentication server 23 (S16). When a public key certification issue requesting signal is received, constitute the registration server 22 from this embodiment so that an issue requesting signal may be unconditionally transmitted to the authentication server 22, but. Since transmission of an issue requesting signal is specified, accommodate the information on the purport that issue of a public key certification is further required of a public key certification issue requesting signal at the authentication server 23, and the registration server 22, When this information is accommodated in the public key certification issue requesting signal, it may constitute so that an issue requesting signal may be transmitted to the authentication server 22.
[0063]
the person himself/herself [as opposed to / when the authentication server 23 receives an issue requesting signal from the registration server 22 / the automatic setting equipment 11 of the registration server 22] -- authentication is trusted and issue processing of a public key certification is promptly performed to the public key of the automatic setting equipment 11 (S17).
[0064]
If it describes in details more about the issue processing of this public key certification, in Fig.9, the authentication server 23 will judge [whether the public key certification of the authentication server 23 exists, and] first whether it is effective by referring to an authentication server public

key certification storage part (S21). A judgment whether to be effective or not is made by judging whether it appears in whether the public key certification of the authentication server 23 concerned is within the term of validity, and a certificate cancellation list, when the public key certification of the authentication server 23 exists. It is within the term of validity and it is judged that it is effective when not appearing in a certificate cancellation list, and when it is outside the term of validity or appears in the certificate cancellation list, it is judged that it is not effective.
[0065]
The public key certification of the authentication server 23 does not exist as a result of judgment, Or when not effective, to (No) the authentication server 23, A cryptographic key pair (the public key and secret key of the authentication server 23) required in order to draw up the public key certification of the automatic setting equipment 11 is generated (S22), The public key certification of the authentication server 23 is drawn up by performing a digital signature to the public key of the authentication server 23 newly generated by the processing S22 using the secret key for a self signature (S23), The public key certification of the created authentication server 23 is memorized to an authentication server public key certification storage part (S24), and the public key certification of the newly created authentication server 23 is distributed to all the automatic setting equipment 11 (S25). This distribution is distributed by changing into a state with the automatic setting equipment 11 able to acquire the public key certification of the authentication server 23 to the authentication server 23, for example. The state in which this acquisition is possible is realized by installing the public key certification of the authentication server 23 in the part which can be accessed, for example without being accompanied by authentication via a Web server, an LDAP server, etc. In this embodiment, since it was a self signature, the authentication server 23 drew up the public key certification of the authentication server 23 in the processing S23, but. When other certificate authorities perform a digital signature, in the processing S23, issue of the public key certification to the public key generated by the processing S22 to other certificate authorities will be required. In the operation shown in Fig.9, although the cryptographic key pair for a self signature considered it as the effective thing, it may add further the processing which checks the validity of this cryptographic key pair for a self signature.
[0066]
On the other hand, as a result of a check, the public key certification of the authentication server 23 exists, and When effective (Yes), And when the public key certification of the authentication server 23 is newly drawn up by performing the processing S22 thru/or processing S25, the authentication server 23 draws up the public key certification of the automatic setting equipment 11 using the cryptographic key pair of the authentication server 23. That is, the authentication server 23 performs a digital signature to the public key of automatic setting equipment using the secret key of the authentication server 23. In other words, the authentication server 23 adds the signature of the authentication server 23 to the public key of the automatic setting equipment 11 with the secret key of the authentication server 23 (S26). Next, the authentication server 23 matches the public key certification of the created automatic setting equipment 11 with an automatic setting device identifier, and registers it into the repository 105 (S27). Namely, the serial number in the public key certification of the automatic setting equipment 11, the algorithm of a digital certificate, The algorithm in a public key, the start period of the shelf-life denoted by a date time second, The end time of the shelf-life denoted by a date time second, a public key, the version of the standard of a public key certification, the publisher of a certificate, the owner of a certificate, and the public key certification in which the signature depended authentication

server 23 was included are matched with an automatic setting device identifier (cryptographic key pair owner), and it registers with the repository 105.
[0067]
Thus, when the automatic setting equipment 11, the registration server 22, and the authentication server 23 operate, the public key certification by the authentication server 23 is published to the public key of the cryptographic key pair which the automatic setting equipment 11 generated.
[0068]
And when it returns to Fig.8 and the automatic setting equipment 11 desires handing out of the public key certification. the automatic setting equipment 11 -- the automatic setting device identifier of the automatic setting equipment 11 concerned -- and, If the signal transmission (request-for-share-distribution signal) which accommodated the information on the purport that handing out of the public key certification of the automatic setting equipment 11 is required is transmitted to the authentication server 23 (S18) and the authentication server 23 receives this request-for-share-distribution signal, The authentication server 23 searches the repository 105 based on the automatic setting device identifier accommodated in the request-for-share-distribution signal, and transmits the signal transmission (handing out signal) which accommodated the public key certification of the automatic setting equipment 11 to the automatic setting equipment 11 based on search results (S19). The public key certification Management Department 64 of the automatic setting equipment 11 will perform memory processing of the public key certification of the automatic setting equipment 11, if this signal transmission that accommodates the public key certification of the automatic setting equipment 11 from the authentication server 23 is received (S20).
[0069]
If it describes in details more about the memory processing of the public key certification of this automatic setting equipment, in Fig.10, the public key certification Management Department 64 of the automatic setting equipment 11 will verify the public key certification of the automatic setting equipment 11 by the public key of the authentication server 23 (S31). The public key certification Management Department 64 of the automatic setting equipment 11 compares the public key of the automatic setting equipment 11 obtained by verification of this processing S31 with the public key of the automatic setting equipment generated by the processing S11 of Fig.8, and judges whether it corresponds or not (S32). As a result of judgment, the public key certification Management Department 64 of the automatic setting equipment 11, In not corresponding (disagreement), it redoes the public key certification acquisition processing from the processing S11 of Fig.8 (S34), and in corresponding (correspondence), it judges whether the public key certification of this automatic setting equipment 11 is effective (S33). As a result of judgment, the public key certification Management Department 64 of the automatic setting equipment 11 performs processing S34 to (No), when not effective, and on the other hand, when effective (Yes), it memorizes the public key certification of the own automatic setting equipment 11 (S35).
[0070]
By performing such operation, the automatic setting equipment 11 can acquire the public key certification of the automatic setting equipment 11 from the authentication server 23. Here, since generation of a cryptographic key pair will be performed each time by constituting so that such public key certification acquisition processing may be performed at the time of starting of the automatic setting equipment 11, security can be improved. By waiting for reception of a request-for-share-distribution signal from the automatic setting equipment 11, although the public key

certification of the automatic setting equipment 11 is delivered, the authentication server 23 may consist of these embodiments so that it may deliver promptly, when the public key certification of the automatic setting equipment 11 is published.
[0071]
In the issue processing of the public key certification to the public key of the automatic setting equipment 11 performed by receiving an issue requesting signal from the registration server 22, although existence of a public key certification and validity of the authentication server 23 are checked, here the authentication server 23, Also periodically the check of the validity in the public key certification of the authentication server 23 is performed, and in not being effective, it is updating the public key certification of the authentication server 23. It describes about the update process to the public key certification of the authentication server which updates the public key certification of such an authentication server 23 performed periodically.
[0072]
Fig.11 is a sequence diagram showing the operation in the update process to the public key certification of an authentication server. Fig.12 is a flow chart which shows the operation in the update process to the public key certification of an authentication server.
[0073]
In Fig.11, if the time to perform the update process to the public key certification of the authentication server 23 comes, the authentication server 23 will transmit the signal transmission (time request signal) which accommodates the information on the purport that the date and time are required to NTP server 24 in order to take a synchronization (S41). NTP server 24 will reply the signal transmission (time reply signal) which accommodated the present date and time to the authentication server 23, if a time request signal is received (S42).
[0074]
If a time reply signal is received, the authentication server 23 will set an internal clock at the date and time which are accommodated in this signal, will take a synchronization, and will perform the update process to the public key certification of the authentication server 23 (S43).
[0075]
If it describes still in detail about the update process to the public key certification of this authentication server 23, in Fig.12, the authentication server 23 will judge first whether the public key certification of the authentication server 23 is effective by referring to an authentication server public key certification storage part (S51). The check of this validity is performed by judging whether it appears in whether the public key certification of the authentication server 23 concerned is within the term of validity, and certificate cancellation Liszt.
[0076]
When not effective, as a result of judgment to (No), The authentication server 23 performs generation processing of a cryptographic key pair (S52), and performs creation processing of the public key certification of the authentication server 23 (S53), Memory processing of the public key certification of the authentication server 23 is performed (S54), distribution processing of the public key of the newly created authentication server 23 is performed (S55), and processing is ended. Since these processings S52 thru/or the processing S55 are the same as the processing S22 thru/or the processing S25 described using Fig.9, the description is omitted. On the other hand, as a result of judgment, in being effective (Yes), the authentication server 23 ends processing.
[0077]

By operating in this way, the authentication server 23 can judge appropriately the validity of the public key certification of the authentication server 23 by taking the time of NTP server 24, and a synchronization and taking each node in the network 1, and a synchronization. When the authentication server 23 does not have an effective public key certification of the authentication server 23, the public key certification of the new authentication server 23 is acquired, and updating to the public key certification of the authentication server 23 is performed.

[0078]

Next, the tunnel using the authentication server 23 is described about the tunnel automatic setting processing set up automatically. The initial processing which registers information required in order to exchange the information about tunnel automatic setting processing with other automatic setting equipment 11 and to set up a tunnel automatically into the information server 21, It comprises tunnel construction processing which sets up a tunnel automatically, and tunnel deletion which deletes a tunnel automatically.

[0079]

Fig.13 is a sequence diagram showing operation of the initial processing in tunnel automatic setting processing. Fig.14 thru/or Fig.18 are the sequence diagrams (the 1 thru/or its 5) showing operation of the tunnel construction processing in tunnel automatic setting processing.Fig.19 is a flow chart which shows operation of the tunnel construction processing in tunnel automatic setting processing. Fig.20 is a sequence diagram showing the operation in the update process to the public key certification of automatic setting equipment. Fig.21 is a flow chart which shows operation of the usability judging process in the public key certification of automatic setting equipment.

[0080]

First, it describes about the initial processing of tunnel automatic setting processing. If the power supply of the automatic setting equipment 11 is switched on and the automatic setting device identifier in IPsec setup information and the automatic setting equipment 11 of the connection destination of 6o4 tunnel is input from the input part 54 in Fig.13, The tunnel set part 62 in the control part 52 of the automatic setting equipment 11 transmits a connection request to ISP networks 3 (S61). In ISP networks 3, an ISP computer, If a connection request is received, the IPv four address will be assigned to the automatic setting equipment 11 using DHCP server 26, Information required since these assigned Internet access services, such as the IPv four address and default channel information, are provided is transmitted to the automatic setting equipment 11, and an Internet access service is started (S62).

[0081]

Next, the tunnel set part 62 of the automatic setting equipment 11, Use the Internet access service of ISP networks 3, and the information server 21 is accessed using the IP address of the information server 21 in the information storage part 71 for tunnel setting out, An automatic setting device identifier, a tunnel external IP address, and the signal transmission (tunnel external IP address setup information signal) that accommodates the information on the purport that registration is required of the offer tunnel setting information table 102 for these information are created, and it transmits to the information server 21 (S63). A tunnel external IP address is the IPv four address assigned by DHCP server 26 by the processing S62. If a tunnel setup information signal is received, the information server 21 will create a new record and will register into the offer tunnel setting information table 102 the automatic setting device identifier and tunnel external IP address which are accommodated in the tunnel external IP address setup information signal (S64).

[0082]
By operating in this way, a tunnel external IP address required for setting out of 6o4 tunnel is assigned, the assigned tunnel external IP address is registered into the information server 21, and batch management is carried out intensively. It can respond, also when a tunnel external IP address is changed especially, whenever it sets up 6o4 tunnel like [in the case of a dialup connection etc.].
[0083]
Next, the tunnel set part 62 of the automatic setting equipment 11, According to a predetermined procedure, an IPv6 address (inside IP address of a tunnel) is created from an automatic setting device identifier using the inside IP address generation part 63 of a tunnel in order to assign the IPv6 address of the LAN side interface part 51 in the automatic setting equipment 11 concerned (S65).
[0084]
If the predetermined procedure which generates an IPv6 address is a global address not overlapping, although what kind of procedure may be sufficient, in this embodiment, Since the automatic setting device identifier is IPv6 address creation information, creation of an IPv6 address, for example, the thing which the network prefix of the IPv6 address creation information included in the network prefix of the IPv6 address to generate at an automatic setting device identifier is used as it is, and is further done for interface ID addition -- an IPv6 address is generated. If interface ID does not overlap with interface ID of other apparatus connected with the network 2, it may use what kind of interface ID, but in this embodiment, All interface ID contained in the IPv6 address assigned to the LAN side interface part 51 is set to 0.
[0085]
Next, the tunnel set part 62 of the automatic setting equipment 11 sets up the IPv6 address generated by the inside IP address generation part 63 of a tunnel as an IP address (inside IP address of a tunnel) of the LAN side interface part 51 (S66).
[0086]
Next, the tunnel set part 62 of the automatic setting equipment 11, A router device (this embodiment automatic setting equipment 11) starts RA demon who performs the router advertisement (Router Advertisement) which notifies a network prefix to a subordinate's host computer (S67). Next, the tunnel set part 62 of the automatic setting equipment 11 starts the IKE demon who performs IKE (Internet Key Exchange) (S68). IKE is a protocol which is used for setting out of IPsec and performs generation and management of SA (SecurityAssociation). And the tunnel set part 62 of the automatic setting equipment 11 performs tunnel construction processing (S69).
[0087]
Next, it describes about tunnel construction processing of tunnel automatic setting processing. In Fig.14 thru/or Fig.18, the tunnel set part 62 in the control part 52 of the automatic setting equipment 11 of a connecting agency performs the update process which updates the public key certification of the automatic setting equipment 11 (S101).Thus, since the automatic setting equipment 11 performs an update process, it can improve security and can continue an automatic setup of 6o4 tunnel with an effective public key certification.
[0088]
It describes in details more about the update process to the public key certification of this automatic setting equipment 11. In Fig.20, using the clock part 66 in the control part 52, the tunnel set part 62 of the automatic setting equipment 11 transmits the time request signal which

accommodated the information on the purport that the date and time are required to NTP server 24 so that it may take a synchronization (S201). NTP server 24 will reply the time reply signal which accommodated the present date and time to the automatic setting equipment 11, if a time request signal is received (S202). The clock part 66 of the automatic setting equipment 11 will set Uchibe's clock at the date and time which are accommodated in this signal, if a time reply signal is received (S203).

[0089]

By operating in this way, the automatic setting equipment 11, Since the clock of the clock part 66 is set at the date and time of NTP server 24, For example, even when the power supply of the automatic setting equipment 11 without a backup power supply is turned off, the accuracy of a clock is bad or the clock of the automatic setting equipment 11 is wrong for writing, the automatic setting equipment 11 can take the synchronization of the authentication server 23 and current time. For this reason, the validity of the public key certification of the authentication server 23 and the validity of the public key certification of the automatic setting equipment 11 can be judged appropriately.

[0090]

Next, the tunnel set part 62 of the automatic setting equipment 11 creates the signal transmission (authentication server public key certification request-for-share-distribution signal) which accommodated the information on the purport that handing out of the public key certification of the authentication server 23 is required, and transmits to the authentication server 23 (S204). If an authentication server public key certification request-for-share-distribution signal is received, the authentication server 23 will create the signal transmission (authentication server public key certification handing out signal) which accommodated the public key certification of the authentication server 23 memorized by the authentication server public key certification storage part, and will reply it to the automatic setting equipment 11 (S205).

[0091]

It is judged whether the tunnel set part 62 of the automatic setting equipment 11 has the effective public key certification of the authentication server 23 accommodated in this signal, when an authentication server public key certification handing out signal is received (S206). This judgment whether to be effective or not is made by judging whether the time of the clock part 66 is within the shelf-life currently described in the public key certification of the acquired authentication server 23, and when it is within a shelf-life, it is judged that it is effective. In not being effective, it carries out from the processing S201 again after fixed time lapse.

[0092]

Next, the tunnel set part 62 of the automatic setting equipment 11, The usability judging process which judges the usability of the public key certification of the automatic setting equipment 11 is performed using the public key certification Management Department 64, the control part 52 (S207), an update process is ended and the below-mentioned processing S102 in tunnel construction processing is performed.

[0093]

If it describes in details more about the usability judging process in the public key certification of this automatic setting equipment 11, in Fig.21, the public key certification Management Department 64 of the automatic setting equipment 11 will judge whether the public key certification of the automatic setting equipment 11 exists in the security information storage part 72 (S211).

[0094]

When the public key certification of the automatic setting equipment 11 does not exist, as a result of judgment to (No), The public key certification Management Department 64 of the automatic setting equipment 11, The request-for-share-distribution signal which accommodated the information on the purport that handing out of the automatic setting device identifier of the automatic setting equipment 11 concerned and the public key certification of the automatic setting equipment 11 is required that the public key certification of the automatic setting equipment 11 concerned should be acquired from the authentication server 23 is transmitted to the authentication server 23 (S212). If the public key certification Management Department 64 of the automatic setting equipment 11 receives the reply of a handing out reply signal which accommodated the public key certification of the automatic setting equipment 11 from the authentication server 23 and handing out is received (S213), it will perform processing S214. On the other hand, as a result of judgment, also when the public key certification of the automatic setting equipment 11 exists (Yes), the public key certification Management Department 64 of the automatic setting equipment 11 performs processing S214.

[0095]

In the processing S214, the public key certification Management Department 64 of the automatic setting equipment 11 judges whether the public key certification of the automatic setting equipment 11 is effective. This judgment whether to be effective or not is made by judging whether it appears in whether the public key certification of the automatic setting equipment 11 concerned is within the term of validity, and certificate cancellation Liszt.

[0096]

As a result of judgment, when not effective, to (No), the public key certification Management Department 64 of the automatic setting equipment 11 performs above-mentioned public key certification acquisition processing described using Fig.8 (S215), and continues tunnel construction processing to it. On the other hand, as a result of judgment, also when effective (Yes), the public key certification Management Department 64 of the automatic setting equipment 11 continues tunnel construction processing (S216).

[0097]

Thus, when the tunnel set part 62 in the control part 52 of the automatic setting equipment 11 of a connecting agency operates, the update process which updates the public key certification of the automatic setting equipment 11 of a connecting agency is performed.

[0098]

Return to Fig.14 thru/or Fig.18 and the tunnel set part 62 in the control part 52 of the automatic setting equipment 11 of a connecting agency,It connects with the information server 21 using the IP address of the information server 21 of the information storage part 71 for tunnel setting out, The signal transmission (connection destination tunnel external IP address requirement signal) which accommodated the information on the purport that the tunnel external IP address of the automatic setting device identifier of the automatic setting equipment 11 of a connection destination and the automatic setting equipment 11 of a connection destination is required is created, and it transmits to the information server 21 (S102). The information server 21 will search the tunnel external IP address corresponding to this automatic setting device identifier from the offer tunnel setting information table 102 based on the automatic setting device identifier accommodated in this signal, if this connection destination tunnel external IP address requirement signal is received (S103). And the information server 21 creates the signal transmission (connection destination tunnel external IP address reply signal) which accommodated the automatic setting device identifier and the tunnel external IP address

corresponding to this searched automatic setting device identifier, and replies it to the automatic setting equipment 11 (S104). When there is no automatic setting device identifier which the information server 21 is the processing S102, and was accommodated in the connection destination tunnel external IP address requirement signal here in the offer tunnel setting information table 102, The information (information that it does not register) which shows that there is no tunnel external IP address corresponding to an automatic setting device identifier is accommodated in a connection destination tunnel external IP address reply signal, and it replies to the automatic setting equipment 11. The information that it does not register is expressed by symbol strings, such as "****", "vacant", and "Null", for example.

[0099]

Next, it is judged whether the tunnel set part 62 in the automatic setting equipment 11 of a connecting agency has an effective tunnel external IP address of the connection destination accommodated in this signal, if a connection destination tunnel external IP address reply signal is received (S105). This judgment whether to be effective or not is made by judging whether the information that it did not register was accommodated in the connection destination tunnel external IP address reply signal instead of the tunnel external IP address of a connection destination, It is judged that it is effective when it is not the information that it does not register, and in being the information that it does not register, it judges that it is not effective.

[0100]

In not being effective, it judges that initial processing which the automatic setting equipment 11 of the connection destination described using Fig.13 is not performed as a result of judgment, After the lapse of fixed time, it is returned to the processing S102 by processing, and in being effective, For example by a three-way handshake (Three Way Handshake), the tunnel set part 62 in the automatic setting equipment 11 of a connecting agency establishes the automatic setting equipment 11 and the connection of a connection destination, and connects them with the automatic setting equipment of a connection destination so that communication is possible (S106). As for a three-way handshake, the host computer (this embodiment automatic setting equipment of a connecting agency) of a transmitting agency transmits the demand of starting communication to the host computer (this embodiment automatic setting equipment of a connection destination) of a transmission destination (the 1st step), If communication is O.K., it will reply an Acknowledgement (the 2nd step), and the host computer of a transmission destination is the procedure of establishing a connection by what (the 3rd step) the notice of establishment of the host computer of a transmitting agency of a connection is transmitted to the host computer of a transmission destination for.

[0101]

The tunnel set part 62 in the control part 52 of the automatic setting equipment 11 of a connection destination performs the update process which updates the public key certification of the automatic setting equipment 11 (S107). Since this update process is the same as the above-mentioned update process described using Fig.20 and Fig.21, that description is omitted.

[0102]

If a connection is established, the tunnel set part 62 in the automatic setting equipment 11 of a connecting agency will create the signal transmission (automatic setting device identifier notification signal) which accommodates the automatic setting device identifier of the automatic setting equipment 11 concerned, and will transmit to the automatic setting equipment 11 of a connection destination (S108).

[0103]

If this automatic setting device identifier notification signal is received from the automatic setting equipment 11 of a connecting agency, the tunnel set part 62 in the automatic setting equipment 11 of a connection destination, The signal transmission (automatic setting device identifier notification signal) which accommodates an own (automatic setting equipment 11 of a connection destination) automatic setting device identifier is created, and it transmits to the automatic setting equipment 11 of a connecting agency (S109).

[0104]

Next, although the automatic setting equipment 11 of a connecting agency and a connection destination obtains the public key certification of the automatic setting equipment 11 of another side, respectively and it confirms whether the public key certification of ********** 11 of another side which came to hand is genuine, there are two kinds of obtaining methods of this public key certification.

[0105]

First, it describes a connecting agency about the method of obtaining the public key certification of the automatic setting equipment 11 of another side from an authentication server in the automatic setting equipment 11 of a connection destination.

[0106]

The tunnel set part 62 in the automatic setting equipment 11 of a connection destination, The automatic setting device identifier in the automatic setting equipment 11 of a connecting agency and the signal transmission (request-for-share-distribution signal) which accommodated the information on the purport that handing out of the public key certification in the automatic setting equipment 11 of a connecting agency is required are created, and it transmits to the authentication server 23 (S110).

[0107]

If this request-for-share-distribution signal is received, the authentication server 23 will search the public key certification of the automatic setting equipment 11 corresponding to the automatic setting device identifier in the automatic setting equipment 11 of this connection origin with reference to the repository 105 based on the automatic setting device identifier of the received request-for-share-distribution signal (S111). The authentication server 23 creates the signal transmission (handing out signal) which accommodates the public key certification of the automatic setting equipment 11 of the searched connection origin, and replies it to the automatic setting equipment 11 of a connection destination (S112).

[0108]

If this handing out signal is received, the tunnel set part 62 in the automatic setting equipment 11 of a connection destination will verify whether the public key certification of the automatic setting equipment 11 of a connecting agency is genuine using the public key certification of the authentication server 23 (S113).

[0109]

the automatic setting equipment 11 of a connection destination to this automatic setting device identifier notification signal -- receiving (S109) -- the tunnel set part 62 in the automatic setting equipment 11 of a connecting agency, The signal transmission (request-for-share-distribution signal) which accommodated the information on the purport that the automatic setting device identifier in the automatic setting equipment 11 of a connection destination and the public key certification in the automatic setting equipment 11 of a connection destination are required is created, and it transmits to the authentication server 23 (S114).

[0110]