UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/372,208	07/18/2017	9712494	664.1078CON2	6275

33369 7590 06/28/2017

FASTH LAW OFFICES (ROLF FASTH)
1206 Stanridge Drive
Raleigh, NC 27613-7063

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

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

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

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

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

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

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

Sami Vaarala, Helsinki, FINLAND;
MPH Technologies Oy, Espoo, FINLAND;
Antti Nuopponen, Espoo, FINLAND;

PART B - FEE(S) TRANSMITTAL

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

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

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

33369 7560 06/23/2017
FASTH LAW OFFICES (ROLF FASTH)
1206 Stanridge Drive
Raleigh, NC 27613-7063

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

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

Sloan Smith	(Depositor's name)
Sloan Smith	(Signature)
13 June 2017	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/372,208	12/07/2016	Sami Vaarala	664.1078(CON2	6275

TITLE OF INVENTION: METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$960	$0	$0	$960	06/23/2017

EXAMINER	ART UNIT	CLASS-SUBCLASS
TOWFIGH, AFSHAWN M	2469	713-171000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached
- ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

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

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

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

(A) NAME OF ASSIGNEE: MPH Technologies Oy
(B) RESIDENCE: (CITY and STATE OR COUNTRY): Espoo, Finland

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

4a. The following fee(s) are submitted:
- ☑ Issue Fee
- ☐ Publication Fee (No small entity discount permitted)
- ☐ Advance Order - # of Copies

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ☐ A check is enclosed.
- ☐ Payment by credit card. Form PTO-2038 is attached.
- ☑ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number 060243 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ☐ Applicant certifying micro entity status. See 37 CFR 1.29 — NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- ☐ Applicant asserting small entity status. See 37 CFR 1.27 — NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- ☐ Applicant changing to regular undiscounted fee status. — NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

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

Authorized Signature: Rolf Fasth — Date: 13 June 2017
Typed or printed name: Rolf Fasth — Registration No.: 36999

PTOL-85 Part B (10-13) Approved for use through 10/31/2013 OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Attorney Ref. No. 664.1078CON2 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Sami Vaarala, Antti Nuopponen

Serial No. 15/372,208

Filed: 7 December 2016

For: METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION

Date: 13 June 2017

Confirmation No. 6275

CERTIFICATE OF MAILING

I HEREBY CERTIFY THAT THIS PAPER AND THE DOCUMENTS REFERRED TO AS BEING ATTACHED OR ENCLOSED HEREWITH ARE BEING FORWARDED TO THE COMMISSIONER FOR PATENTS, UNITED STATES PATENT OFFICE ELECTRONICALLY ON June 13, 2017

/rfasth/
Rolf Fasth
Attorney for Applicant

TRANSMITTAL LETTER

ELECTRONIC SUBMISSION
COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

In connection with issuance of a patent, enclosed for filing in the above-referenced application are the following:

(X) Form PTOL-85 (Part B - Fee Transmittal)
(X) Issue Fee ($960;)to be charged to Account No. 06-0243.
(X) The Commissioner is hereby authorized to charge any additional fees which may be required in connection with the issuance of a patent or credit over-payment to Account No. 06-0243.

Respectfully submitted,

FASTH LAW OFFICES

/rfasth/

Rolf Fasth
Registration No. 36,999

FASTH LAW OFFICES
1206 Stanridge Drive
Raleigh, North Carolina 27613-7063 USA
Tel: +1-910-687-0001
Fax: +1-919-882-1265

Attorney Ref. No. 664.1078CON2

Electronic Patent Application Fee Transmittal

Application Number:	15372208
Filing Date:	07-Dec-2016
Title of Invention:	METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION
First Named Inventor/Applicant Name:	Sami Vaarala
Filer:	Rolf Fasth/Sloan Smith
Attorney Docket Number:	664.1078CON2

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

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

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
UTILITY APPL ISSUE FEE	1501	1	960	960
PUBL. FEE- EARLY, VOLUNTARY, OR NORMAL	1504	1	0	0
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**960**

Electronic Acknowledgement Receipt

EFS ID:	29478567
Application Number:	15372208
International Application Number:	
Confirmation Number:	6275
Title of Invention:	METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION
First Named Inventor/Applicant Name:	Sami Vaarala
Customer Number:	33369
Filer:	Rolf Fasth/Sloan Smith
Filer Authorized By:	Rolf Fasth
Attorney Docket Number:	664.1078CON2
Receipt Date:	13-JUN-2017
Filing Date:	07-DEC-2016
Time Stamp:	13:07:02
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$960
RAM confirmation Number	061317INTEFSW00010675060243
Deposit Account	060243
Authorized User	Sloan Smith

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

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

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	PART_B.pdf	1853116 066d1012e51ee7d3b58ec70576d230d31edadf71	no	1
Warnings:					
Information:					
2	Transmittal Letter	TRX.pdf	245084 893ad74b7d3ce76fe06a3039b65482f539a27535	no	1
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	32264 f3e1b5012523b50f45a301e4f2adccf5084fcb64	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	2130464		

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
P.O.BOX 1450
ALEXANDRIA VA 22313-1451

PRESORTED
FIRST-CLASS MAIL
U.S. POSTAGE PAID
POSTEDIGITAL
NNNNN

FASTH LAW OFFICES (ROLF FASTH)
1206 Stanridge Drive
Raleigh, NC 27613-7063

Courtesy Reminder for
Application Serial No: 15/372,208

Attorney Docket No: 664.1078CON2
Customer Number: 33369
Date of Electronic Notification: 03/23/2017

This is a courtesy reminder that new correspondence is available for this application. If you have not done so already, please review the correspondence. The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

An email notification regarding the correspondence was sent to the following email address(es) associated with your customer number:
sloan.smith@fasthlaw.com

To view your correspondence online or update your email addresses, please visit us anytime at **https://sportal.uspto.gov/secure/myportal/privatepair.** If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov or call 1-866-217-9197.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
15/372,208	12/07/2016	Sami Vaarala	664.1078CON2

CONFIRMATION NO. 6275

33369
FASTH LAW OFFICES (ROLF FASTH)
1206 Stanridge Drive
Raleigh, NC 27613-7063

PUBLICATION NOTICE

OC000000090296543

Title:METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION

Publication No.US-2017-0093799-A1
Publication Date:03/30/2017

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 (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, 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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

33369 7590 03/23/2017

FASTH LAW OFFICES (ROLF FASTH)
1206 Stanridge Drive
Raleigh, NC 27613-7063

EXAMINER
TOWFIGHI, AFSHAWN M

ART UNIT	PAPER NUMBER
2469	

DATE MAILED: 03/23/2017

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/372,208	12/07/2016	Sami Vaarala	664.1078CON2	6275

TITLE OF INVENTION: METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$960	$0	$0	$960	06/23/2017

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

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

HOW TO REPLY TO THIS NOTICE:

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

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

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

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

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

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

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

PART B - FEE(S) TRANSMITTAL

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

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

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

33369 7590 03/23/2017
FASTH LAW OFFICES (ROLF FASTH)
1206 Stanridge Drive
Raleigh, NC 27613-7063

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

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

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/372,208	12/07/2016	Sami Vaarala	664.1078CON2	6275

TITLE OF INVENTION: METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$960	$0	$0	$960	06/23/2017

EXAMINER	ART UNIT	CLASS-SUBCLASS
TOWFIGHI, AFSHAWN M	2469	713-171000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

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

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

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

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

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

4a. The following fee(s) are submitted:
- ❑ Issue Fee
- ❑ Publication Fee (No small entity discount permitted)
- ❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ❑ A check is enclosed.
- ❑ Payment by credit card. Form PTO-2038 is attached.
- ❑ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ❑ Applicant certifying micro entity status. See 37 CFR 1.29
  NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- ❑ Applicant asserting small entity status. See 37 CFR 1.27
  NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- ❑ Applicant changing to regular undiscounted fee status.
  NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

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

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/372,208	12/07/2016	Sami Vaarala	664.1078CON2	6275

33369 7590 03/23/2017

FASTH LAW OFFICES (ROLF FASTH)
1206 Stanridge Drive
Raleigh, NC 27613-7063

EXAMINER	
TOWFIGHI, AFSHAWN M	

ART UNIT	PAPER NUMBER
2469	

DATE MAILED: 03/23/2017

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

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

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

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

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

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

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

Privacy Act Statement

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

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

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

Notice of Allowability	Application No. 15/372,208	Applicant(s) VAARALA ET AL.	
	Examiner AFSHAWN TOWFIGHI	Art Unit 2469	AIA (First Inventor to File) Status No

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

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

1. ☒ This communication is responsive to *claims filed 12/13/16*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *1-11*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.
4. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☒ All b) ☐ Some *c) ☐ None of the:
   1. ☒ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

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

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

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☒ Interview Summary (PTO-413), Paper No./Mail Date *3/15/17* .
5. ☒ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/AFSHAWN TOWFIGHI/
Primary Examiner, Art Unit 2469

EXAMINER'S AMENDMENT

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

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in an interview with Rolf Fasth on 3/15/17.

The application has been amended as follows:

1. (Amended) An intermediate computer for secure forwarding of messages in a telecommunication network, comprising:

an intermediate computer configured to connect to a telecommunication network;

the intermediate computer configured to be assigned with a first network address in the telecommunication network;

the intermediate computer configured to receive from a mobile computer a secure message sent to the first network address having an encrypted data payload of a message and a unique identity, the data payload encrypted with a cryptographic key derived from a key exchange protocol;

the intermediate computer configured to read the unique identity from the secure message sent to the first network address; and

the intermediate computer configured to access a translation table, to find a destination address from the translation table using the unique identity, and

to securely forward the encrypted data payload to the destination address using a network address of the intermediate computer as a source address of a forwarded message containing the encrypted data payload wherein the intermediate computer does not have the cryptographic key to decrypt the encrypted data payload.

2. (Previously presented) The intermediate computer of claim 1, wherein the intermediate computer is further configured to substitute the unique identity read from the secure message with another unique identity prior to forwarding the encrypted data payload.

3. (Previously presented) The intermediate computer of claim 1, wherein the translation table is stored at the intermediate computer.

4. (Previously presented) The intermediate computer of claim 1, wherein the translation table includes two partitions, the first partition containing information fields related to the connection over which the secure message is sent to the first network address, the second partition containing information fields related to the connection over which the forwarded encrypted data payload is sent to the destination address.

5. (Previously presented) The intermediate computer of claim 1, wherein the intermediate computer is not configured to access cryptographic keys used to encrypt or authenticate the messages.

6. (Previously presented) The intermediate computer of claim 1, wherein the intermediate computer is configured to forward the encrypted data payload using SSL or TLS protocol.

7. (Previously presented) The intermediate computer of claim 1, wherein the intermediate computer is configured to receive secure messages using SSL or TLS protocol.

8. (Previously presented) The intermediate computer of claim 1, wherein the unique identity read from the secure message includes one or more Security Parameter Index values.

9. (Previously presented) The intermediate computer of claim 1, wherein the intermediate computer is configured to modify the translation table entry address fields in response to a signaling message sent from the mobile computer when the mobile computer changes its address such that the intermediate computer can know that the address of the mobile computer is changed.

10. (Previously presented) The intermediate computer of claim 1, wherein the intermediate computer is a server.

11. (Previously presented) The intermediate computer of claim 1, wherein the source address of the forwarded message is the same as the first network address.

12-21. Canceled.

Allowable Subject Matter

3. Claims 1-11 (amended) are allowed.

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

Amended claims 1-11 are allowable over prior art since the prior art taken individually or in combination fails to particularly disclose, fairly suggests, or render obvious the following limitations:

In claim 1, … *the intermediate computer configured to receive from a mobile computer a secure message sent to the first network address having an encrypted data payload of a message and a unique identity, the data payload encrypted with a cryptographic key derived from a key exchange protocol; the intermediate computer configured to read the unique identity from the secure message sent to the first network address; and*

the intermediate computer configured to access a translation table, to find a destination address from the translation table using the unique identity, and to securely forward the encrypted data payload to the destination address using a network address of the intermediate computer as a source address of a forwarded message containing the encrypted data payload wherein the intermediate computer does not have the cryptographic key to decrypt the encrypted data payload...in combination with other limitations recited as specified in Claim 1.

The first closest prior art of record is Kunzinger et al (Pub No: 2002/0091921), herein Kunzinger. Kunzinger teaches a method for end to end data sending via and intermediate gateway and a hash value of IPSec used in a packet and tables to route the packet do its destination. Kunzinger et al does not teach *the intermediate computer configured to receive from a mobile computer a secure message sent to the first network address having an encrypted data payload of a message and a unique identity, the data payload encrypted with a cryptographic key derived from a key exchange protocol; the intermediate computer configured to read the unique identity from the secure message sent to the first network address; and the intermediate computer configured to access a translation table, to find a destination address from the translation table using the unique identity, and to securely forward the encrypted data payload to the destination address using a network address of the intermediate computer as a source address of a forwarded message containing the encrypted data*

payload wherein the intermediate computer does not have the cryptographic key to decrypt the encrypted data payload.

The second closest prior art of record is Gunter et al (Patent: 7,055,027), herein Gunter. Gunter discloses a system for forming of a connection without a firewall present. When a connection has been formed, a device in an internal network sends the keys to a firewall so the firewall can follow the connection. Gunter fails to disclose *the intermediate computer configured to receive from a mobile computer a secure message sent to the first network address having an encrypted data payload of a message and a unique identity, the data payload encrypted with a cryptographic key derived from a key exchange protocol; the intermediate computer configured to read the unique identity from the secure message sent to the first network address; and the intermediate computer configured to access a translation table, to find a destination address from the translation table using the unique identity, and to securely forward the encrypted data payload to the destination address using a network address of the intermediate computer as a source address of a forwarded message containing the encrypted data payload wherein the intermediate computer does not have the cryptographic key to decrypt the encrypted data payload.*

For these reasons, in conjunction with the other limitations of the independent claims, puts this case in condition for allowance.

Additional reasons for allowance can be found in the Notice of Alowance for parent application 10/500,930 dated 1/12/12 and 13/685,544 dated 10/21/13.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance.”

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to AFSHAWN TOWFIGHI whose telephone number is (571)270-7296. The examiner can normally be reached on Monday - Friday 9:00 A.M. to 6:00 P.M..

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Ian Moore can be reached on (571)272-3085. 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.

/AFSHAWN TOWFIGHI/

Primary Examiner, Art Unit 2469

Examiner-Initiated Interview Summary	Application No.	Applicant(s)	
	15/372,208	VAARALA ET AL.	
	Examiner	Art Unit	
	AFSHAWN TOWFIGHI	2469	

All participants (applicant, applicant's representative, PTO personnel):

(1) *AFSHAWN TOWFIGHI*. (3)_____.

(2) *Rolf Fasth*. (4)_____.

Date of Interview: *15 March 2017*.

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: *n/a*.

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...)

Authorization was given via email authorization to add clafication on the key exchange to the secure connection to claim 1. Examiner asked for a TD to be filed.

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of 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

/AFSHAWN TOWFIGHI/ Primary Examiner, Art Unit 2469	

Notice of References Cited	Application/Control No. 15/372,208	Applicant(s)/Patent Under Reexamination VAARALA ET AL.	
	Examiner AFSHAWN TOWFIGHI	Art Unit 2469	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-6,732,269 B1	05-2004	Baskey; Michael Edward	H04L63/166	713/153
*	B	US-6,718,388 B1	04-2004	Yarborough; William Jordan	H04L63/0227	709/217
*	C	US-6,957,346 B1	10-2005	Kivinen; Tero	H04L12/4633	713/153
*	D	US-6,795,917 B1	09-2004	Ylonen; Tatu	H04L29/06	713/160
*	E	US-7,055,027 B1	05-2006	Gunter; David	H04L63/30	709/223
*	F	US-2002/0091921 A1	07-2002	Kunzinger, Charles A.	H04L63/0428	713/153
*	G	US-2002/0004900 A1	01-2002	PATEL, BAIJU V.	G06Q30/02	713/155
*	H	US-2001/0047487 A1	11-2001	Linnakangas, Tommi	H04L63/0428	726/12
*	I	US-6,985,953 B1	01-2006	Sandhu; Ravi	G06F17/3089	709/225
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2010/03/15 11:04
S2	4057	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2010/03/15 14:29
S3	10	S2 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2010/03/15 14:29
S4	393	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2010/08/20 11:49
S5	112	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2010/08/20 12:00
S6	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2010/08/21 22:59
S7	7	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2010/08/21 23:00
S8	16	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2010/08/21 23:01
S9	2210	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2010/08/23 11:02
S10	1902	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2010/08/23 11:02
S11	1902	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2010/08/23 11:02
S12	1468	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2010/08/23 11:03
S13	1468	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2010/08/23 11:03
S14	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2011/01/17 20:28
S15	4607	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2011/01/17 20:28
S16	12	S15 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2011/01/17 20:28
S17	417	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2011/01/17 20:28
S18	122	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2011/01/17 20:28
S19	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2011/01/17 20:28
S20	7	ipsec same tunnel$3 same IKE	US-PGPUB;	OR	OFF	2011/01/17

		same (gateway or proxy or intermediate) and cookie	USPAT			20:28
S21	17	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2011/01/17 20:28
S22	2374	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/01/17 20:28
S23	2040	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/01/17 20:28
S24	2040	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/01/17 20:28
S25	1580	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/01/17 20:28
S26	1580	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/01/17 20:28
S27	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2011/04/18 08:40
S28	4741	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2011/04/18 08:40
S29	12	S28 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2011/04/18 08:40
S30	436	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2011/04/18 08:40
S31	128	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2011/04/18 08:40
S32	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2011/04/18 08:40
S33	8	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2011/04/18 08:40
S34	18	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2011/04/18 08:40
S35	2487	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/04/18 08:40
S36	2139	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/04/18 08:40
S37	2139	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/04/18 08:40
S38	1642	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/04/18 08:40
S39	1642	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/04/18 08:40
S40	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2011/04/18 08:40
S41	4741	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2011/04/18 08:40
S42	12	S41 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2011/04/18 08:40
S43	436	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2011/04/18 08:40
S44	128	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2011/04/18 08:40

S45	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2011/04/18 08:40
S46	8	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2011/04/18 08:40
S47	18	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2011/04/18 08:40
S48	2487	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/04/18 08:40
S49	2139	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/04/18 08:40
S50	2139	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/04/18 08:40
S51	1642	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/04/18 08:40
S52	1642	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/04/18 08:40
S54	1	"7882538"	US-PGPUB; USPAT	OR	OFF	2011/04/27 16:38
S55	15	"6744741"	US-PGPUB; USPAT	OR	OFF	2011/04/27 16:40
S56	9	"7055027"	US-PGPUB; USPAT	OR	OFF	2011/04/28 11:51
S57	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S58	5125	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S59	13	S58 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S60	501	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S61	152	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S62	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2011/12/28 20:07
S63	10	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S64	20	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S65	2794	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S66	2398	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S67	2398	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S68	1829	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S69	1829	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07

S70	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S71	5125	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S72	13	S71 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S73	501	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S74	152	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S75	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2011/12/28 20:07
S76	10	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S77	20	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S78	2794	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S79	2398	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S80	2398	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S81	1829	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S82	1829	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S83	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S84	5125	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S85	13	S84 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S86	501	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S87	152	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S88	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2011/12/28 20:07
S89	10	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S90	20	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S91	2794	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S92	2398	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S93	2398	ipsec with (ssl or tls)	US-PGPUB;	OR	OFF	2011/12/28

			USPAT			20:07
S94	1829	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S95	1829	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S96	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S97	5125	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S98	13	S97 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S99	501	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S100	152	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S101	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2011/12/28 20:07
S102	10	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S103	20	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S104	2794	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S105	2398	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S106	2398	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S107	1829	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S108	1829	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S109	1	"7882538"	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S110	18	"6744741"	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S111	13	"7055027"	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
S112	9	((SAMI) near2 (VAARALA)).INV.	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:09
S113	9	((ANTTI) near2 (NUOPPONEN)).INV.	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:10
S114	9	S112 or S113	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:11
S115	8	S114 and (secure adj connection).clm.	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:11
S116	7	S114 and (secure adj connection with address).clm.	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:11
S117	1	S114 and (secure adj connection with intermediate with address).clm.	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:12

S121	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S122	5426	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S123	15	S122 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S124	544	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S125	170	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S126	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2012/08/12 17:25
S127	10	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S128	21	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S129	3132	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S130	2700	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S131	2700	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S132	2068	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S133	2068	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S134	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S135	5426	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S136	15	S135 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S137	544	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S138	170	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S139	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2012/08/12 17:25
S140	10	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S141	21	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S142	3132	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S143	2700	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S144	2700	ipsec with (ssl or tls)	US-PGPUB;	OR	OFF	2012/08/12

			USPAT			17:25
S145	2068	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S146	2068	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S147	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S148	5426	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S149	15	S148 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S150	544	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S151	170	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S152	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2012/08/12 17:25
S153	10	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S154	21	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S155	3132	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S156	2700	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S157	2700	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S158	2068	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S159	2068	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S160	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S161	5426	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S162	15	S161 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S163	544	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S164	170	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S165	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2012/08/12 17:25
S166	10	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S167	21	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25

S168	3132	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S169	2700	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S170	2700	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S171	2068	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S172	2068	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S173	4	"7882538"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S174	20	"6744741"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S175	19	"7055027"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S176	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S177	5426	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S178	15	S177 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S179	544	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S180	170	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S181	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2012/08/12 17:25
S182	10	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S183	21	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S184	3132	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S185	2700	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S186	2700	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S187	2068	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S188	2068	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S189	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S190	5426	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S191	15	S190 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S192	544	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25

S193	170	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S194	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2012/08/12 17:25
S195	10	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S196	21	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S197	3132	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S198	2700	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S199	2700	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S200	2068	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S201	2068	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S202	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S203	5426	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S204	15	S203 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S205	544	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S206	170	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S207	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2012/08/12 17:25
S208	10	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S209	21	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S210	3132	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S211	2700	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S212	2700	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S213	2068	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S214	2068	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S215	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S216	5426	709/236.ccls. or 709/245.ccls.	US-PGPUB;	OR	OFF	2012/08/12

			USPAT			17:25
S217	15	S216 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S218	544	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S219	170	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S220	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2012/08/12 17:25
S221	10	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S222	21	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S223	3132	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S224	2700	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S225	2700	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S226	2068	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S227	2068	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S228	4	"7882538"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S229	20	"6744741"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S230	19	"7055027"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S231	9	((SAMI) near2 (VAARALA)).INV.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S232	9	((ANTTI) near2 (NUOPPONEN)).INV.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S233	9	S231 or S232	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S234	8	S233 and (secure adj connection).clm.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S235	7	S233 and (secure adj connection with address).clm.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S236	1	S233 and (secure adj connection with intermediate with address).clm.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
S237	107613	("6732269" "6718388" "6957346" "6795917")".pn"	US-PGPUB; USPAT; EPO; JPO	OR	ON	2012/08/12 17:47
S238	4	("6732269" "6718388" "6957346" "6795917").pn.	US-PGPUB; USPAT; EPO; JPO	OR	ON	2012/08/12 17:47
S239	5426	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S240	3132	ipsec same (ssl or tls)	US-PGPUB;	OR	OFF	2012/08/12

			USPAT			17:57
S241	2700	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S242	2700	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S243	2068	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S244	5426	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S245	3132	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S246	2700	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S247	2700	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S248	2068	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S249	5426	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S250	3132	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S251	2700	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S252	2700	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S253	2068	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S254	5426	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S255	3132	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S256	2700	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S257	2700	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S258	2068	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S259	4	"7882538"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S260	5426	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S261	3132	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S262	2700	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S263	2700	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S264	2068	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S265	5426	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S266	3132	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S267	2700	ipsec with(ssl or tls)	US-PGPUB;	OR	OFF	2012/08/12

			USPAT			17:57
S268	2700	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S269	2068	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S270	5426	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S271	3132	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S272	2700	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S273	2700	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S274	2068	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S275	5426	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S276	3132	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S277	2700	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S278	2700	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S279	2068	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S280	4	"7882538"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S281	9	S231 or S232	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S282	8	S233 and (secure adj connection).clm.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S283	7	S233 and (secure adj connection with address).clm.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S284	1	S233 and (secure adj connection with intermediate with address).clm.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S285	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S286	15	S122 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S287	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2012/08/12 17:57
S288	10	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S289	21	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S290	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S291	15	S135 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S292	2	"US 20060173968"	US-PGPUB;	OR	OFF	2012/08/12

			USPAT; USOCR; DERWENT			17:57
S293	10	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S294	21	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S295	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S296	15	S148 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S297	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2012/08/12 17:57
S298	10	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S299	21	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S300	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S301	15	S161 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S302	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2012/08/12 17:57
S303	10	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S304	21	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S305	20	"6744741"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S306	19	"7055027"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S307	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S308	15	S177 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S309	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2012/08/12 17:57
S310	10	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S311	21	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S312	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S313	15	S190 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S314	2	"US 20060173968"	US-PGPUB;	OR	OFF	2012/08/12

			USPAT; USOCR; DERWENT			17:57
S315	10	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S316	21	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S317	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S318	15	S203 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S319	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2012/08/12 17:57
S320	10	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S321	21	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S322	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S323	15	S216 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S324	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2012/08/12 17:57
S325	10	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S326	21	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S327	20	"6744741"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S328	19	"7055027"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S329	9	((SAMI) near2 (VAARALA)).INV.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S330	9	((ANTTI) near2 (NUOPPONEN)).INV.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S331	170	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S332	170	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S333	170	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S334	170	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S335	170	ipsec same tunnel$3 same IKE same (gateway or proxy or	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57

		intermediate)				
S336	170	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S337	170	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S338	170	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S339	544	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S340	544	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S341	544	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S342	544	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S343	544	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S344	544	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S345	544	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S346	544	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S347	2068	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S348	2068	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S349	2068	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S350	2068	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S351	2068	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S352	2068	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S353	2068	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S354	2068	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
S355	107613	("6732269" "6718388" "6957346" "6795917")".pn"	US-PGPUB; USPAT; EPO; JPO	OR	ON	2012/08/12 17:57
S356	4	("6732269" "6718388" "6957346" "6795917").pn.	US-PGPUB; USPAT; EPO; JPO	OR	ON	2012/08/12 17:57
S363	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S364	5980	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S365	19	S364 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53

S366	625	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S367	192	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S368	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2013/10/08 12:53
S369	12	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S370	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S371	3955	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S372	3472	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S373	3472	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S374	2591	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S375	2591	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S376	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S377	5980	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S378	19	S377 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S379	625	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S380	192	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S381	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2013/10/08 12:53
S382	12	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S383	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S384	3955	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S385	3472	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S386	3472	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S387	2591	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S388	2591	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S389	2	"20010047487"	US-PGPUB;	OR	OFF	2013/10/08

			USPAT			12:53
S390	5980	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S391	19	S390 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S392	625	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S393	192	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S394	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2013/10/08 12:53
S395	12	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S396	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S397	3955	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S398	3472	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S399	3472	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S400	2591	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S401	2591	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S402	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S403	5980	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S404	19	S403 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S405	625	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S406	192	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S407	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2013/10/08 12:53
S408	12	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S409	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S410	3955	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S411	3472	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S412	3472	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53

S413	2591	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S414	2591	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S415	5	"7882538"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S416	21	"6744741"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S417	25	"7055027"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S418	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S419	5980	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S420	19	S419 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S421	625	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S422	192	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S423	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2013/10/08 12:53
S424	12	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S425	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S426	3955	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S427	3472	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S428	3472	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S429	2591	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S430	2591	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S431	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S432	5980	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S433	19	S432 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S434	625	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S435	192	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S436	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2013/10/08 12:53

S437	12	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S438	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S439	3955	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S440	3472	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S441	3472	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S442	2591	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S443	2591	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S444	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S445	5980	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S446	19	S445 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S447	625	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S448	192	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S449	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2013/10/08 12:53
S450	12	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S451	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S452	3955	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S453	3472	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S454	3472	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S455	2591	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S456	2591	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S457	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S458	5980	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S459	19	S458 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S460	625	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S461	192	ipsec same tunnel$3 same IKE same (gateway or proxy or	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53

		intermediate)				
S462	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2013/10/08 12:53
S463	12	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S464	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S465	3955	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S466	3472	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S467	3472	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S468	2591	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S469	2591	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S470	5	"7882538"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S471	21	"6744741"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S472	25	"7055027"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S473	11	((SAMI) near2 (VAARALA)).INV.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S474	11	((ANTTI) near2 (NUOPPONEN)).INV.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S475	11	S473 or S474	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S476	10	S475 and (secure adj connection).clm.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S477	9	S475 and (secure adj connection with address).clm.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S478	3	S475 and (secure adj connection with intermediate with address).clm.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S479	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S480	5980	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S481	19	S480 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S482	625	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S483	192	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S484	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2013/10/08 12:53
S485	12	ipsec same tunnel$3 same IKE	US-PGPUB;	OR	OFF	2013/10/08

		same (gateway or proxy or intermediate) and cookie	USPAT			12:53
S486	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S487	3955	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S488	3472	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S489	3472	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S490	2591	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S491	2591	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S492	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S493	5980	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S494	19	S493 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S495	625	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S496	192	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S497	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2013/10/08 12:53
S498	12	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S499	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S500	3955	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S501	3472	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S502	3472	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S503	2591	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S504	2591	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S505	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S506	5980	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S507	19	S506 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S508	625	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S509	192	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53

S510	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2013/10/08 12:53
S511	12	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S512	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S513	3955	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S514	3472	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S515	3472	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S516	2591	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S517	2591	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S518	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S519	5980	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S520	19	S519 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S521	625	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S522	192	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S523	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2013/10/08 12:53
S524	12	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S525	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S526	3955	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S527	3472	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S528	3472	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S529	2591	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S530	2591	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S531	5	"7882538"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S532	21	"6744741"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S533	25	"7055027"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53

S534	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S535	5980	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S536	19	S535 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S537	625	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S538	192	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S539	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2013/10/08 12:53
S540	12	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S541	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S542	3955	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S543	3472	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S544	3472	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S545	2591	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S546	2591	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S547	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S548	5980	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S549	19	S548 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S550	625	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S551	192	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S552	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2013/10/08 12:53
S553	12	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S554	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S555	3955	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S556	3472	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S557	3472	ipsec with (ssl or tls)	US-PGPUB;	OR	OFF	2013/10/08

			USPAT			12:53
S558	2591	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S559	2591	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S560	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S561	5980	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S562	19	S561 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S563	625	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S564	192	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S565	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2013/10/08 12:53
S566	12	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S567	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S568	3955	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S569	3472	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S570	3472	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S571	2591	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S572	2591	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S573	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S574	5980	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S575	19	S574 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S576	625	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S577	192	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S578	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2013/10/08 12:53
S579	12	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S580	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53

S581	3955	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S582	3472	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S583	3472	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S584	2591	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S585	2591	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S586	5	"7882538"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S587	21	"6744741"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S588	25	"7055027"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S589	11	((SAMI) near2 (VAARALA)).INV.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S590	11	((ANTTI) near2 (NUOPPONEN)).INV.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S591	11	S589 or S590	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S592	10	S591 and (secure adj connection).clm.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S593	9	S591 and (secure adj connection with address).clm.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S594	3	S591 and (secure adj connection with intermediate with address).clm.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S595	118275	("6732269" "6718388" "6957346" "6795917")".pn"	US-PGPUB; USPAT; EPO; JPO	OR	ON	2013/10/08 12:53
S596	4	("6732269" "6718388" "6957346" "6795917").pn.	US-PGPUB; USPAT; EPO; JPO	OR	ON	2013/10/08 12:53
S597	5980	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S598	3955	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S599	3472	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S600	3472	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S601	2591	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S602	5980	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S603	3955	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S604	3472	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S605	3472	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S606	2591	ipsec near5(ssl or tls)	US-PGPUB;	OR	OFF	2013/10/08

			USPAT			12:53
S607	5980	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S608	3955	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S609	3472	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S610	3472	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S611	2591	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S612	5980	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S613	3955	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S614	3472	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S615	3472	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S616	2591	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S617	5	"7882538"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S618	5980	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S619	3955	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S620	3472	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S621	3472	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S622	2591	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S623	5980	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S624	3955	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S625	3472	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S626	3472	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S627	2591	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S628	5980	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S629	3955	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S630	3472	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S631	3472	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S632	2591	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S633	5980	709/236.ccls. or 709/245.ccls.	US-PGPUB;	OR	OFF	2013/10/08

			USPAT			12:53
S634	3955	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S635	3472	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S636	3472	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S637	2591	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S638	5	"7882538"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S639	11	S589 or S590	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S640	10	S591 and (secure adj connection).clm.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S641	9	S591 and (secure adj connection with address).clm.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S642	3	S591 and (secure adj connection with intermediate with address).clm.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S643	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S644	19	S480 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S645	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2013/10/08 12:53
S646	12	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S647	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S648	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S649	19	S493 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S650	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2013/10/08 12:53
S651	12	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S652	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S653	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S654	19	S506 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S655	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2013/10/08 12:53
S656	12	ipsec same tunnel$3 same IKE	US-PGPUB;	OR	OFF	2013/10/08

		same (gateway or proxy or intermediate) and cookie	USPAT			12:53
S657	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S658	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S659	19	S519 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S660	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2013/10/08 12:53
S661	12	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S662	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S663	21	"6744741"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S664	25	"7055027"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S665	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S666	19	S535 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S667	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2013/10/08 12:53
S668	12	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S669	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S670	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S671	19	S548 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S672	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2013/10/08 12:53
S673	12	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S674	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S675	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S676	19	S561 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S677	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2013/10/08 12:53
S678	12	ipsec same tunnel$3 same IKE	US-PGPUB;	OR	OFF	2013/10/08

		same (gateway or proxy or intermediate) and cookie	USPAT			12:53
S679	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S680	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S681	19	S574 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S682	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2013/10/08 12:53
S683	12	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S684	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S685	21	"6744741"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S686	25	"7055027"	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S687	11	((SAMI) near2 (VAARALA)).INV.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S688	11	((ANTTI) near2 (NUOPPONEN)).INV.	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S689	192	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S690	192	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S691	192	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S692	192	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S693	192	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S694	192	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S695	192	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S696	192	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S697	625	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S698	625	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S699	625	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S700	625	ipsec same tunnel$3 same IKE	US-PGPUB;	OR	OFF	2013/10/08

			USPAT			12:53
S701	625	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S702	625	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S703	625	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S704	625	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S705	2591	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S706	2591	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S707	2591	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S708	2591	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S709	2591	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S710	2591	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S711	2591	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S712	2591	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2013/10/08 12:53
S713	118275	("6732269" "6718388" "6957346" "6795917")".pn"	US-PGPUB; USPAT; EPO; JPO	OR	ON	2013/10/08 12:53
S714	4	("6732269" "6718388" "6957346" "6795917").pn.	US-PGPUB; USPAT; EPO; JPO	OR	ON	2013/10/08 12:53
S724	14	advanced with dns with lookup	US-PGPUB; USPAT; EPO; JPO	OR	ON	2013/10/08 15:12
S725	1	pre?fetch with dns with lookup	US-PGPUB; USPAT; EPO; JPO	OR	ON	2013/10/08 15:13
S726	3	pre?fetch$3 with dns with lookup	US-PGPUB; USPAT; EPO; JPO	OR	ON	2013/10/08 15:13
S727	174	(webpage or website) with block$3 with collect$3	US-PGPUB; USPAT; EPO; JPO	OR	ON	2013/10/08 15:22
S728	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S729	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S730	27	S729 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S731	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S732	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S733	3	"US 20060173968"	US-PGPUB;	OR	OFF	2016/12/06

			USPAT; USOCR; DERWENT			18:36
S734	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S735	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S736	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S737	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S738	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S739	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S740	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S741	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S742	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S743	27	S742 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S744	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S745	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S746	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S747	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S748	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S749	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S750	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S751	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S752	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S753	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S754	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S755	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S756	27	S755 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S757	862	ipsec same tunnel$3 same IKE	US-PGPUB;	OR	OFF	2016/12/06

			USPAT			18:36
S758	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S759	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S760	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S761	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S762	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S763	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S764	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S765	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S766	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S767	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S768	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S769	27	S768 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S770	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S771	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S772	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S773	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S774	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S775	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S776	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S777	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S778	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S779	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S780	16	"7882538"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36

S781	23	"6744741"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S782	42	"7055027"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S783	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S784	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S785	27	S784 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S786	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S787	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S788	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S789	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S790	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S791	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S792	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S793	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S794	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S795	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S796	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S797	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S798	27	S797 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S799	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S800	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S801	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S802	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S803	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S804	7044	ipsec same (ssl or tls)	US-PGPUB;	OR	OFF	2016/12/06

			USPAT			18:36
S805	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S806	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S807	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S808	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S809	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S810	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S811	27	S810 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S812	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S813	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S814	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S815	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S816	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S817	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S818	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S819	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S820	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S821	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S822	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S823	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S824	27	S823 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S825	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S826	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S827	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S828	19	ipsec same tunnel$3 same IKE	US-PGPUB;	OR	OFF	2016/12/06

		same (gateway or proxy or intermediate) and cookie	USPAT			18:36
S829	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S830	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S831	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S832	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S833	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S834	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S835	16	"7882538"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S836	23	"6744741"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S837	42	"7055027"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S838	11	((SAMI) near2 (VAARALA)).INV.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S839	11	((ANTTI) near2 (NUOPPONEN)).INV.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S840	11	S838 or S839	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S841	10	S840 and (secure adj connection).clm.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S842	9	S840 and (secure adj connection with address).clm.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S843	3	S840 and (secure adj connection with intermediate with address).clm.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S844	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S845	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S846	27	S845 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S847	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S848	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S849	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S850	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S851	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S852	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36

S853	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S854	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S855	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S856	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S857	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S858	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S859	27	S858 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S860	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S861	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S862	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S863	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S864	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S865	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S866	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S867	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S868	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S869	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S870	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S871	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S872	27	S871 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S873	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S874	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S875	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S876	19	ipsec same tunnel$3 same IKE same (gateway or proxy or	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36

		intermediate) and cookie				
S877	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S878	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S879	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S880	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S881	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S882	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S883	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S884	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S885	27	S884 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S886	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S887	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S888	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S889	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S890	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S891	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S892	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S893	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S894	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S895	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S896	16	"7882538"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S897	23	"6744741"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S898	42	"7055027"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S899	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S900	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S901	27	S900 and secure near10 key near10	US-PGPUB;	OR	OFF	2016/12/06

		exchang$3	USPAT			18:36
S902	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S903	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S904	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S905	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S906	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S907	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S908	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S909	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S910	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S911	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S912	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S913	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S914	27	S913 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S915	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S916	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S917	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S918	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S919	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S920	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S921	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S922	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S923	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S924	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36

S925	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S926	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S927	27	S926 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S928	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S929	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S930	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S931	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S932	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S933	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S934	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S935	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S936	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S937	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S938	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S939	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S940	27	S939 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S941	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S942	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S943	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S944	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S945	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S946	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S947	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S948	6367	ipsec with (ssl or tls)	US-PGPUB;	OR	OFF	2016/12/06

			USPAT			18:36
S949	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S950	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S951	16	"7882538"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S952	23	"6744741"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S953	42	"7055027"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S954	11	((SAMI) near2 (VAARALA)).INV.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S955	11	((ANTTI) near2 (NUOPPONEN)).INV.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S956	11	S954 or S955	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S957	10	S956 and (secure adj connection).clm.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S958	9	S956 and (secure adj connection with address).clm.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S959	3	S956 and (secure adj connection with intermediate with address).clm.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S960	149692	("6732269" "6718388" "6957346" "6795917")".pn"	US-PGPUB; USPAT; EPO; JPO	OR	ON	2016/12/06 18:36
S961	4	("6732269" "6718388" "6957346" "6795917").pn.	US-PGPUB; USPAT; EPO; JPO	OR	ON	2016/12/06 18:36
S962	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S963	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S964	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S965	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S966	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S967	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S968	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S969	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S970	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S971	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S972	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S973	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36

S974	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S975	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S976	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S977	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S978	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S979	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S980	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S981	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S982	16	"7882538"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S983	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S984	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S985	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S986	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S987	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S988	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S989	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S990	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S991	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S992	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S993	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S994	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S995	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S996	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S997	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S998	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S999	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1000	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36

S1001	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1002	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1003	16	"7882538"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1004	11	S954 or S955	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1005	10	S956 and (secure adj connection).clm.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1006	9	S956 and (secure adj connection with address).clm.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1007	3	S956 and (secure adj connection with intermediate with address).clm.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1008	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1009	27	S845 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1010	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S1011	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1012	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1013	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1014	27	S858 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1015	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S1016	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1017	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1018	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1019	27	S871 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1020	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S1021	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1022	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1023	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36

S1024	27	S884 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1025	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S1026	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1027	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1028	23	"6744741"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1029	42	"7055027"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1030	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1031	27	S900 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1032	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S1033	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1034	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1035	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1036	27	S913 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1037	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S1038	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1039	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1040	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1041	27	S926 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1042	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S1043	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1044	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1045	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36

S1046	27	S939 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1047	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S1048	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1049	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1050	23	"6744741"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1051	42	"7055027"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1052	11	((SAMI) near2 (VAARALA)).INV.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1053	11	((ANTTI) near2 (NUOPPONEN)).INV.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1054	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1055	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1056	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1057	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1058	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1059	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1060	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1061	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1062	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1063	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1064	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1065	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1066	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1067	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36

S1068	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1069	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1070	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1071	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1072	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1073	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1074	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1075	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1076	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1077	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1078	149692	("6732269" "6718388" "6957346" "6795917")".pn"	US-PGPUB; USPAT; EPO; JPO	OR	ON	2016/12/06 18:36
S1079	4	("6732269" "6718388" "6957346" "6795917").pn.	US-PGPUB; USPAT; EPO; JPO	OR	ON	2016/12/06 18:36
S1080	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1081	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1082	27	S1081 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1083	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1084	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1085	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S1086	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1087	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1088	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1089	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1090	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1091	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1092	4519	ipsec near5 (ssl or tls)	US-PGPUB;	OR	OFF	2016/12/06

			USPAT			18:36
S1093	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1094	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1095	27	S1094 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1096	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1097	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1098	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S1099	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1100	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1101	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1102	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1103	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1104	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1105	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1106	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1107	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1108	27	S1107 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1109	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1110	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1111	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S1112	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1113	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1114	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1115	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36

S1116	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1117	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1118	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1119	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1120	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1121	27	S1120 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1122	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1123	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1124	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S1125	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1126	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1127	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1128	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1129	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1130	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1131	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1132	16	"7882538"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1133	23	"6744741"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1134	42	"7055027"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1135	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1136	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1137	27	S1136 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1138	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1139	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1140	3	"US 20060173968"	US-PGPUB; USPAT;	OR	OFF	2016/12/06 18:36

			USOCR; DERWENT			
S1141	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1142	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1143	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1144	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1145	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1146	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1147	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1148	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1149	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1150	27	S1149 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1151	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1152	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1153	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S1154	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1155	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1156	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1157	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1158	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1159	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1160	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1161	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1162	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1163	27	S1162 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1164	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36

S1165	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1166	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S1167	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1168	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1169	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1170	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1171	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1172	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1173	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1174	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1175	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1176	27	S1175 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1177	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1178	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1179	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S1180	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1181	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1182	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1183	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1184	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1185	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1186	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1187	16	"7882538"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1188	23	"6744741"	US-PGPUB;	OR	OFF	2016/12/06

			USPAT			18:36
S1189	42	"7055027"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1190	11	((SAMI) near2 (VAARALA)).INV.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1191	11	((ANTTI) near2 (NUOPPONEN)).INV.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1192	11	S1190 or S1191	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1193	10	S1192 and (secure adj connection).clm.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1194	9	S1192 and (secure adj connection with address).clm.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1195	3	S1192 and (secure adj connection with intermediate with address).clm.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1196	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1197	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1198	27	S1197 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1199	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1200	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1201	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S1202	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1203	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1204	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1205	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1206	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1207	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1208	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1209	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1210	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1211	27	S1210 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1212	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36

S1213	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1214	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S1215	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1216	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1217	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1218	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1219	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1220	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1221	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1222	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1223	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1224	27	S1223 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1225	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1226	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1227	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S1228	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1229	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1230	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1231	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1232	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1233	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1234	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1235	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1236	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB;	OR	OFF	2016/12/06

			USPAT			18:36
S1237	27	S1236 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1238	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1239	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1240	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S1241	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1242	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1243	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1244	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1245	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1246	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1247	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1248	16	"7882538"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1249	23	"6744741"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1250	42	"7055027"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1251	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1252	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1253	27	S1252 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1254	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1255	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1256	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S1257	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1258	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1259	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36

S1260	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1261	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1262	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1263	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1264	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1265	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1266	27	S1265 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1267	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1268	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1269	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S1270	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1271	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1272	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1273	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1274	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1275	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1276	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1277	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1278	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1279	27	S1278 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1280	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1281	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1282	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S1283	19	ipsec same tunnel$3 same IKE same (gateway or proxy or	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36

		intermediate) and cookie				
S1284	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1285	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1286	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1287	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1288	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1289	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1290	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1291	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1292	27	S1291 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1293	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1294	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1295	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S1296	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1297	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1298	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1299	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1300	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1301	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1302	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1303	16	"7882538"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1304	23	"6744741"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1305	42	"7055027"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1306	11	((SAMI) near2 (VAARALA)).INV.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1307	11	((ANTTI) near2 (NUOPPONEN)).INV.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1308	11	S1306 or S1307	US-PGPUB;	OR	OFF	2016/12/06

			USPAT			18:36
S1309	10	S1308 and (secure adj connection).clm.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1310	9	S1308 and (secure adj connection with address).clm.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1311	3	S1308 and (secure adj connection with intermediate with address).clm.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1312	149692	("6732269" "6718388" "6957346" "6795917")".pn"	US-PGPUB; USPAT; EPO; JPO	OR	ON	2016/12/06 18:36
S1313	4	("6732269" "6718388" "6957346" "6795917").pn.	US-PGPUB; USPAT; EPO; JPO	OR	ON	2016/12/06 18:36
S1314	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1315	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1316	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1317	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1318	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1319	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1320	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1321	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1322	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1323	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1324	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1325	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1326	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1327	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1328	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1329	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1330	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1331	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1332	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1333	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36

S1334	16	"7882538"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1335	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1336	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1337	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1338	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1339	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1340	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1341	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1342	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1343	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1344	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1345	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1346	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1347	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1348	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1349	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1350	6882	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1351	7044	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1352	6367	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1353	6367	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1354	4519	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1355	16	"7882538"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1356	11	S1306 or S1307	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1357	10	S1308 and (secure adj connection).clm.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1358	9	S1308 and (secure adj connection with address).clm.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1359	3	S1308 and (secure adj connection with intermediate with address).clm.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1360	2	"20010047487"	US-PGPUB;	OR	OFF	2016/12/06

			USPAT			18:36
S1361	27	S1197 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1362	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S1363	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1364	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1365	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1366	27	S1210 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1367	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S1368	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1369	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1370	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1371	27	S1223 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1372	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S1373	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1374	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1375	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1376	27	S1236 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1377	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S1378	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1379	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1380	23	"6744741"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1381	42	"7055027"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1382	2	"20010047487"	US-PGPUB;	OR	OFF	2016/12/06

			USPAT			18:36
S1383	27	S1252 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1384	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S1385	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1386	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1387	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1388	27	S1265 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1389	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S1390	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1391	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1392	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1393	27	S1278 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1394	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S1395	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1396	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1397	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1398	27	S1291 and secure near10 key near10 exchang$3	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1399	3	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2016/12/06 18:36
S1400	19	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1401	24	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1402	23	"6744741"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1403	42	"7055027"	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1404	11	((SAMI) near2 (VAARALA)).INV.	US-PGPUB;	OR	OFF	2016/12/06

			USPAT			18:36
S1405	11	((ANTTI) near2 (NUOPPONEN)).INV.	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1406	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1407	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1408	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1409	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1410	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1411	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1412	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1413	271	ipsec same tunnel$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1414	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1415	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1416	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1417	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1418	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1419	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1420	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1421	862	ipsec same tunnel$3 same IKE	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1422	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1423	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1424	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1425	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1426	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1427	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36

S1428	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1429	4519	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2016/12/06 18:36
S1430	149692	("6732269" "6718388" "6957346" "6795917")".pn"	US-PGPUB; USPAT; EPO; JPO	OR	ON	2016/12/06 18:36
S1431	4	("6732269" "6718388" "6957346" "6795917").pn.	US-PGPUB; USPAT; EPO; JPO	OR	ON	2016/12/06 18:36
S1432	15	advanced with dns with lookup	US-PGPUB; USPAT; EPO; JPO	OR	ON	2016/12/06 18:36
S1433	5	pre?fetch with dns with lookup	US-PGPUB; USPAT; EPO; JPO	OR	ON	2016/12/06 18:36
S1434	13	pre?fetch$3 with dns with lookup	US-PGPUB; USPAT; EPO; JPO	OR	ON	2016/12/06 18:36
S1435	326	(webpage or website) with block$3 with collect$3	US-PGPUB; USPAT; EPO; JPO	OR	ON	2016/12/06 18:36
S1454	11	((relay intermediate) with encrypt$3 with forward$3 with table)	US-PGPUB; USPAT; EPO; JPO	OR	OFF	2017/03/02 15:45
S1455	1921	((relay intermediate) with forward$3 with table)	US-PGPUB; USPAT; EPO; JPO	OR	OFF	2017/03/02 15:46
S1456	348	((relay intermediate) with forward$3 with table with address)	US-PGPUB; USPAT; EPO; JPO	OR	OFF	2017/03/02 15:46
S1457	36	((relay intermediate) with forward$3 with table with address) and (encrypt$3 with (payload packet frame data))	US-PGPUB; USPAT; EPO; JPO	OR	OFF	2017/03/02 15:50
S1458	23	((relay intermediate) with forward$3 with table with address with secure)	US-PGPUB; USPAT; EPO; JPO	OR	OFF	2017/03/02 15:56
S1459	91	((relay intermediate) with forward$3 with table with address and secure)	US-PGPUB; USPAT; EPO; JPO	OR	OFF	2017/03/02 15:57
S1460	103	((relay intermediate) with forward$3 with table with address and (encrypt$3 secure))	US-PGPUB; USPAT; EPO; JPO	OR	OFF	2017/03/02 15:57
S1461	51	((relay intermediate) with forward$3 with table with address with translat$3)	US-PGPUB; USPAT; EPO; JPO	OR	OFF	2017/03/02 16:01
S1462	2	"20120213261"	US-PGPUB; USPAT; EPO; JPO	OR	OFF	2017/03/06 15:14

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S118	1	(secure adj connection with intermediate with address).clm.	USPAT	OR	OFF	2011/12/28 20:12

S119	13	(secure adj connection with (intermediate or gateway or proxy) with address).clm.	USPAT	OR	OFF	2011/12/28 20:12
S120	1	(secure adj connection with (intermediate or gateway or proxy) with (key or token) with address).clm.	USPAT	OR	OFF	2011/12/28 20:13
S357	1	(secure adj connection with intermediate with address).clm.	USPAT	OR	OFF	2012/08/12 17:25
S358	14	(secure adj connection with (intermediate or gateway or proxy) with address).clm.	USPAT	OR	OFF	2012/08/12 17:25
S359	1	(secure adj connection with (intermediate or gateway or proxy) with (key or token) with address).clm.	USPAT	OR	OFF	2012/08/12 17:25
S360	1	(secure adj connection with intermediate with address).clm.	USPAT	OR	OFF	2012/08/12 17:57
S361	14	(secure adj connection with (intermediate or gateway or proxy) with address).clm.	USPAT	OR	OFF	2012/08/12 17:57
S362	1	(secure adj connection with (intermediate or gateway or proxy) with (key or token) with address).clm.	USPAT	OR	OFF	2012/08/12 17:57
S715	2	(secure adj connection with intermediate with address).clm.	USPAT	OR	OFF	2013/10/08 12:53
S716	16	(secure adj connection with (intermediate or gateway or proxy) with address).clm.	USPAT	OR	OFF	2013/10/08 12:53
S717	3	(secure adj connection with (intermediate or gateway or proxy) with (key or token) with address).clm.	USPAT	OR	OFF	2013/10/08 12:53
S718	2	(secure adj connection with intermediate with address).clm.	USPAT	OR	OFF	2013/10/08 12:53
S719	16	(secure adj connection with (intermediate or gateway or proxy) with address).clm.	USPAT	OR	OFF	2013/10/08 12:53
S720	3	(secure adj connection with (intermediate or gateway or proxy) with (key or token) with address).clm.	USPAT	OR	OFF	2013/10/08 12:53
S721	2	(secure adj connection with intermediate with address).clm.	USPAT	OR	OFF	2013/10/08 12:53
S722	16	(secure adj connection with (intermediate or gateway or proxy) with address).clm.	USPAT	OR	OFF	2013/10/08 12:53
S723	3	(secure adj connection with (intermediate or gateway or proxy) with (key or token) with address).clm.	USPAT	OR	OFF	2013/10/08 12:53
S1436	2	(secure adj connection with intermediate with address).clm.	USPAT	OR	OFF	2016/12/06 18:36
S1437	21	(secure adj connection with (intermediate or gateway or proxy) with address).clm.	USPAT	OR	OFF	2016/12/06 18:36
S1438	3	(secure adj connection with (intermediate or gateway or proxy) with (key or token) with address).clm.	USPAT	OR	OFF	2016/12/06 18:36
S1439	2	(secure adj connection with intermediate with address).clm.	USPAT	OR	OFF	2016/12/06 18:36
S1440	21	(secure adj connection with (intermediate or gateway or proxy) with address).clm.	USPAT	OR	OFF	2016/12/06 18:36
S1441	3	(secure adj connection with (intermediate or gateway or proxy) with (key or token) with address).clm.	USPAT	OR	OFF	2016/12/06 18:36
S1442	2	(secure adj connection with intermediate with	USPAT	OR	OFF	2016/12/06

		address).clm.				18:36
S1443	21	(secure adj connection with (intermediate or gateway or proxy) with address).clm.	USPAT	OR	OFF	2016/12/06 18:36
S1444	3	(secure adj connection with (intermediate or gateway or proxy) with (key or token) with address).clm.	USPAT	OR	OFF	2016/12/06 18:36
S1445	2	(secure adj connection with intermediate with address).clm.	USPAT	OR	OFF	2016/12/06 18:36
S1446	21	(secure adj connection with (intermediate or gateway or proxy) with address).clm.	USPAT	OR	OFF	2016/12/06 18:36
S1447	3	(secure adj connection with (intermediate or gateway or proxy) with (key or token) with address).clm.	USPAT	OR	OFF	2016/12/06 18:36
S1448	2	(secure adj connection with intermediate with address).clm.	USPAT	OR	OFF	2016/12/06 18:36
S1449	21	(secure adj connection with (intermediate or gateway or proxy) with address).clm.	USPAT	OR	OFF	2016/12/06 18:36
S1450	3	(secure adj connection with (intermediate or gateway or proxy) with (key or token) with address).clm.	USPAT	OR	OFF	2016/12/06 18:36
S1451	2	(secure adj connection with intermediate with address).clm.	USPAT	OR	OFF	2016/12/06 18:36
S1452	21	(secure adj connection with (intermediate or gateway or proxy) with address).clm.	USPAT	OR	OFF	2016/12/06 18:36
S1453	3	(secure adj connection with (intermediate or gateway or proxy) with (key or token) with address).clm.	USPAT	OR	OFF	2016/12/06 18:36

3/15/2017 1:48:04 PM
C:\Users\atowfighi\Documents\EAST\Workspaces\jeff930.wsp

UNITED STATES PATENT AND TRADEMARK OFFICE

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

BIB DATA SHEET

CONFIRMATION NO. 6275

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
15/372,208	12/07/2016	713	2469	664.1078CON2

APPLICANTS

MPH Technologies Oy, Espoo, FINLAND;

INVENTORS

Sami Vaarala, Helsinki, FINLAND;
Antti Nuopponen, Espoo, FINLAND;

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

This application is a CON of 13/685,544 11/26/2012
which is a CON of 10/500,930 10/19/2005 PAT 8346949
which is a 371 of PCT/FI03/00045 01/21/2003

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

FINLAND 20020112 01/22/2002

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****

12/15/2016

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	/AFSHAWN M TOWFIGHI/ Examiner's Signature	☐ Initials	FINLAND	6	11	1

ADDRESS

FASTH LAW OFFICES (ROLF FASTH)
1206 Stanridge Drive
Raleigh, NC 27613-7063
UNITED STATES

TITLE

METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION

FILING FEE RECEIVED		
1820	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15372208	VAARALA ET AL.
	Examiner	**Art Unit**
	AFSHAWN TOWFIGHI	2469

CPC							
Symbol						**Type**	**Version**
H04L		63	/	0281		F	2013-01-01
H04L		9	/	0841		I	2013-01-01
H04L		63	/	0428		I	2013-01-01
H04L		63	/	123		I	2013-01-01
H04L		61	/	256		I	2013-01-01
			/				
			/				
			/				
			/				
			/				
			/				
			/				
			/				
			/				
			/				

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

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	11	
/AFSHAWN TOWFIGHI/ Primary Examiner.Art Unit 2469	03/15/2017	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)		11

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15372208	VAARALA ET AL.
	Examiner	**Art Unit**
	AFSHAWN TOWFIGHI	2469

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**
713	171

CROSS REFERENCE(S)					
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**				
709	229				

INTERNATIONAL CLASSIFICATION					
CLAIMED					**NON-CLAIMED**
H	0	4	L	9 / 32 (2006.01.01)	
G	0	6	F	15 / 16 (2006.01.01)	

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	11	
/AFSHAWN TOWFIGHI/ Primary Examiner.Art Unit 2469	03/15/2017	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)		11

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15372208	VAARALA ET AL.
	Examiner	**Art Unit**
	AFSHAWN TOWFIGHI	2469

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

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

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 11	
/AFSHAWN TOWFIGHI/ Primary Examiner.Art Unit 2469 (Primary Examiner)	03/15/2017 (Date)	O.G. Print Claim(s)	O.G. Print Figure 11

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15372208	VAARALA ET AL.
	Examiner	Art Unit
	AFSHAWN TOWFIGHI	2469

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
709	236, 239, 245	3/15/2017	AT

SEARCH NOTES		
Search Notes	Date	Examiner
EAST (USPAT, USPGPUB, EPO, JPO) - see search history printout	3/15/2017	AT
Inventor Search in EAST - see search history printout	3/15/2017	AT
Assignee Search in EAST - see search history printout	3/15/2017	AT

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
	Interference Search - see search history printout	3/15/2017	AT

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15372208	VAARALA ET AL.
	Examiner	Art Unit
	AFSHAWN TOWFIGHI	2469

✓	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	03/15/2017								
1	1	=								
2	2	=								
3	3	=								
4	4	=								
5	5	=								
6	6	=								
7	7	=								
8	8	=								
9	9	=								
10	10	=								
11	11	=								
	12	-								
	13	-								
	14	-								
	15	-								
	16	-								
	17	-								
	18	-								
	19	-								
	20	-								
	21	-								

Doc Code: DIST.E.FILE **Document Description: Electronic Terminal Disclaimer - Filed**	PTO/SB/25 PTO/SB/26 U.S. Patent and Trademark Office Department of Commerce

Electronic Petition Request	**TERMINAL DISCLAIMER TO OBVIATE A PROVISIONAL DOUBLE PATENTING REJECTION OVER A PENDING "REFERENCE" APPLICATION AND TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT**
Application Number	15372208
Filing Date	07-Dec-2016
First Named Inventor	Sami Vaarala
Attorney Docket Number	664.1078CON2
Title of Invention	METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION

☒ Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action

☒ This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.

Owner	Percent Interest
MPH Technologies Oy	100 %

The owner(s) of percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending reference Application Number(s)

13685544 filed on 11/26/2012

as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the reference application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term of any patent granted on said reference application, "as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application," in the event that any such patent granted on the pending reference application: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

The owner(s) with percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of prior patent number(s)

as the term of said prior patent is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the prior patent are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the prior patent, "as the term of said prior patent is presently shortened by any terminal disclaimer," in the event that said prior patent later:
- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

(●) Terminal disclaimer fee under 37 CFR 1.20(d) is included with Electronic Terminal Disclaimer request.

( ) I certify, in accordance with 37 CFR 1.4(d)(4), that the terminal disclaimer fee under 37 CFR 1.20(d) required for this terminal disclaimer has already been paid in the above-identified application.

Applicants claims the following fee status:

( ) Small Entity

( ) Micro Entity

(●) Regular Undiscounted

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.

THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES

I certify, in accordance with 37 CFR 1.4(d)(4) that I am:

(●) An attorney or agent registered to practice before the Patent and Trademark Office who is of record in this application

Registration Number 36999

( ) A sole inventor

( ) A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors as evidenced by the power of attorney in the application

( ) A joint inventor; all of whom are signing this request

Signature	/rfasth/
Name	Rolf Fasth

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

Electronic Patent Application Fee Transmittal

Application Number:	15372208
Filing Date:	07-Dec-2016
Title of Invention:	METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION
First Named Inventor/Applicant Name:	Sami Vaarala
Filer:	Rolf Fasth/Smith Sloan
Attorney Docket Number:	664.1078CON2

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
STATUTORY OR TERMINAL DISCLAIMER	1814	1	160	160
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**160**

Doc Code: DISQ.E.FILE
Document Description: Electronic Terminal Disclaimer – Approved

Application No.: 15372208

Filing Date: 07-Dec-2016

Applicant/Patent under Reexamination: Vaarala

Electronic Terminal Disclaimer filed on March 16, 2017

☒ APPROVED

This patent is subject to a terminal disclaimer

☐ DISAPPROVED

Approved/Disapproved by: Electronic Terminal Disclaimer automatically approved by EFS-Web

U.S. Patent and Trademark Office

Electronic Acknowledgement Receipt

EFS ID:	28645596
Application Number:	15372208
International Application Number:	
Confirmation Number:	6275
Title of Invention:	METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION
First Named Inventor/Applicant Name:	Sami Vaarala
Customer Number:	33369
Filer:	Rolf Fasth/Smith Sloan
Filer Authorized By:	Rolf Fasth
Attorney Docket Number:	664.1078CON2
Receipt Date:	16-MAR-2017
Filing Date:	07-DEC-2016
Time Stamp:	11:04:41
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$160
RAM confirmation Number	031617INTEFSW00010906060243
Deposit Account	060243
Authorized User	Sloan Smith

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

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

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Electronic Terminal Disclaimer-Filed	eTerminal-Disclaimer.pdf	35960 e8e476a0f7f488e3f5042c72ab9ef56402ca70ba	no	3
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30249 a4159daed486f7dba712acde2ccfb3aaa2f6102b	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	66209		

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 ASSIGNMENT COVER SHEET

Electronic Version v1.1
Stylesheet Version v1.2

EPAS ID: PAT4252324

SUBMISSION TYPE:	NEW ASSIGNMENT
NATURE OF CONVEYANCE:	ASSIGNMENT

CONVEYING PARTY DATA

Name	Execution Date
SAMI VAARALA	12/07/2016
ANTTI NUOPPONEN	12/31/2016

RECEIVING PARTY DATA

Name:	MPH TECHNOLOGIES OY
Street Address:	KEILARANTA 1
City:	FI-02150 ESPOO
State/Country:	FINLAND

PROPERTY NUMBERS Total: 1

Property Type	Number
Application Number:	15372208

CORRESPONDENCE DATA

Fax Number:

Correspondence will be sent to the e-mail address first; if that is unsuccessful, it will be sent using a fax number, if provided; if that is unsuccessful, it will be sent via US Mail.

Email: sloan.smith@fasthlaw.com
Correspondent Name: FASTH LAW OFFICES
Address Line 1: 1206 STANRIDGE DRIVE
Address Line 4: RALEIGH, NORTH CAROLINA 27613

ATTORNEY DOCKET NUMBER:	664.1078CON2
NAME OF SUBMITTER:	ROLF FASTH
SIGNATURE:	/rfasth/
DATE SIGNED:	01/31/2017
	This document serves as an Oath/Declaration (37 CFR 1.63).

Total Attachments: 4
source=DECL_ASN#page1.tif
source=DECL_ASN#page2.tif
source=DECL_ASN#page3.tif
source=DECL_ASN#page4.tif

ASSIGNMENT AND INVENTOR'S DECLARATION

WHEREAS, we, Sami Vaarala (Assignor 1) of Neljas Linja 22A, FIN-00503 Helsinki, Finland and Antti Nuopponen (Assignor 2) of Kaksoiskiventie 7-9 A1, FIN-02760 Espoo, Finland have invented a certain invention entitled METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION for which we are making application for Letters Patent of the United States, the specification of which is enclosed herewith; and

WHEREAS, MPH Technologies Oy (Assignee), a corporation organized under the laws of Finland, having an address at Keilaranta 1, FI-02150 Espoo, Finland, is desirous of acquiring the entire interest, title and interest in and to the application and invention, and to any United States patents to be obtained therefor;

NOW, THEREFORE, in consideration of good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, we, Sami Vaarala and Antti Nuopponen, hereby sell, assign and transfer to MPH Technologies Oy, its successors and assigns, the entire right, title and interest in and to said invention, patent application and patent rights in the United States including all rights of priority from the filing of the application; said invention, application and letters patent in the United States, all divisions, continuations, reissues and extensions thereof, including any right to bring or maintain an action for infringement under the provisional rights granted pursuant to Title 35, Section 154 of the United States Code or any other cause of action for acts which would constitute infringement occurring prior to this assignment, and including the right to claim priority under the International Convention

of Paris (1883), as amended, or in any corresponding foreign patent application, and we request the Director of the U.S. Patent and Trademark Office to issue any Letters Patent granted upon the invention set forth in the application to MPH Technologies Oy, its successors and assigns.

As a below named inventor, I hereby declare that this assignment and declaration is directed to the above-identified application having the title shown above. The above-identified application was made or was authorized to be made by me. I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby declare and acknowledge 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._____ _____

Legal name of first joint inventor: Sami Vaarala

Inventor's signature

Date December 7, 2016

Residence: Helsinki, Finland

Citizenship: Finland

Post Office address: Neljas Linja 22A

FIN-00503 Helsinki, Finland

Legal name of second joint inventor: Antti Nuopponen

Inventor's signature _____

Date December 31, 2016

Residence: Espoo, Finland

Citizenship: Finland

Post Office address: Kaksoiskiventie 7-9 A1

FIN-02760 Espoo, Finland

Attorney Ref. No. 664.1078CON2 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Sami Vaarala, Antti Nuopponen

Serial No. 15/372,208

Filed: 7 December 2016

For: METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION

Date: 16 January 2017

Confirmation No. 6275

CERTIFICATE OF MAILING

I HEREBY CERTIFY THAT THIS PAPER AND THE DOCUMENTS REFERRED TO AS BEING ATTACHED OR ENCLOSED HEREWITH ARE BEING FORWARDED TO THE COMMISSIONER FOR PATENTS, UNITED STATES PATENT OFFICE ELECTRONICALLY ON January 16, 2017

/rfasth/
Rolf Fasth
Attorney for Applicant

TRANSMITTAL LETTER

ELECTRONIC SUBMISSION

COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

Enclosed for filing in the above-referenced application are the following:

(X) Inventors' Oath or Declaration
(X) The Commissioner is hereby authorized to charge any additional fees which may be required in connection with the filing of this correspondence, or credit over-payment, to Account No. 06-0243.

Respectfully submitted,

FASTH LAW OFFICES

/rfasth/

Rolf Fasth
Registration No. 36,999

FASTH LAW OFFICES
1206 Stanridge Drive
Raleigh, North Carolina 27613-7063 USA
Tel: +1-910-687-0001
Fax: +1-919-882-1265

Attorney Ref. No. 664.1078CON2

Electronic Acknowledgement Receipt

EFS ID:	28069716
Application Number:	15372208
International Application Number:	
Confirmation Number:	6275
Title of Invention:	METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION
First Named Inventor/Applicant Name:	Sami Vaarala
Customer Number:	33369
Filer:	Rolf Fasth/Sloan Smith
Filer Authorized By:	Rolf Fasth
Attorney Docket Number:	664.1078CON2
Receipt Date:	16-JAN-2017
Filing Date:	07-DEC-2016
Time Stamp:	12:57:52
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Oath or Declaration filed	DECL_ASN.pdf	2604719 0d02ac65edafe919aae4d5975cd459c4237e164a	no	4

Warnings:

Information:					
2	Transmittal Letter	TRX.pdf	236311 9b89b2c943e301588d6fa9385b8cef17e56b229f	no	1
Warnings:					
Information:					
			Total Files Size (in bytes):	2841030	

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.

ASSIGNMENT AND INVENTOR'S DECLARATION

WHEREAS, we, Sami Vaarala (Assignor 1) of Neljas Linja 22A, FIN-00503 Helsinki, Finland and Antti Nuopponen (Assignor 2) of Kaksoiskiventie 7-9 A1, FIN-02760 Espoo, Finland have invented a certain invention entitled METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION for which we are making application for Letters Patent of the United States, the specification of which is enclosed herewith; and

WHEREAS, MPH Technologies Oy (Assignee), a corporation organized under the laws of Finland, having an address at Keilaranta 1, FI-02150 Espoo, Finland, is desirous of acquiring the entire interest, title and interest in and to the application and invention, and to any United States patents to be obtained therefor;

NOW, THEREFORE, in consideration of good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, we, Sami Vaarala and Antti Nuopponen, hereby sell, assign and transfer to MPH Technologies Oy, its successors and assigns, the entire right, title and interest in and to said invention, patent application and patent rights in the United States including all rights of priority from the filing of the application; said invention, application and letters patent in the United States, all divisions, continuations, reissues and extensions thereof, including any right to bring or maintain an action for infringement under the provisional rights granted pursuant to Title 35, Section 154 of the United States Code or any other cause of action for acts which would constitute infringement occurring prior to this assignment, and including the right to claim priority under the International Convention

of Paris (1883), as amended, or in any corresponding foreign patent application, and we request the Director of the U.S. Patent and Trademark Office to issue any Letters Patent granted upon the invention set forth in the application to MPH Technologies Oy, its successors and assigns.

As a below named inventor, I hereby declare that this assignment and declaration is directed to the above-identified application having the title shown above. The above-identified application was made or was authorized to be made by me. I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby declare and acknowledge 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._____ _____

Legal name of first joint inventor: Sami Vaarala

Inventor's signature

Date December 7, 2016

Residence: Helsinki, Finland

Citizenship: Finland

Post Office address: Neljas Linja 22A

FIN-00503 Helsinki, Finland

Legal name of second joint inventor: Antti Nuopponen

Inventor's signature _____

Date December 31, 2016

Residence: Espoo, Finland

Citizenship: Finland

Post Office address: Kaksoiskiventie 7-9 A1

FIN-02760 Espoo, Finland

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 15/372,208

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	280
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	600
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	720
TOTAL CLAIMS (37 CFR 1.16(i))	11 minus 20 =	*			OR	x 80 =	0.00
INDEPENDENT CLAIMS (37 CFR 1.16(h))	1 minus 3 =	*				x 420 =	0.00
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	1600

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
15/372,208	12/07/2016	Sami Vaarala	664.1078CON2

CONFIRMATION NO. 6275

33369
FASTH LAW OFFICES (ROLF FASTH)
1206 Stanridge Drive
Raleigh, NC 27613-7063

INFORMAL NOTICE

OC000000087953099

Date Mailed: 12/19/2016

INFORMATIONAL NOTICE TO APPLICANT

Applicant is notified that the above-identified application contains the deficiencies noted below. No period for reply is set forth in this notice for correction of these deficiencies. However, if a deficiency relates to the inventor's oath or declaration, the applicant must file an oath or declaration in compliance with 37 CFR 1.63, or a substitute statement in compliance with 37 CFR 1.64, executed by or with respect to each actual inventor no later than the expiration of the time period set in the "Notice of Allowability" to avoid abandonment. See 37 CFR 1.53(f).

The item(s) indicated below are also required and should be submitted with any reply to this notice to avoid further processing delays.

- A properly executed inventor's oath or declaration has not been received for the following inventor(s):
  Sami Vaarala
  Antti Nuopponen

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/tle/

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
15/372,208	12/07/2016	2431	1820	664.1078CON2	11	1

CONFIRMATION NO. 6275

33369
FASTH LAW OFFICES (ROLF FASTH)
1206 Stanridge Drive
Raleigh, NC 27613-7063

FILING RECEIPT

OC000000087953098

Date Mailed: 12/19/2016

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

Inventor(s)

Sami Vaarala, Helsinki, FINLAND;
Antti Nuopponen, Espoo, FINLAND;

Applicant(s)

MPH Technologies Oy, Espoo, FINLAND;

Power of Attorney:
Rolf Fasth--36999

Domestic Priority data as claimed by applicant

This application is a CON of 13/685,544 11/26/2012
which is a CON of 10/500,930 10/19/2005 PAT 8346949
which is a 371 of PCT/FI03/00045 01/21/2003

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.)
FINLAND 20020112 01/22/2002 No Access Code Provided

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 12/15/2016

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 15/372,208**

Projected Publication Date: 03/30/2017

Non-Publication Request: No

Early Publication Request: No

Title

METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION

Preliminary Class

726

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

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

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

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

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

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

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

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

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

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

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

NOT GRANTED

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of Art Unit

Sami Vaarala, Antti Nuopponen

Serial No. 15,372,208

Filed: 7 December 2016

For: METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION

Examiner:

Date: 13 December 2016

Attorney Reference No. 664.1078CON2

PRELIMINARY AMENDMENT

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

Preliminary to examination, please amend the above-identified patent application as follows:

In the claims:

Please amend the claims as follows:

1. (Previously presented) An intermediate computer for secure forwarding of messages in a telecommunication network, comprising:

an intermediate computer configured to connect to a telecommunication network;

the intermediate computer configured to be assigned with a first network address in the telecommunication network;

the intermediate computer configured to receive from a mobile computer a secure message sent to the first network address having an encrypted data payload of a message and a unique identity;

the intermediate computer configured to read the unique identity from the secure message sent to the first network address; and

the intermediate computer configured to access a translation table, to find a destination address from the translation table using the unique identity, and

to forward the encrypted data payload to the destination address using a network address of the intermediate computer as a source address of a forwarded message containing the encrypted data payload.

2. (Previously presented) The intermediate computer of claim 1, wherein the intermediate computer is further configured to substitute the unique identity read from the secure message with another unique identity prior to forwarding the encrypted data payload.

3. (Previously presented) The intermediate computer of claim 1, wherein the translation table is stored at the intermediate computer.

4. (Previously presented) The intermediate computer of claim 1, wherein the translation table includes two partitions, the first partition containing information fields related to the connection over which the secure message is sent to the first network address, the second partition containing information fields related to the connection over which the forwarded encrypted data payload is sent to the destination address.

5. (Previously presented) The intermediate computer of claim 1, wherein the intermediate computer is not configured to access cryptographic keys used to encrypt or authenticate the messages.

6. (Previously presented) The intermediate computer of claim 1, wherein the intermediate computer is configured to forward

the encrypted data payload using SSL or TLS protocol.

7. (Previously presented) The intermediate computer of claim 1, wherein the intermediate computer is configured to receive secure messages using SSL or TLS protocol.

8. (Previously presented) The intermediate computer of claim 1, wherein the unique identity read from the secure message includes one or more Security Parameter Index values.

9. (Previously presented) The intermediate computer of claim 1, wherein the intermediate computer is configured to modify the translation table entry address fields in response to a signaling message sent from the mobile computer when the mobile computer changes its address such that the intermediate computer can know that the address of the mobile computer is changed.

10. (Previously presented) The intermediate computer of claim 1, wherein the intermediate computer is a server.

11. (Previously presented) The intermediate computer of claim 1, wherein the source address of the forwarded message is the same as the first network address.

12-21. Canceled

REMARKS

Reconsideration of the application is respectfully requested. Claims 12-21 have been canceled.

The application is submitted to be in condition for allowance, and such action is respectfully requested.

Respectfully submitted,

FASTH LAW OFFICES

/rfasth/

Rolf Fasth
Registration No. 36,999

ATTORNEY REFERENCE NO. 664.1078CON2

FASTH LAW OFFICES
1206 Stanridge Drive
Raleigh, NC 27613-7063

Telephone: (910) 687-0001
Facsimile: (919) 882-1265
Email: rolf.fasth@fasthlaw.com

Attorney Ref. No. 664.1078CON2 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Sami Vaarala, Antti Nuopponen

Serial No. 15/372,208

Filed: 7 December 2016

For: METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION

Date: 13 December 2016

Confirmation No. 6275

CERTIFICATE OF MAILING

I HEREBY CERTIFY THAT THIS PAPER AND THE DOCUMENTS REFERRED TO AS BEING ATTACHED OR ENCLOSED HEREWITH ARE BEING FORWARDED TO THE COMMISSIONER FOR PATENTS, UNITED STATES PATENT OFFICE ELECTRONICALLY ON December 13, 2016

/rfasth/
Rolf Fasth
Attorney for Applicant

TRANSMITTAL LETTER

ELECTRONIC SUBMISSION

COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

Enclosed for filing in the above-referenced application are the following:

(X) Preliminary Amendment
(X) The Commissioner is hereby authorized to charge any additional fees which may be required in connection with the filing of this correspondence, or credit over-payment, to Account No. 06-0243.

Respectfully submitted,

FASTH LAW OFFICES

/rfasth/

Rolf Fasth
Registration No. 36,999

FASTH LAW OFFICES
1206 Stanridge Drive
Raleigh, North Carolina 27613-7063 USA
Tel: +1-910-687-0001
Fax: +1-919-882-1265

Attorney Ref. No. 664.1078CON2

Electronic Acknowledgement Receipt

EFS ID:	27777283
Application Number:	15372208
International Application Number:	
Confirmation Number:	6275
Title of Invention:	METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION
First Named Inventor/Applicant Name:	Sami Vaarala
Customer Number:	33369
Filer:	Rolf Fasth/Sloan Smith
Filer Authorized By:	Rolf Fasth
Attorney Docket Number:	664.1078CON2
Receipt Date:	13-DEC-2016
Filing Date:	
Time Stamp:	14:04:46
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	Preliminary Amendment	PRELIM_AMD.pdf	597192 030ece7efc3802999a7a8b4d8482b447d50e5672	no	5

Warnings:

Information:					
2	Miscellaneous Incoming Letter	TRX.pdf	235591 3fc499d77984eb0c557e910e5c12677745e9a4aa	no	1
Warnings:					
Information:					
			Total Files Size (in bytes):	832783	

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

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 15/372,208	Filing Date 12/07/2016	☐ 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 **12/13/2016**

	(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))	* 11	Minus	** 20	= 0	X $80 =	0
Independent (37 CFR 1.16(h))	* 1	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.

LDRC
ANDREW JAMES JR

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	Filing Date	☐ To be Mailed
15/372,208	12/07/2016	

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

12/13/2016	(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))	* 11	Minus	** 20	= 0	X $80 =	0
Independent (37 CFR 1.16(h))	* 1	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.

LDRC
ANDREW JAMES JR

Attorney Ref. No. 664.1078CON2 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Sami Vaarala, Antti Nuopponen

Serial No. 15/372,208

Filed: 7 December 2016

For: METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION

Date: 8 December 2016

Confirmation No. 6275

CERTIFICATE OF MAILING

I HEREBY CERTIFY THAT THIS PAPER AND THE DOCUMENTS REFERRED TO AS BEING ATTACHED OR ENCLOSED HEREWITH ARE BEING FORWARDED TO THE COMMISSIONER FOR PATENTS, UNITED STATES PATENT OFFICE ELECTRONICALLY ON December 8, 2016

/rfasth/
Rolf Fasth
Attorney for Applicant

TRANSMITTAL LETTER

ELECTRONIC SUBMISSION

COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

Enclosed for filing in the above-referenced application are the following:

(X) Marked-up copy of Specification
(X) The Commissioner is hereby authorized to charge any additional fees which may be required in connection with the filing of this correspondence, or credit over-payment, to Account No. 06-0243.

Respectfully submitted,

FASTH LAW OFFICES

/rfasth/

Rolf Fasth
Registration No. 36,999

FASTH LAW OFFICES
1206 Stanridge Drive
Raleigh, North Carolina 27613-7063 USA
Tel: +1-910-687-0001
Fax: +1-919-882-1265

Attorney Ref. No. 664.1078CON2

METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION

PRIOR APPLICATIONS

This application is a U.S. Continuation Patent Application based on U.S. Continuation Patent Application No. 13/685,544, filed 26 November 2012 that claims priority from US Patent Application Serial No. 10/500,930, filed 19 October 2005, which claims priority from PCT/FI03/00045, filed 21 January 2003, that claims priority from Finnish Pat. App. No. 20020112, filed 22 Jan 2002.

TECHNICAL FIELD

The method and system of the invention are intended to secure connections in telecommunication networks. Especially, it is meant for wireless Internet Service Provider (ISP) connections.

TECHNICAL BACKGROUND

An internetwork is a collection of individual networks connected with intermediate networking devices that function as a single large network. Different networks can be interconnected by routers and other networking devices to create an internetwork.

A local area network (LAN) is a data network that covers a relatively small geographic area. It typically connects workstations, personal computers, printers and other devices. A wide area network (WAN) is a data communication network that covers a relatively broad geographic area. Wide area networks (WANS) interconnect LANs across normal telephone lines and, for instance, optical networks; thereby interconnecting geographically disposed users.

There is a need to protect data and resources from disclosure, to guarantee the authenticity of data, and to protect systems from network based attacks. More in detail, there is a need for confidentiality (protecting the contents of data from being read) integrity (protecting the data from being modified, which is a property that is independent of confidentiality), authentication (obtaining assurance about she actual sender of data), replay protection (guaranteeing that data is fresh, and not a copy of previously sent data), identity protection (keeping the identities of parties exchanging data secret from outsiders), high availability, i.e. denial-of-service protection (ensuring that the system functions even when under attack) and access control. IPSec is a technology providing most of these, but not all of them. (In

particulars identity protection is not completely handled by IPSec, and neither is denial-of-service protection.)

The IP security protocols (IPSec) provides the capability to secure communications between arbitrary hosts, e.g. across a LAN, across private and public wide area networks (WANs) and across the internet IPSec can be used in different ways, such as for building secure virtual private networks, to gain a secure access to a company network, or to secure communication with other organisations, ensuring authentication and confidentiality and providing a key exchange mechanism. IPSec ensures confidentiality integrity, authentication, replay protection, limited traffic flow confidentiality, limited identity protection, and access control based on authenticated identities. Even if some applications already have built in security protocols, the use of IPSec further enhances the security.

IPSec can encrypt and/or authenticate traffic at IP level. Traffic going in to a WAN is typically compressed and encrypted and traffic coming from a WAN is decrypted and decompressed. IPSec is defined by certain documents, which contain rules for the IPSec architecture. The documents that define IPSec, are, for the time being, the Request For

Comments (RFC) series of the Internet Engineering Task Force (IETF), in particular, RFCs 2401-2412.

Two protocols are used to provide security at the IP layer; an authentication protocol designated by the header of the protocol, Authentication Header (AH), and a combined encryption/authentication protocol designated by the format of the packet for that protocol, Encapsulating Security Payload (ESP) AH and ESP are however similar protocols, both operating by adding a protocol header. Both AH and ESP are vehicles for access control based on the distribution of cryptographic keys and the management of traffic flows related to these security protocols.

Security association (SA) is a key concept in the authentication and the confidentiality mechanisms for IP. A security association is a one-way relationship between a sender and a receiver that offers security services to the traffic carried on it if a secure two-way relationship is needed, then two security associations are required. If ESP and AH are combined, or if ESP and/or AH are applied more than once, the term SA bundle is used, meaning that two or more SAs are used. Thus, SA bundle refers to one or more SAs applied in sequence, e.g. by first performing an ESP

protection, and then an AH protection. The SA bundle is the combination of all SAs used to secure a packet.

The term IPsec connection is used in what follows in place of an IPSec bundle of one or more security associations, or a pair of IPSec bundles—one bundle for each direction—of one or more security associations. This term thus covers both unidirectional and bi-directional traffic protection. There is no implication of symmetry of the directions, i.e., the algorithms and IPSec transforms used for each direction may be different.

A security association is uniquely identified by three parameters. The first one, the Security Parameters Index (SPI), is a bit string assigned to this SA The SPI is carried in AH and ESP headers to enable the receiving system to select the SA under which a received packet will be processed. IP destination address is the second parameter, which is the address of the destination end point of the SA, which may be an end user system or a network system such as a firewall or a router. The third parameter, the security protocol identifier indicates whether the association is an AH or ESP security association.

In each IPSec implementation, there is a nominal security association data base (SADB) that defines the parameters associated with each SA. A security association is normally defined by the following parameters. The Sequence Number Counter is a 32-bit value used to generate the sequence number field in AH or ESP headers. The Sequence Counter Overflow is a flag indicating whether overflow of the sequence number counter should generate an auditable event and prevent further transmission of packets on this SA. An Anti-Replay Window is used to determine whether an inbound AH or ESP packet is a replay. AH information involves information about the authentication algorithm, keys and related parameters being used with AH. ESP information involves information of encryption and authentication algorithms, keys, initialisation vectors, and related parameters being used with IPSec. AH information consists of the authentication algorithm, keys and related parameters being used with AH. ESP information consists of encryption and authentication algorithms, keys, cryptographic initialisation vectors and related parameters being used with ESP. The sixth parameter, Lifetime of this Security Association, is a time-interval and/or byte-count after which this SA must be replaced with a new SA (and new SPI) or terminated plus an indication of which of these

actions should occur. IPSec Protocol Mode is either tunnel or transport mode. Maximum Transfer Unit (MTU), an optional feature, defines the maximum size of a packet that can be transmitted without fragmentation. Optionally an MTU discovery protocol may be used to determine the actual MTU for a given route, however, such a protocol is optional.

Both AH and ESP support two modes used, transport and tunnel mode.

Transport mode provides protection primarily for upper layer protocols and extends to the payload of an IP packet Typically, transport mode is used for end-to-end communication between two hosts. Transport mode may be used in conjunction with a tunnelling protocol, other than IPSec tunnelling, to provide a tunnelling capability.

Tunnel mode provides protection to the entire IP packet and is usually used for sending messages through more than two components, although tunnel mode may also be used for end-to-end communication between two hosts. Tunnel mode is often used when one or both ends of a SA is a security gateway, such as a firewall or a router that implements IPSec. With tunnel mode, a number of hosts on networks behind firewalls may engage in secure communications

without implementing IPSec. The unprotected packets generated by such hosts are tunnelled through external networks by tunnel mode SAs set up by the IPSec software in the firewall or secure router at boundary of the local network.

To achieve this, after the AH or ESP fields are added to the IP packet, the entire packet plus security fields are treated as the payload of a new outer IP packet with a new outer IP header. The entire original, or inner, packet travels through a tunnel from one point of an IP network to another: no routers along the way are able to examine the inner IP packet. Because the original packet is encapsulated, the new larger packet may have totally different source and destination addresses, adding to the security. In other words, the first step in protecting the packet using tunnel mode is to add a new IP header to the packet; thus the "IP|payload" packet becomes "IP|IP|payload". The next step is to secure the packet using ESP and/or AH. In case of ESP, the resulting packet is "IP|ESP|IP|payload". The whole inner packet is covered by the ESP and/or AH protection. AH also protects parts of the outer header, in addition to the whole inner packet.

The IPSec tunnel mode operates e.g. in such a way that if a host on a network generates an IP packet with a destination address of another host on another network, the packet is routed from the originating host to a security gateway (SGW), firewall or other secure router at the boundary of the first network. The SGW or the like filters all outgoing packets to determine the need for IPSec processing. If this packet from the first host to another host requires IPSec, the firewall performs IPSec processing and encapsulates the packet in an outer IP header. The source IP address of this outer IP header is this firewall and the destination address may be a firewall that forms the boundary to the other local network. This packet is now routed to the other host's firewall with intermediate routers examining only the outer IP header At the other host firewall, the outer IP header is stripped off and the inner packet is delivered to the other host.

ESP in tunnel mode encrypts and optionally authenticates the entire inner IP packet, including the inner IP header AH in tunnel mode authenticates the entire inner IP packet, including the inner IP header, and selected portions of the outer IP header.

The key management portion of IPSec involves the determination and distribution of secret keys. The default automated key management protocol for IPSec is referred to as ISAKMP/Oakley and consists of the Oakley key determination protocol and Internet Security Association and Key Management Protocol (ISAKMP). Internet key exchange (IKE) is a newer name for the ISAKMP/Oakley protocol. IKE is based on the Diffie-Hellman algorithm and supports RSA signature authentication among other modes. IKE is an extensible protocol, and allows future and vendor-specific features to be added without compromising functionality.

IPSec has been designed to provide confidentiality, integrity, and replay protection for IP packets. However, IPSec is intended to work with static network topology, where hosts are fixed to certain subnetworks. For instance, when an IPSec tunnel has been formed by using Internet Key Exchange (IKE) protocol, the tunnel endpoints are fixed and remain constant. If IPSec is used with a mobile host, the IKE key exchange will have to be redone from every new visited network. This is problematic, because IKE key exchanges involve computationally expensive Diffie-Hellman key exchange algorithm calculations and possibly RSA calculations. Furthermore, the key exchange requires at

least three round trips (six messages) if using the IKE aggressive mode followed by IKE quick mode, and nine messages if using IKE main mode followed by IKE quick mode. This may be a big problem in high latency networks, such as General Packet Radio Service (GPRS) regardless of the computational expenses.

In this text, the term mobility and mobile terminal does not only mean physical mobility, instead the term mobility is in the first hand meant moving from one network to another, which can be performed by a physically fixed terminal as well.

The problem with standard IPSec is thus that it has been designed for static connections. For instance, the end points of an IPSec tunnel mode SA are fixed. There is also no method for changing any of the parameters of an SA, other than by establishing a new SA that replaces the previous one. However, establishing SAs is costly in terms of both computation time and network latency.

An example of a specific scenario where these problems occur is described next in order to illustrate the problem.

In the scenario, there is a standard IPSec security gateway, which is used by a mobile terminal e.g. for remote

access. The mobile terminal is mobile in the sense that it changes its network point of attachment frequently. A mobile terminal can in this text thus be physically fixed or mobile. Because it may be connected to networks administered by third parties, it may also have a point of attachment that uses private addresses—i.e., the network is behind a router that performs network address translation (NAT). In addition, the networks used by the mobile terminal for access may be wireless, and may have poor quality of service in terms of throughput and e.g. packet drop rate.

Standard IPSec does not work well in the scenario. Since IPSec connections are bound to fixed addresses, the mobile terminal must establish a new IPSec connection from each point of attachment. If an automated key exchange protocol, such as IKE, is used, setting up a new IPsec connection is costly in terms of computation and network latency, and may require a manual authentication phase (for instance, a one-time password). If IPSec connections are set up manually, there is considerable manual work involved in configuring the IPSec connection parameters.

Standard IPSec does e.g. not work through NAT devices at the moment. A standard IPSec NAT traversal protocol is

currently being specified, but the security gateway in the scenario might not support an IPSec protocol extended in this way. Furthermore, the current IPSec NAT traversal protocols are not well suited to mobility.

There are no provisions for improving quality of service over wireless links in the standard IPSec protocol. If the access network suffers from high packet drop rates, the applications running in the mobile host and a host that the mobile terminal is communicating with will suffer from packet drops.

A known method of solving some of these problems is based on having an intermediate host between the mobile terminal and the IPSec security gateway. The intermediate host might be a Mobile IP home agent, that provides mobility for the connection between the mobile terminal and the home agent, while the connection from the mobile node to the security gateway is an ordinary IPSec connection. In this case, packets sent by an application in the mobile client are first processed by IPSec, and then by Mobile IP.

In the general case, this implies both Mobile IP and IPSec header fields for packets exchanged by the mobile terminal and the home agent. The Mobile IP headers are removed by

the home agent prior to delivering packets to the security gateway, and added when delivering packets to the mobile terminal. Because of the use of two tunnelling protocols (Mobile IP and IPSec tunnelling), the solution is referred to as "double tunnelling" in this document.

The above method solves the mobility problem, at the cost of adding extra headers to packets. This may have a significant impact on networks that have low throughput such as the General Packet Radio System (GPRS).

Another known method is again to use an intermediate host between the mobile client and the IPSec security gateway. The intermediate host has an IPSec implementation that may support NAT traversal, and possibly some proprietary extensions for improving quality of service of the access network, for instance.

The mobile host would now establish an IPSec connection between itself and the intermediate host, and would also establish an IPSec connection between itself and the IPSec security gateway. This solution is similar to the first known method, except that two IPSec tunnels are used. It solves a different set of problems—for instance, NAT

traversal—but also adds packet size overhead because of double IPsec tunnelling.

A third known method is to use a similar intermediate host as in the second known method, but establish an IPSec connection between the mobile terminal and the intermediate host, and another, separate IPSec connection between the intermediate host and the security gateway. The IPSec connection between the mobile terminal and the intermediate host may support NAT traversal, for instance, while the second IPSec connection does not need to.

When packets are sent by an application in the mobile terminal, the packets are IPSec-processed using the IPSec connection shared by the mobile terminal and the intermediate host. Upon receiving these packets, the intermediate host undoes the IPSec-processing. For instance, if the packet was encrypted, the intermediate host decrypts the packet. The original packet would now be revealed in plaintext to the intermediate host. After this, the intermediate host IPSec-processes the packet using the IPSec connection shared by the intermediate host and the security gateway, and forwards the packet to the security gateway.

This solution allows the use of an IPSec implementation that support NAT traversal, and possibly a number of other (possibly vendor specific) improvements, addressing problems such as the access network quality of service variations. Regardless of these added features, the IPSec security gateway remains unaware of the improvements, and is not required to implement any of the protocols involved in improving service. However, the solution has a major drawback: the IPsec packets are decrypted in the intermediate host, and thus possibly sensitive data is unprotected in the intermediate host.

Consider a business scenario where a single intermediate host provides improved service to a number of separate customer networks, each having its own standard IPSec security gateway. Having decrypted packets of various customer networks in plaintext form in the intermediate host is clearly a major security problem.

To summarise, the known solutions either employ extra tunnelling, causing extra packet size overhead, or use separate tunnels, causing potential security problems in the intermediate host(s) that terminate such tunnels.

THE OBJECT OF THE INVENTION

The object of the invention is to develop a method for forwarding secure messages between two computers, especially, via an intermediate computer by avoiding the above mentioned disadvantages.

Especially, the object of the invention is to forward secure messages in a way that enables changes to be made in the secure connection

SUMMARY OF THE INVENTION

The method and system of the invention enable secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network. It is mainly characterized in that a message is formed in the first computer or in a computer that is served by the first computer, and in the latter case, sending the message to the first computer. In the first computer, a secure message is then formed by giving the message a unique identity and a destination address. The message is sent from the first computer to the intermediate computer, whereafter said destination address and the unique identity are used to find an address to the second computer. The current destination address is substituted with the found address to the second computer,

and the unique identity is substituted with another unique identity. Then the message is forwarded to the second computer.

Preferably, the first computer processes the formed message using a security protocol and encapsulates the message at least in an outer IP header. The outer IP header source address is the current address of the first computer, while the destination address is that of the intermediate computer. The message is then sent to the intermediate computer, which matches the outer IP header address fields together with a unique identifier used by the security protocol, and performs a translation of the outer addresses and the unique identity used by the security protocol. The translated packet is then sent to the second computer, which processes it using the standard security protocol in question. In the method of the invention, there is no extra encapsulation overhead as in the prior art methods. Also, the intermediate computer does not need to undo the security processing, e.g. decryption, and thus does not compromise security as in the prior art methods.

Corresponding steps are performed when the messages are sent in the reverse direction, i.e. from the second computer to the first computer.

Preferably, the secure message is formed by making use of the IPSec protocols, whereby the secure message is formed by using an IPsec connection between the first computer and the intermediate computer. The message sent from the first computer contains message data, an inner IP header containing actual sender and receiver addresses, an outer IP header containing the addresses of the first computer and the intermediate computer, a unique identity, and other security parameters. The unique identity is one or more SPI values and the other security parameters contain e.g. the IPsec sequence number(s). The number of SPI values depends on the SA bundle size (e.g. ESP+AH bundle would have two SPI values). In the following, when an SA is referred to, the same applies to an SA bundle. The other related security parameters, containing e.g. the algorithm to be used, a traffic description, and the lifetime of the SA, are not sent on the wire. Only SPI and sequence number are sent for each IPsec processed header (one SPI and one sequence number if e.g. ESP only is used; two SPIs and two sequence numbers if e.g. ESP+AH is used, etc.).

Thus, the unsecured data packet message is formed by the sending computer, which may or may not be the first computer. The IP header of this packet has IP source and

destination address fields (among other things). The packet is encapsulated e.g. wrapped inside a tunnel, and the resulting packet is secured. The secured packet has a new outer IP header, which contains another set of IP source and destination addresses (in the outer header—the inner header is untouched), i.e. there are two outer addresses (source and destination) and two inner addresses. The processed packet has a unique identity, the IPsec SPI value(s).

An essential idea of the invention is to use the standard protocol (IPSec) between the intermediate computer and the second computer and an "enhanced IPSec protocol" between the first computer and the intermediate computer. IPsec-protected packets are translated by the intermediate computer, without undoing the IPsec processing. This avoids both the overhead of double tunneling and the security problem involved in using separate tunnels.

The translation is performed e.g. by means of a translation table stored at the intermediate computer. The outer IP header address fields and/or the SPI-values are changed by the intermediate computer so that the message can be forwarded to the second computer.

By modifying the translation table and parameters associated to a given translation table entry, the properties of the connection between the first and the intermediate computers can be changed without establishing a new IPsec connection, or involving the second computer in any way.

One example of a change in the SA between the first computer and the intermediate computer is the change of addresses for enabling mobility. This can be accomplished in the invention simply by modifying the translation table entry address fields. Signaling messages may be used to request such a change. Such signalling messages may be authenticated and/or encrypted, or sent in plaintext. One method of doing authentication and/or encryption is to use an IPsec connection between the first computer and the intermediate computer. The second computer is unaware of this IPsec connection, and does not need to participate in the signalling protocol in any way. Several other methods of signalling exist, for instance, the IKE key exchange protocol maybe extended to carry such signalling messages.

In the signalling, e.g. a registration request is sent from the first computer to the intermediate computer which causes the intermediate computer to modify the addresses in

the mapping table and thus, the intermediate computer can identify the mobile next time a message is sent. Preferably, as a result of a registration request, a reply registration is sent from the intermediate computer back to the first computer.

Other examples of possible modifications to the SA—or in general, the packet processing behaviour—between the first computer and the intermediate computer are the following.

One example is the first computer and the intermediate computer performs some sort of retransmission protocol that ensures that the IPSec protected packets are not dropped in the route between the first and the intermediate computer. This may have useful applications when the first computer is connected using a network access method that has a high packet drop rate—for instance, GPRS.

Such a protocol can be easily based on e.g. IPsec sequence number field and the replay protection window, which provide a way to detect that packet(s) have been lost. When a receiving host detects missing packets, it can send a request message for those particular packets. The request can of course be piggy-backed on an existing data packet that is being sent to the other host. Another method of

doing the retransmissions may be based on using an extra protocol inside which the IPSec packets are wrapped for transmission between the first and intermediate computer. In any case, the second computer remains unaware of such a retransmission protocol.

Another example is performing a Network Address Translation (NAT) traversal encapsulation between the first and the intermediate computer. This method could be based on e.g. using UDP encapsulation for transmission of packets between the first and the intermediate computer. The second computer remains unaware about this processing and does not even need to support NAT traversal at all. This is beneficial because there are several existing IPSec products that have no support for NAT traversal.

The system of the invention is a telecommunication network for secure forwarding of messages and comprises at least a first computer, a second computer and an intermediate computer. It is characterized in that the first and the second computers have means to perform IPSec processing, and the intermediate computer have means to perform IPSec translation and possibly key exchange protocol, such as IKE, translation, preferably by means of mapping tables. The intermediate computer may perform IPSec processing

related to other features, such as mobility signalling described above or other enhancements.

The IPSec translation method is independent of the key exchange translation method. Also manual keying can be used instead of automatic keying. If automatic keying is used, any key exchange protocol can be modified for that purpose; however, the idea is to keep the second computer unaware of the interplay of the first and the intermediate computer.

An automatic key exchange protocol may be used in the invention in several ways. The essential idea is that the second computer sees a standard key exchange protocol run, while the first and the intermediate computer perform a modified key exchange. The modified key exchange protocol used between the first and the intermediate computer ensures that the IPsec translation table and other parameters required by the invention are set up as a side-effect of the key exchange protocol. One such modified protocol is presented in the application for the IKE key exchange protocol.

Each translation table consists of entries that are divided into two partitions. The first partition contains information fields related to the connection between the

first computer and the intermediate computer, while the second partition contains information fields related to the connection between the intermediate computer and the second computer.

The translation occurs by identifying the translation table entry by comparing against one partition, and mapping into the other. For traffic that is flowing from the first computer towards the second computer, through the intermediate computer, the entry is found by comparing the received packet against entries in the first partition, and then translating said fields using information found in the second partition of the same entry. For traffic flowing in the opposite direction, the second partition is used for finding the proper translation table entry, and the first partition for translating the packet fields.

The IPSec translation table partitions consist of the following information: the IP local address and the IP remote address (tunnel endpoint addresses) and SPIs for sending and receiving data.

As mentioned, a translation table entry consists of two such partitions, one for communication between first computer and the intermediate computer, and another for

communication between the intermediate computer and the second computer.

The invention described solves the above problems of prior art. The solution is based on giving the first computer, e.g. if it is mobile, an appearance of a standard computer for the second computer. Thus, the second computer will believe it is talking to a standard IPSec host, while the intermediate computer and the second computer will work together using a modified protocol, for instance a slightly modified IPSec and IKE that helps to accomplish this goal. There are, however, several other control protocols that could conceivably be used between the first and the intermediate computer.

In the following, the invention is described more in detail by using figures by means of some embodiment examples to carry out the invention. The invention is not restricted to the details of the figures and accompanying text, or any existing protocols, such as the currently standardised IPSec or IKE.

Especially, the invention can be concerned with other kinds of telecommunication networks wherein the method of the invention can be applied than that of the figures.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates an example of a telecommunication network of the invention.

FIG. 2 describes generally an example of the method of the invention.

FIG. 3 illustrates an example of an IPSec translation table used by the intermediate computer to change the outer IP address and SPI value.

FIG. 4 describes a detailed example of how the SA is formed in the invention.

FIG. 5 illustrates an example of translation tables for the modified key exchange of the invention.

FIG. 6 shows a mapping table for identification values of the user Security Gateway (SGW) addresses.

DETAILED DESCRIPTION OF THE INVENTION

An example of a telecommunication network of the invention is illustrated in FIG. 1, comprising a first computer, here a client computer **1** served by an intermediate computer,

here as a server **2**, and a host computer **4**, that is served by the second computer, here a security gateway (SGW) **3**. The security gateway supports the standard IPSec protocol and optionally the IKE key exchange protocol. The client computer and the server computer support a modified IPSec and IKE protocol.

The invention is not restricted to the topology of FIG. 1. In other embodiments, the first computer may e.g. be a router; or there might e.g. not be a host behind the second computer (in which case the first and the second computer are talking to each other directly), etc.

The IPSec translations taking place in the scenario of FIGS. 1, 2, and **3** are discussed first. The IPSec connections (such as SAs) in the scenario may be established manually, or using some key exchange protocol, such as the Internet Key Exchange (IKE). To illustrate how a key exchange protocol would be used in the scenario of FIG. 1, a modified IKE protocol based on IKE translation is also presented later.

In the invention, an IPSec connection is shared by the first computer and the second computer, while the intermediate computer holds information required to perform

address and IPSec SPI translations for the packets. These translations accomplish the effect of "double tunnelling" (described in the technical background section), but with the method of the invention the confidentiality of the packets is not compromised, while simultaneously having no extra overhead when compared to standard IPSec. The intermediate computer does not know the cryptographic keys used to encrypt and/or authenticate the packets, and can thus not reveal their contents.

The advantage of the invention is that the logical IPSec connection shared by the first and the second computer can be enhanced by the first and the intermediate computer without involvement of the second computer. In particular the so-called "ingress filtering" performed by some routers does not pose any problems when translations of addresses are used. In the example presented, each host also manages its own IPSec SPI space independently.

In the example of FIG. 1, an IPSec connection is formed between the client computer **1** (the first computer) and the security gateway **3** (the second computer). To create an IPSec tunnel, a SA (or usually a SA bundle) is formed between the respective computers with a preceding key exchange. The key exchange between the first and the second

computer can take place manually or it can be performed with an automatic key exchange protocol such as the IKE protocol. For performing said key exchange, a standard IKE protocol is used between the server **2** and the security gateway **3**, and a modified IKE protocol is used between the client computer **1** and the server **2**. An example of a modified IKE protocol that can be used in the invention is described in connection with FIG. 4.

Messages to be sent to the host terminal **4** from the client computer **1** are first sent to the server **2**, wherein an IPSec translation and an IKE translation takes place. After that the message can be sent to the security gateway **3**, which sends the message further in plain text to the host terminal **4**.

The method of the invention, wherein messages in packet form are sent by routing to the end destination, is generally described in connection with FIG. 2. It is assumed in the following description that the IPSec connection between the first and second computer already is formed. The IPSec connection can be set up manually or automatically by e.g. an IKE exchange protocol which is described later.

FIG. 2 illustrates the sequence of events that take place when the first computer, corresponding to the mobile terminal in FIG. 1, sends a packet to a destination host, labelled X in the figure, and when the host X sends a packet to the mobile terminal.

IP packets consist of different parts, such as a data payload and protocol headers. The protocol headers in turn consist of fields.

In step **1** of FIG. 2, the first computer, e.g. a mobile terminal, forms an IP packet that is to be sent to host X. Typically, this packet is created by an application running on the mobile terminal. The IP packet source address is the address of the mobile terminal, while the destination address is host X.

The packet is processed using an IPSec tunnel mode SA, which encapsulates the IP packet securely. The example assumes that IPSec encryption and/or authentication of ESP type is used for processing the-packet, although the invention is not limited to the use of only ESP; instead, an arbitrary IPsec connection may be used.

In said processing, a new IP header is constructed for the packet, with so-called outer IP addresses. The outer source

address of the packet can be the same as the inner IP address—i.e., the address of the mobile terminal—but can be different, if the mobile terminal is visiting a network. The outer source address corresponds to the care of address obtained by the mobile terminal from the visited network, in this case. The outer destination address is the address of the intermediate computer. In addition to the new IP header, an ESP header is added, when using IPSec ESP mode. The SPI field of the ESP header added by the IPSec processing is set to the SPI value that the intermediate computer uses for receiving packets from the mobile terminal. In general, there may be more than one SPI field in a packet.

The processing of packets in the intermediate computer is based on a translation table i.e. an IPSec translation table shown in FIG. 3. The table has been divided into two partitions. The left one, identified by the prefix "c-", refers to the network connection between the first computer (host **1** in FIG. 1) and the intermediate computer (host **2** in FIG. 1). The right one, identified by the prefix "s-", refers to the network connection between the intermediate computer and the second computer (computer **3** in FIG. 1). The postfix number ("-1", "-2", or "-3") identifies the

host in question. Thus, the address fields ("addr") refer to outer addresses of a packet, while the SPI fields ("SPI") refer to the receiver of packets, which packets were sent with this SPI. Thus, "c-SPI-2" is the SPI value used by host **2** (the intermediate computer) when receiving packets from host **1** (the first computer), and the SPI-value "c-SPI-1" is the SPI-value with which the first computer receives messages and the SPI-value with which the intermediate computer sends messages to the first computer and so on.

In terms of FIG. 3, the outer source address would be "c-addr-1" (195.1.2.3), the outer destination address "c-addr-2" (212.90.65.1), while the SPI field would be "c-SPI-2" (0×12341234). The notation 0×NNNNNNNN indicates a 32-bit unsigned integer value, encoded using a hexadecimal notation (base **16**). The inner source address is processed by IPSec in the first computer, and would typically be encrypted. In this example, the inner source address would be the static address of the mobile terminal, e.g. 10.0.0.1.

When the intermediate computer receives the packet sent in step **1** described above, it performs an address and SPI translation, ensuring that the security gateway (host **3** of

FIG. 1) can accept the packet. Most of the packet is secured using IPSec, and since the intermediate computer does not have the cryptographic keys to undo the IPSec processing done by the mobile terminal, it cannot decrypt any encrypted portions of the packet but is able to use the outer IP addresses and the incoming SPI value to determine how to modify the outer address and the SPI to suite the second computer, which is the next destination. SPI is now changed to 0×56785678 in the intermediate computer and the address is changed to the address of the second computer. This is done by means of the IPSec translation table of FIG. 3.

The first row of FIG. 3 is a row that the intermediate computer has found that matches the packet in the example, and thus the intermediate computer chooses it for translation. The new outer source address s-addr-**2** (212.90.65.1) is substituted for the outer source address c-addr-**1** (195.1.2.3), and the new outer destination address s-addr-**3** (103.6.5.4) is substituted for the outer destination address c-addr-**2** (212.90.65.1). The new SPI value, s-SPI-**3** (0×56785678), is substituted for the SPI value c-SPI-**2** (0×12341234). If more than one SPI values are used, all the SPI values are substituted similarly. In the

example, s-addr-**2** and c-addr-**2** happen to be the same on both partitions of the table. This is not necessarily so but the intermediate computer might use another address for sending.

In step **2** of FIG. 2, the translated packet is sent further to the second computer. The inner IP packet has not been modified after that the first computer sent the packet. The second computer processes the packet using standard IPSec algorithms. The security gateway (the second computer) can e.g. decipher and/or check the authenticity of the packet, then remove the IPSec tunnelling, and forward the original packet towards the destination host, X. Thus, the entire original packet was unaffected by the translation as the IP header, and thus the address fields, was covered by IPSec.

After uncovering the original packet from the IPsec tunnel, the second computer makes a routing decision based on the IP header of the original packet. In the example, the IP destination address is X (host X in FIG. 2), and thus the second computer delivers the packet either directly to X, or to the next hop router.

In step **3** of FIG. 2, the packet is sent from the second computer (corresponding to SGW in FIG. 1) to host X, having

now only the original source IP address 10.0.0.1 and the original destination IP address X in the IP header. Thus, in step **3**, host X receives the packet sent by the second computer. Usually, an application process running on host X would generate some return traffic. This would cause an IP packet to be generated and sent to the second computer.

If a packet is sent back from host X to the first computer (corresponding to the client computer in FIG. 1), steps analogous to steps **1-3** are performed. The packet is thus first sent to the second computer, with the source IP address being X and the destination IP address being 10.0.0.1, in step **4**. The generated packet is then received by the second computer. The IPSec policy of the second computer requires that the packet be IPSec-processed using a tunnel mode IPSec SA. This processing is similar to the one in steps **1** and **2**. A new, outer IP header is added to the packet in the second computer, after which the resulting packet is secured using the IPSec SA. The outer IP source address is set to s-addr-**3** (103.6.5.4) while the outer IP destination address is set to s-addr-**2** (212.90.65.1). The SPI field is set to s-SPI-**2** (0×c1230012). In step **5**, the resulting packet is sent to the address indicated by the new outer IP destination

address, s-addr-**2**, the intermediate computer. The intermediate computer receives the packet and performs a similar address and SPI translation.

The inner addresses are still the same, and are not modified by the intermediate computer. Since the packet intended to be sent to the first computer, the new, translated outer destination IP address indicate the address of the first computer.

The resulting packet is sent to the first computer in step **6**.

As a result of step **6**, the packet is received by the first computer. The IPSec processing is undone, i.e. decryption and/or authentication is performed, and the original packet is uncovered from the IPSec tunnel. The original packet is then delivered to the application running on the first computer. In case the first computer acts as a router, the packet may be delivered to a host in a subnet for which the first computer acts as a router.

The first computer may be a mobile terminal, the outer address of which changes from time to time. The translation table is then modified using some form of signalling messages, as described in the summary section. Upon

receiving a request for modifying a translation, the intermediate computer updates the related translation table entry to match the new information supplied by the first computer. The operation of the protocol then proceeds as discussed above.

The above discussion is a limited example for illustration purposes. In other embodiments e.g. more than one SA for the connection—for instance, ESP followed by AH, can be used. This introduces two SPI values that must be translated. More than two is also, of course, possible. Furthermore, the example was considered for IPsec ESP only. The changes required for an embodiment in which AH (or ESP+AH) is used, are discussed next.

Changes for Using AH:

If the Authentication Header (AH) IPSec security transform is to be used, there are more considerations than in the previous example. In particular, modifications of the packet fields—even the outer IP header—are detected if AH is used. Thus, the following nominal processing is required by the first computer. The second computer performs standard IPSec processing also in this case.

In step **1**, when sending a packet, the first computer must perform IPsec processing using the SPI values and addresses used in the connection between the intermediate computer and the second computer. For instance, the SPI value would be s-SPI-**3**, the outer source address s-addr-**2**, and the outer destination address s-addr-**3**. The AH integrity check value (ICV) must be computed using these values. ICV is a value, which authenticates most of the fields of the packet. In practice, all fields that are never modified by routers are authenticated.

After computing the AH integrity check value, the outer addresses and the SPI value are replaced with the values used between the first computer and the intermediate computer: c-addr-**1** for the outer source address, c-addr-**2** for the outer destination address, and c-SPI-**2** for the SPI.

In step **2**, the intermediate computer performs the address and SPI translations as in the example with ESP described above. The resulting packet is identical to the one used by the first computer for the AH integrity check value calculation, except possibly for fields not covered by AH (such as the Time-To-Live field, the header checksum, etc). Thus, the AH integrity check value is now correct.

In step **3**, the second computer performs standard IPSec processing of AH. The packet, which now is uncovered from the tunnel is sent to the host X. As in the previous example, an application in host X usually generates a return packet that is to be sent to the first computer. This packet is sent to the second computer in step **4**.

Upon receiving the packet, the processing of the second computer are the same as in the example with ESP. The second computer computes an AH integrity check value of the tunneled packet it is sending to the mobile terminal. The integrity check value is computed against the outer source address of s-addr-**3**, outer destination address of s-addr-**2**, and the SPI value of s-SPI-**2**.

In step **5**, when the intermediate computer receives the packet, it performs ordinary translation of the packet. The new outer source address is c-addr-**2**, the outer destination address is c-addr-**1**, and the SPI value is c-SPI-**1**. At this point the AH integrity check value is incorrect, which was caused by the translations.

When the mobile terminal receives the packet, it performs a translation of the current outer addresses and the SPI field for the original ones used by the second computer: s-

addr-**3** for the outer source address, s-addr-**2** for the outer destination address, and s-SPI-**2** for the SPI value. This reproduces the packet originally sent by the second computer, except possibly for fields not covered by AH. This operation restores the AH integrity check value to its original, correct value. The AH integrity check is then performed against these fields.

Key Exchange Considerations

The above example discussed the "steady state" IPSec translations performed by the intermediate computer. The IPSec SAs and the IPSec translation table entries may be set up manually, or using some automated protocol, such as the Internet Key Exchange (IKE) protocol.

Because the security gateway (the second computer) is a standard IPSec host, it implements some standard key exchange protocol, such as IKE. The first computer and the intermediate computer may use some modified version of IKE, or any other suitable automatic key exchange protocol.

The key exchange must appear as a standard key exchange according to the key exchange protocol supported by the security gateway (the second computer), such as IKE. Also, the overall key exchange performed by the first,

intermediate, and second computer must establish not only cryptographic keys, but also the IPSec translation table entries. The overall key exchange protocol should not reveal the IPSec cryptographic keys to the intermediate computer to avoid even the potential for security problems.

In the following, an example of a modified IKE protocol is presented to outline the functionality of such a protocol in the context of the invention. The protocol provides the functionality described above. In particular, the intermediate computer has no knowledge of the IPSec cryptographic keys established. The protocol is presented on a general level to simplify the presentation.

The automatic IKE protocol is used prior to other protocols to provide strongly authenticated cryptographic session keys for the IPSec protocols ESP and AH. IKE performs the following functions: (1) security policy negotiation (what algorithms shall be used, lifetimes etc.), (2) a Diffie-Hellman key exchange, and (3) strong user/host authentication (usually using either RSA-based signatures or pre-shared authentication keys). IKE is divided into two phases: phase **1** and phase **2**. Phase **1** negotiates and establishes cryptographic keys for internal use of the IKE protocol itself, and also performs the strong user or host

authentication. Phase **2** negotiates and establishes cryptographic keys for IPSec. If IPSec tunnel mode is used, phase **2** also negotiates the kind of traffic that may be sent using the tunnel (so-called traffic selectors).

The IKE framework supports several "sub-protocols" for phase **1** and phase **2**. The required ones are "main mode" for phase **1**, and "quick mode" for phase **2**. These are used as illustrations, but the invention is not limited to these sub-protocols of IKE.

For the security gateway (second computer), the IKE session seems to be coming from the address s-addr-**2** in FIG. 3. Since there may be any number of mobile terminals served by the intermediate computer, the intermediate computer should either (1) manage a pool of addresses to be used for the s-addr-**2** translation table address, thus providing each user with a separate "surrogate address", or (2) use the same address (or a limited set of addresses), and ensure that the mobile terminals are identified using some other means than their IP address (IKE provides for such identification types, so this is not a problem).

The modified IKE protocol specified is analogous to the IPSec translation table approach. However, instead of SPIs,

the so-called IKE cookies are used as translation indices instead. IKE cookies are essentially IKE session identifiers, and are thus analogous to the IPSec SPI values, which is another form of a session or context identifier. There are two cookies: the initiator cookie, chosen by the host that initiates the IKE session, and the responder cookie, chosen by the host that responds to a session initiation.

The essential features of the protocol are (1) that it appears to be an entirely ordinary IKE key exchange for the security gateway, (2) that the IPsec translation table entry is formed by the intermediate computer during the execution of the protocol, (3) that the first computer obtains all the necessary information for its packet processing, and (4) that the intermediate computer does not obtain the IPsec cryptographic session keys.

The overall steps of the protocol are:

- 1. The first computer initiates the key exchange protocol by sending a message to the intermediate computer. This message is essentially the IKE

main mode initiation message, with some modifications required for this application.

- 2. The intermediate computer determines which security gateway (second computer) to forward this IKE session to, and also establishes a preliminary IKE translation table entry based on the information available from the message.
- 3. The security gateway (the second computer) replies to the IKE main mode initiation message.
- 4. The intermediate computer completes the IKE mapping based on the reply message.
- 5. The modified IKE protocol run continues through IKE main mode (the phase **1** exchange), which is followed by quick mode (the phase **2** exchange). Extensions of standard IKE messages are used between the first computer and the intermediate computer to accomplish the extra goals required by this modified IKE protocol.

In FIG. 4, the IKE session is described message by message. The following text indicates the contents of each message, and how they are processed by the various hosts. There are six main mode messages in the protocol, named mm**1**, mm**2**, . .

. , mm**6**, and three quick mode messages, named qm**1**, qm**2**, and qm**3**.

FIG. 5 illustrates the IKE translation table entry related to the modified IKE key exchange being performed. The bolded entries in each step are added or changed in that step as a result of the processing described in the text.

The IKE translation table partition for the connection between the first computer and the intermediate computer is as follows (the field name in FIG. 5 is given in parentheses):

Local and remote IP address (c-addr-**1**, c-addr-**2**)

Initiator and responder cookie (c-icky, c-rcky)

IKE identification of the first computer (c-userid, e.g. joe@netseal.com)

The IKE translation table partition for the connection between the intermediate computer and the second computer is as follows (the field name in FIG. 5 is given in parentheses):

Local and remote IP address (s-addr-**2**, s-addr-**3**)

Initiator cookie and responder cookie (s-icky, s-rcky)

In addition to these entries, other data may be kept by the intermediate computer and/or the first computer.

The key exchange is initiated by generating an initiator cookie and sending a zero responder cookie to the second computer. A responder cookie is generated in the second computer and a mapping between IP addresses and IKE cookie values in the intermediate computer is established. A translation table to modify IKE packets in flight by modifying the external IP addresses and possibly IKE cookies of the IKE packets is used.

Either the modified IKE protocol between the first computer and the intermediate computer is modified such that the IKE keys are transmitted from the first computer to the intermediate computer for decryption and modification of IKE packets or, alternatively, the modified IKE protocol between the first computer and the intermediate computer is modified such that the IKE keys are not transmitted from the first computer to the intermediate computer for decryption and modification of IKE packets, and the modification of IKE packets is done by the first computer with the intermediate computer requesting such modifications. The latter alternative is discussed in the

example that follows, since it is more secure than the first alternative.

Extra information, such as user information and SPI change requests, to be sent between the first and the intermediate computer, is sent by appending the extra information to the standard IKE messages. The IKE standard has message encoding rules that indicate a definite length, thus the added extra information can be separated from the IKE message itself. The extra information fields are preferably encrypted and authenticated, for instance by using a secret shared by the first computer and the intermediate computer. The details of this process are not relevant to the invention.

The extra information slot in each IKE message is called the message "tail" in the following.

IKE messages consist of an IKE header, which includes the cookie fields and message ID field, and of a list of payloads. A payload has a type, and associated information.

FIG. 4 considers an example of the routing of packets according to the invention considering IPSec security association set-up for distribution of keys. As in the foregoing FIG. 2, the session begins with sending a packet

from the client (first computer) to the server (intermediate computer).

The key exchange is initiated by the first computer. Thus, in step **1** of FIG. 4, the first computer constructs mm**1**. The IP header of the message contains the following values:

- IP source address: 195.1.2.3 (c-addr-**1**)
- IP destination address: 212.90.65.1 (c-addr-**2**)

The IKE header contains the following values (step **1** in Figure X):

- Initiator cookie: CKY**1** (c-icky)
- Responder cookie: **0** (c-rcky)
- Message ID: **0**

The message contains the following payloads:

- A Security Association (SA) payload, which contains the IKE phase **1** security policy offers from the first computer.

- The message may contain additional payloads, such as Vendor Identification (VID) payloads, certificate requests/responses, etc.
- A VID payload can be used to indicate that the first computer supports the protocol described here.

The message tail contains the following information:

- User identification type and value—the c-userid field. These are used by the intermediate computer to choose a security gateway to forward this session to. The identification type may be any of the IKE types, but additional types can be defined. An alternative to this field is to directly indicate the security gateway for forwarding. There are other alternatives as well, but these are not essential to the invention.

In step **2**, the mm**1** is received by the intermediate computer. The intermediate computer examines the message, and forms the preliminary IKE translation table entry. FIG. 5, step **1** illustrates the contents of this preliminary entry. The c-userid field is sent in the mm**1** tail.

The intermediate computer then determines which security gateway to forward this IKE session to. The determination may be based on any available information, static configuration, load balancing, or availability requirements. The presented, simple method is to use the identification information in the mm**1** tail to look up the first matching identification type and value from a table. An example of such a table is presented in FIG. 6.

The identification mapping table of FIG. 6, is one method for choosing a security gateway that matches the incoming mobile terminal. The identification table would in this example be an ordered list of identification type/value entries, that match to a given security gateway address. When the incoming mobile terminal identification matches the identification in the table, the corresponding security gateway is used. For instance, john.smith@netseal.com would match the first row of the table, i.e., the security gateway 123.1.2.3, while joe@netseal.com matches the second row, i.e., the security gateway 103.6.5.4. The identification types include any identification types defined for the IKE protocol, and may contain other types as well, such as employee numbers, etc.

Other methods of determining the security gateway to be used may be employed. One such method is for the mobile terminal to directly indicate a given security gateway to be used. The mobile terminal may also indicate a group of security gateways, one of which is used. The exact details are not relevant to the invention.

In addition to determining the security gateway address, the intermediate computer determines which address its for communication between itself and the second computer. The same address as is used for the communication between the first and the intermediate computer may be used, but a new address may also be used. The address can be determined using a table similar to the one in FIG. 6, or the table of FIG. 6 may be extended to include this address.

The intermediate computer then generates its own initiator cookie. This is done to keep the two session identifier spaces entirely separate, although the same initiator cookie may be passed as is.

After these determinations, the preliminary translation table entry is modified. FIG. 5, step **2** illustrates the contents of the entry at this point.

The original IP header fields are modified as follows (step **2** in FIG. 4):

- IP source address: 212.90.65.1 (s-addr-**2**)
- IP destination address: 103.6.5.4 (s-addr-**3**)

The IKE header is modified as follows:

- Initiator cookie: CKY**2** (s-icky)
- Responder cookie: **0** (s-rcky)
- Message ID: **0**

The message tail is removed. The VID payload that identifies support for this modified protocol is also removed. The mm**1** is then forwarded to the second computer.

In step **3**, the second computer responds with mm**2**. The IP header of the message contains the following values (step **3** in FIG. 4):

- IP source address: 103.6.5.4 (s-addr-**3**)
- IP destination address: 212.90.65.1 (s-addr-**2**)

The IKE header contains the following values:

- Initiator cookie: CKY**2** (s-icky)
- Responder cookie: CKY**3** (s-rcky)
- Message ID: **0**

The message contains the following payloads:

- Security Association (SA) payload. This is a reply to the offer by the first computer, and indicates which security configuration is acceptable for the second computer (this scenario assumes success, so the case of an error reply is not considered).
- Possibly optional IKE payloads, such as VID payloads, certificate requests/replies, etc.

There is no message tail.

In step **4**, the mm**2** is received by the intermediate computer. The intermediate computer updates its IKE translation table based on the received message. Step **3** in

FIG. 5 illustrates the contents of the translation table entry at this point.

The intermediate computer generates its own responder cookie, CKY**4**, and updates the translation table yet again. Step **4** in FIG. 5 illustrates the entry at this point. After this step, the translation table entry is complete, and the address and cookie translations are performed as in steps **1-4** for the following messages.

The translated message contains the following IP header fields (FIG. 4, step **4**)

- IP source address: 212.90.65.1 (c-addr-**2**)
- IP destination address: 195.1.2.3 (c-addr-**1**)

The translated IKE header contains the following fields:

- Initiator cookie: CKY**1** (c-icky)
- Responder cookie: CKY**4** (c-rcky)

The message contains the following payloads:

- The SA payload sent by the second computer.
- Any optional payloads sent by the second computer.
- A VID payload may be added to indicate support of this modified protocol to the first computer.

A message tail is added, and contains the following information:

- Address and/or identification information of the chosen security gateway (the second computer). This information can be used by the client to choose proper authentication information, such as RSA keys.

The message is then forwarded to the first computer.

In step **5**, the first computer constructs mm**3**. The message contains the following payloads:

- A Key Exchange (KE) payload, that contains Diffie-Hellman key exchange data of the first computer.

- A Nonce (NONCE) payload, that contains a random number chosen by the first computer.
- Possibly optional IKE payloads.

The message is sent to the intermediate computer.

In step **6**, the mm**3** is forwarded to the second computer. The contents of the message are not changed, only the IP header addresses and the IKE cookies, in the manner described in steps **1-4**.

In step **7**, the second computer receives mm**3** and responds with mm**4**. The message contains the following payloads:

- A Key Exchange (KE) payload, that contains Diffie-Hellman key exchange data of the second computer.
- A Nonce (NONCE) payload, that contains a random number chosen by the second computer.
- Possibly optional IKE payloads.

In step **8**, the mm**4** is forwarded to the first computer.

In step **9**, the first computer constructs mm**5**, which is the first encrypted message in the session. All subsequent

messages are encrypted using the IKE session keys established from the previous Diffie-Hellman key exchange (the messages mm**3** and mm**4**) by means of hash operations, as described in the IKE specification. Note that the intermediate computer does not possess these keys, and can thus not examine the contents of any subsequent IKE messages. In fact, the intermediate computer has no advantage compared to a hostile attacker if it attempts to decipher the IKE traffic. Instead, the intermediate computer indirectly modifies some fields in the IKE messages by sending a modification request in the IKE message tail to the first computer, which does the requested modifications before IKE encryption processing.

The message contains the following payloads:

- An Identification (ID) payload, that identifies the first computer to the second computer. This identification may be the same as the identification sent in the mm**1** tail, but may differ from that. These two identifications serve different purposes: the mm**1** tail identification (c-userid) is used to select a security gateway

for IKE session forwarding (the second computer), while the ID payload in this message is used by the second computer for IKE authentication purposes, for instance, to select proper RSA authentication keys.

- A Signature (SIG) or Hash (HASH) payload, that serves as an authenticator. A signature payload is used if RSA- or DSS-based authentication is used, while a hash payload is used for pre-shared key authentication. There are other authentication methods in IKE, and IKE can also be extended with new authentication methods. These are not essential to the invention, and the following text assumes RSA authentication (i.e., use of the signature payload).
- Possibly optional IKE payloads.

The message tail contains the-following information:

- The SPI value that the first computer wants to use for receiving IPsec-protected messages from the intermediate computer, i.e., the c-SPI-**1** value of the IPsec translation table in FIG. 3.

More than one SPI value could be transmitted here, but for simplicity, the following discussion assumes that only a single SPI is necessary (i.e. only one SA is applied for IPsec traffic processing). Extending the scheme to multiple SPIs is straightforward.

In step **10**, the mm**5** is forwarded to the second computer.

The intermediate computer removes the message tail, and performs the IKE translation discussed previously, and then forwards the message to the second computer.

In step **11**, the second computer receives the mm**5** message, and authenticates the user (or the host, depending on what identification type is used). Assuming that the authentication succeeds, the second computer proceeds to authenticate itself to the first computer.

The mm**6** message contains the following payloads:

- An Identification (ID) payload, that identifies the second computer to the first computer.
- A Signature (SIG) payload (here RSA authentication is assumed).

- Possibly optional IKE payloads.

In step **12**, the mm**6** is received by the intermediate computer. The intermediate computer does not change the message itself, but adds a tail with the following information:

- The SPI value that the intermediate computer wants the first computer to offer to the second computer in the qm**1** message. Since the intermediate computer cannot access the contents of the IKE messages, this modification request is made using the message tail (see the discussion of step **9**). The SPI value sent matches the s-SPI-**2** field of the IPsec translation table of FIG. 3.
- The SPI value that the intermediate computer wants the first computer to use for messages sent to itself. This matches the c-SPI-**2** field of the IPsec translation table of FIG. 3.

The resulting message is forwarded to the first computer.

In step **13**, the first computer constructs qm**1**, which contains the following IKE payloads:

- A Hash (HASH) payload, that serves as an authenticator of the message.
- A Security Association (SA) payload, which contains the IKE phase **2** security policy offers from the first computer, i.e., the IPsec security policy offers. The SA payload contains the SPI value assigned to the first computer in the mm**6** message, i.e., s-SPI-**2** in FIG. 3.
- Optionally, a Key Exchange (KE) payload, if a new Diffie-Hellman key exchange is to be performed in phase **2** (this depends on the contents of the SA payload).
- A Nonce (NONCE) payload, which contains a random value chosen by the first computer.
- Optionally, two Identification (ID) payloads that indicate the IPsec traffic selectors that the first computer proposes for an IPsec tunnel mode SA. If IPsec transport mode is used, these are not necessary, but they may still be used. They may also be omitted if IPsec tunnel mode is used.

The IKE header is the same as previously, except that the Message ID field now contains a non-zero 32-bit value, that

serves as a phase **2** session identifier. This identifier remains constant for the entire quick mode exchange.

The message is sent to the intermediate computer.

In step **14**, the intermediate computer forwards the qm**1** message to the second computer.

In step **15**, the second computer inspects the security policy offers and other information contained in the qm**1** message, and determines which security policy offer matches its own security policy (the case when no security policies match results in an error notification message).

The second computer responds with qm**2** message that contains the following payloads:

- A Hash (HASH) payload, that serves as an authenticator of the message.
- A Security Association (SA) payload, which indicates the security policy offer chosen by the second computer. The message also contains the SPI value that the second computer wants to use when receiving IPsec-protected messages. The SPI

value matches s-SPI-**3** of the IPsec translation table in FIG. 3.

- Optionally, a Key Exchange (KE) payload, if a new Diffie-Hellman key exchange is to be performed in phase **2**.
- A Nonce (NONCE) payload, which contains a random value chosen by the second computer.
- If Identification (ID) payloads were sent by the first computer, the second computer also sends Identification payloads.

In step **16**, the intermediate computer forwards the qm**2** message to the first computer.

In step **17**, the first computer constructs qm**3** message, which contains the following payloads:

- A Hash (HASH) payload, that serves as an authenticator of the message.

The following information is sent in the message tail:

- The SPI value sent by the second computer in the qm**2** message. This is sent here, because the intermediate computer cannot decrypt the qm**2** message and look up the SPI from there. The SPI value matches s-SPI-**3** of the IPsec translation table in FIG. 3.

In step **18**, the intermediate computer receives the qm**3** and reads the s-SPI-**3** value from the message tail. All the information required to construct the IPsec translation table entry is now gathered, and the entry can be added to the translation table. In particular, the information fields are as follows:

- c-addr-**1**: same as c-addr-**1** of the IKE session (195.1.2.3).
- c-addr-**2**: same as c-addr-**2** of the IKE session (212.90.65.1).
- c-SPI-**1**: received in the mm**5** message tail from the first computer.
- c-SPI-**2**: chosen by the intermediate computer, sent to the first computer in the mm**6** message tail.

- s-addr-**2**: same as s-addr-**2** of the IKE session (212.90.65.1 in this example, may be different than c-addr-**2**).
- s-addr-**3**: same as s-addr-**3** of the IKE session (103.6.5.4).
- s-SPI-**2**: chosen by the intermediate computer, sent to the first computer in mm**6** message tail.
- s-SPI-**3**: sent by the second computer in qm**2** to the first computer, which sends it to the intermediate computer in qm**3** message tail.

The intermediate computer forwards the qm**3** message to the second computer, which completes the IKE key exchange, and the IPsec translation table set up.

The IPsec cryptographic keys established using the modified IKE key exchange presented above are either derived from the Diffie-Hellman key exchange performed in IKE main mode, or from the (optional) Diffie-Hellman key exchange performed in quick mode. In both cases, the intermediate computer has no access to the shared secret established using the Diffie-Hellman algorithm. In fact, the intermediate computer has no advantage when compared to a random, hostile attacker.

The above presentation was simplified and exemplified to increase clarity of the presentation. There are several issues not discussed, but these issues are not essential to the invention.

Some of these issues are the following:

- The phase **1** used main mode. Any other IKE phase **1** exchange can be used; this changes the details of the protocol but not the essential ideas.
- There are other approaches than the one presented here. One approach is for the first computer to reveal the IKE keys to the intermediate computer, so that the second computer is able to modify the required fields of the message (namely, SPI values).
- The discussion assumes that the first computer initiates the IKE exchange. The opposite direction is possible, too, but requires more considerations.
- The commit bit feature of IKE is not used. Adding that is simple.

- Security gateway selection is based on a table lookup indexed by an identification type/value pair sent by the first computer. Other mechanisms are easy to implement.
- The discussion assumes a successful IKE key exchange. Error cases are easy to handle.
- Phase **1** policy lookup (when processing mm**1** and mm**2** messages) is not based on the identity of the IKE counterpart. This is not a major issue, since the phase **1** security policy can be independent of the counterpart without limiting usability.
- Phase **1** is a pre-requisite for executing the protocol in the example. This can be easily changed by moving some of the "tail" items to phase **2**.
- The protocol establishes a pair of SAs, one for each direction, and manages the SPI value modifications of these SAs. It is easy to extend this to cover SA bundles with more than one SA, i.e., SAs applied in sequence (ESP followed by AH, for instance). This requires more than one SPI for each direction, but is easy to add to the protocol described.

The invention is not concerned with the details of the key exchange protocol. The presented outline for one such protocol is given as an example, several other alternatives exist. The invention is also not concerned with the IKE key exchange protocol: other key exchange protocols exist, and similar ideas can be applied in using them in the content of the invention.

While the present invention has been described in accordance with preferred compositions and embodiments, it is to be understood that certain substitutions and alterations may be made thereto without departing from the spirit and scope of the following claims.

We claim:

1. (New) An intermediate computer for secure forwarding of messages in a telecommunication network, comprising:

an intermediate computer configured to connect to a telecommunication network;

the intermediate computer configured to be assigned with a first network address in the telecommunication network;

the intermediate computer configured to receive from a mobile computer a secure message sent to the first network address having an encrypted data payload of a message and a unique identity;

the intermediate computer configured to read the unique identity from the secure message sent to the first network address; and

the intermediate computer configured to access a translation table, to find a destination address from the translation table using the unique identity, and

to forward the encrypted data payload to the destination address using a network address of the intermediate computer as a source address of a forwarded message containing the encrypted data payload.

2. (New) The intermediate computer of claim 1, wherein the intermediate computer is further configured to substitute the unique identity read from the secure message with

another unique identity prior to forwarding the encrypted data payload.

3. (New) The intermediate computer of claim 1, wherein the translation table is stored at the intermediate computer.

4. (New) The intermediate computer of claim 1, wherein the translation table includes two partitions, the first partition containing information fields related to the connection over which the secure message is sent to the first network address, the second partition containing information fields related to the connection over which the forwarded encrypted data payload is sent to the destination address.

5. (New) The intermediate computer of claim 1, wherein the intermediate computer is not configured to access cryptographic keys used to encrypt or authenticate the messages.

6. (New) The intermediate computer of claim 1, wherein the intermediate computer is configured to forward the encrypted data payload using SSL or TLS protocol.

7. (New) The intermediate computer of claim 1, wherein the intermediate computer is configured to receive secure

messages using SSL or TLS protocol.

8. (New) The intermediate computer of claim 1, wherein the unique identity read from the secure message includes one or more Security Parameter Index values.

9. (New) The intermediate computer of claim 1, wherein the intermediate computer is configured to modify the translation table entry address fields in response to a signaling message sent from the mobile computer when the mobile computer changes its address such that the intermediate computer can know that the address of the mobile computer is changed.

10. (New) The intermediate computer of claim 1, wherein the intermediate computer is a server.

11. (New) The intermediate computer of claim 1, wherein the source address of the forwarded message is the same as the first network address.

12. (New) A computer for sending secure messages, and for enabling secure forwarding of messages in a telecommunication network by an intermediate computer to a recipient computer, comprising:
a computer configured to connect to a telecommunication

network;

the computer configured to be assigned with a network address in the telecommunication network, wherein the computer is a mobile computer in that the address of the mobile computer changes;

the computer configured to form a secure message by encrypting the data payload of a message and giving the message a unique identity and a destination address of an intermediate computer, wherein the unique identity and the destination address are capable of being used by the intermediate computer to find an address to a recipient computer;

the computer configured to send the secure message to the intermediate computer for forwarding of the encrypted data payload to the recipient computer; and

the computer configured to set up a secure connection using a key exchange protocol.

13. (New) The computer of claim 12, wherein the computer is configured to form the secure message using a message received by the computer.

14. (New) The computer of claim 12, wherein the computer is configured to encapsulate the message in an outer IP header.

15. (New) The computer of claim 12, wherein the computer is

configured to form secure messages using IPSec protocols.

16. (New) The computer of claim 12, wherein the computer is configured to form secure messages containing data payload of a message, an inner IP header containing actual sender and receiver addresses, an outer IP header containing the addresses of the computer and the intermediate computer, and a unique identity.

17. (New) The computer of claim 12, wherein the unique identity is one or more Security Parameter Index values.

18. (New) The computer of claim 12, wherein the computer is configured to send a signaling message to the intermediate computer when the computer changes its address such that the intermediate computer can know that the address of the computer is changed.

19. (New) The computer of claim 18, wherein the computer is configured to send the signaling message encrypted.

20. (New) The computer of claim 19, wherein the computer is configured to send the signaling message authenticated.

21. (New) The computer of claim 12, wherein the computer is

configured to send the secure message using SSL or TLS protocol.

Abstract of Disclosure

The method and system enable secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network. A message is formed in the first computer or in a computer that is served by the first computer, and in the latter case, sending the message to the first computer. In the first computer, a secure message is then formed by giving the message a unique identity and a destination address. The message is sent from the first computer to the intermediate computer after which the destination address and the unique identity are used to find an address to the second computer. The current destination address is substituted with the found address to the second computer, and the unique identity is substituted with another unique identity. Then the message is forwarded to the second computer.

Electronic Acknowledgement Receipt

EFS ID:	27729950
Application Number:	15372208
International Application Number:	
Confirmation Number:	6275
Title of Invention:	METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION
First Named Inventor/Applicant Name:	Sami Vaarala
Customer Number:	33369
Filer:	Rolf Fasth/Sloan Smith
Filer Authorized By:	Rolf Fasth
Attorney Docket Number:	664.1078CON2
Receipt Date:	08-DEC-2016
Filing Date:	
Time Stamp:	08:11:14
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	TRX.pdf	237037 340481c751220a56f733b97129f9a994ad913af0	no	1
Warnings:					

Information:					
2	Miscellaneous Incoming Letter	MARKED_UP.pdf	14018487 c3b15e8cfa556d0a4b4fd1a39b96cf58503e6200	no	76
Warnings:					
Information:					
			Total Files Size (in bytes):	14255524	

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.

METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION

PRIOR APPLICATIONS

This application is a U.S. Continuation Patent Application based on U.S. Continuation Patent Application No. 13/685,544, filed 26 November 2012 that claims priority from US Patent Application Serial No. 10/500,930, filed 19 October 2005, which claims priority from PCT/FI03/00045, filed 21 January 2003, that claims priority from Finnish Pat. App. No. 20020112, filed 22 Jan 2002.

TECHNICAL FIELD

The method and system of the invention are intended to secure connections in telecommunication networks. Especially, it is meant for wireless Internet Service Provider (ISP) connections.

TECHNICAL BACKGROUND

An internetwork is a collection of individual networks connected with intermediate networking devices that function as a single large network. Different networks can be interconnected by routers and other networking devices to create an internetwork.

A local area network (LAN) is a data network that covers a relatively small geographic area. It typically connects workstations, personal computers, printers and other devices. A wide area network (WAN) is a data communication network that covers a relatively broad geographic area. Wide area networks (WANS) interconnect LANs across normal telephone lines and, for instance, optical networks; thereby interconnecting geographically disposed users.

There is a need to protect data and resources from disclosure, to guarantee the authenticity of data, and to protect systems from network based attacks. More in detail, there is a need for confidentiality (protecting the contents of data from being read) integrity (protecting the data from being modified, which is a property that is independent of confidentiality), authentication (obtaining assurance about she actual sender of data), replay protection (guaranteeing that data is fresh, and not a copy of previously sent data), identity protection (keeping the identities of parties exchanging data secret from outsiders), high availability, i.e. denial-of-service protection (ensuring that the system functions even when under attack) and access control. IPSec is a technology providing most of these, but not all of them. (In

particulars identity protection is not completely handled by IPSec, and neither is denial-of-service protection.)

The IP security protocols (IPSec) provides the capability to secure communications between arbitrary hosts, e.g. across a LAN, across private and public wide area networks (WANs) and across the internet IPSec can be used in different ways, such as for building secure virtual private networks, to gain a secure access to a company network, or to secure communication with other organisations, ensuring authentication and confidentiality and providing a key exchange mechanism. IPSec ensures confidentiality integrity, authentication, replay protection, limited traffic flow confidentiality, limited identity protection, and access control based on authenticated identities. Even if some applications already have built in security protocols, the use of IPSec further enhances the security.

IPSec can encrypt and/or authenticate traffic at IP level. Traffic going in to a WAN is typically compressed and encrypted and traffic coming from a WAN is decrypted and decompressed. IPSec is defined by certain documents, which contain rules for the IPSec architecture. The documents that define IPSec, are, for the time being, the Request For

Comments (RFC) series of the Internet Engineering Task Force (IETF), in particular, RFCs 2401-2412.

Two protocols are used to provide security at the IP layer; an authentication protocol designated by the header of the protocol, Authentication Header (AH), and a combined encryption/authentication protocol designated by the format of the packet for that protocol, Encapsulating Security Payload (ESP) AH and ESP are however similar protocols, both operating by adding a protocol header. Both AH and ESP are vehicles for access control based on the distribution of cryptographic keys and the management of traffic flows related to these security protocols.

Security association (SA) is a key concept in the authentication and the confidentiality mechanisms for IP. A security association is a one-way relationship between a sender and a receiver that offers security services to the traffic carried on it if a secure two-way relationship is needed, then two security associations are required. If ESP and AH are combined, or if ESP and/or AH are applied more than once, the term SA bundle is used, meaning that two or more SAs are used. Thus, SA bundle refers to one or more SAs applied in sequence, e.g. by first performing an ESP

protection, and then an AH protection. The SA bundle is the combination of all SAs used to secure a packet.

The term IPsec connection is used in what follows in place of an IPSec bundle of one or more security associations, or a pair of IPSec bundles—one bundle for each direction—of one or more security associations. This term thus covers both unidirectional and bi-directional traffic protection. There is no implication of symmetry of the directions, i.e., the algorithms and IPSec transforms used for each direction may be different.

A security association is uniquely identified by three parameters. The first one, the Security Parameters Index (SPI), is a bit string assigned to this SA The SPI is carried in AH and ESP headers to enable the receiving system to select the SA under which a received packet will be processed. IP destination address is the second parameter, which is the address of the destination end point of the SA, which may be an end user system or a network system such as a firewall or a router. The third parameter, the security protocol identifier indicates whether the association is an AH or ESP security association.

In each IPSec implementation, there is a nominal security association data base (SADB) that defines the parameters associated with each SA. A security association is normally defined by the following parameters. The Sequence Number Counter is a 32-bit value used to generate the sequence number field in AH or ESP headers. The Sequence Counter Overflow is a flag indicating whether overflow of the sequence number counter should generate an auditable event and prevent further transmission of packets on this SA. An Anti-Replay Window is used to determine whether an inbound AH or ESP packet is a replay. AH information involves information about the authentication algorithm, keys and related parameters being used with AH. ESP information involves information of encryption and authentication algorithms, keys, initialisation vectors, and related parameters being used with IPSec. AH information consists of the authentication algorithm, keys and related parameters being used with AH. ESP information consists of encryption and authentication algorithms, keys, cryptographic initialisation vectors and related parameters being used with ESP. The sixth parameter, Lifetime of this Security Association, is a time-interval and/or byte-count after which this SA must be replaced with a new SA (and new SPI) or terminated plus an indication of which of these

actions should occur. IPSec Protocol Mode is either tunnel or transport mode. Maximum Transfer Unit (MTU), an optional feature, defines the maximum size of a packet that can be transmitted without fragmentation. Optionally an MTU discovery protocol may be used to determine the actual MTU for a given route, however, such a protocol is optional.

Both AH and ESP support two modes used, transport and tunnel mode.

Transport mode provides protection primarily for upper layer protocols and extends to the payload of an IP packet Typically, transport mode is used for end-to-end communication between two hosts. Transport mode may be used in conjunction with a tunnelling protocol, other than IPSec tunnelling, to provide a tunnelling capability.

Tunnel mode provides protection to the entire IP packet and is usually used for sending messages through more than two components, although tunnel mode may also be used for end-to-end communication between two hosts. Tunnel mode is often used when one or both ends of a SA is a security gateway, such as a firewall or a router that implements IPSec. With tunnel mode, a number of hosts on networks behind firewalls may engage in secure communications

without implementing IPSec. The unprotected packets generated by such hosts are tunnelled through external networks by tunnel mode SAs set up by the IPSec software in the firewall or secure router at boundary of the local network.

To achieve this, after the AH or ESP fields are added to the IP packet, the entire packet plus security fields are treated as the payload of a new outer IP packet with a new outer IP header. The entire original, or inner, packet travels through a tunnel from one point of an IP network to another: no routers along the way are able to examine the inner IP packet. Because the original packet is encapsulated, the new larger packet may have totally different source and destination addresses, adding to the security. In other words, the first step in protecting the packet using tunnel mode is to add a new IP header to the packet; thus the "IP|payload" packet becomes "IP|IP|payload". The next step is to secure the packet using ESP and/or AH. In case of ESP, the resulting packet is "IP|ESP|IP|payload". The whole inner packet is covered by the ESP and/or AH protection. AH also protects parts of the outer header, in addition to the whole inner packet.

The IPSec tunnel mode operates e.g. in such a way that if a host on a network generates an IP packet with a destination address of another host on another network, the packet is routed from the originating host to a security gateway (SGW), firewall or other secure router at the boundary of the first network. The SGW or the like filters all outgoing packets to determine the need for IPSec processing. If this packet from the first host to another host requires IPSec, the firewall performs IPSec processing and encapsulates the packet in an outer IP header. The source IP address of this outer IP header is this firewall and the destination address may be a firewall that forms the boundary to the other local network. This packet is now routed to the other host's firewall with intermediate routers examining only the outer IP header At the other host firewall, the outer IP header is stripped off and the inner packet is delivered to the other host.

ESP in tunnel mode encrypts and optionally authenticates the entire inner IP packet, including the inner IP header AH in tunnel mode authenticates the entire inner IP packet, including the inner IP header, and selected portions of the outer IP header.

The key management portion of IPSec involves the determination and distribution of secret keys. The default automated key management protocol for IPSec is referred to as ISAKMP/Oakley and consists of the Oakley key determination protocol and Internet Security Association and Key Management Protocol (ISAKMP). Internet key exchange (IKE) is a newer name for the ISAKMP/Oakley protocol. IKE is based on the Diffie-Hellman algorithm and supports RSA signature authentication among other modes. IKE is an extensible protocol, and allows future and vendor-specific features to be added without compromising functionality.

IPSec has been designed to provide confidentiality, integrity, and replay protection for IP packets. However, IPSec is intended to work with static network topology, where hosts are fixed to certain subnetworks. For instance, when an IPSec tunnel has been formed by using Internet Key Exchange (IKE) protocol, the tunnel endpoints are fixed and remain constant. If IPSec is used with a mobile host, the IKE key exchange will have to be redone from every new visited network. This is problematic, because IKE key exchanges involve computationally expensive Diffie-Hellman key exchange algorithm calculations and possibly RSA calculations. Furthermore, the key exchange requires at

least three round trips (six messages) if using the IKE aggressive mode followed by IKE quick mode, and nine messages if using IKE main mode followed by IKE quick mode. This may be a big problem in high latency networks, such as General Packet Radio Service (GPRS) regardless of the computational expenses.

In this text, the term mobility and mobile terminal does not only mean physical mobility, instead the term mobility is in the first hand meant moving from one network to another, which can be performed by a physically fixed terminal as well.

The problem with standard IPSec is thus that it has been designed for static connections. For instance, the end points of an IPSec tunnel mode SA are fixed. There is also no method for changing any of the parameters of an SA, other than by establishing a new SA that replaces the previous one. However, establishing SAs is costly in terms of both computation time and network latency.

An example of a specific scenario where these problems occur is described next in order to illustrate the problem.

In the scenario, there is a standard IPSec security gateway, which is used by a mobile terminal e.g. for remote

access. The mobile terminal is mobile in the sense that it changes its network point of attachment frequently. A mobile terminal can in this text thus be physically fixed or mobile. Because it may be connected to networks administered by third parties, it may also have a point of attachment that uses private addresses—i.e., the network is behind a router that performs network address translation (NAT). In addition, the networks used by the mobile terminal for access may be wireless, and may have poor quality of service in terms of throughput and e.g. packet drop rate.

Standard IPSec does not work well in the scenario. Since IPSec connections are bound to fixed addresses, the mobile terminal must establish a new IPSec connection from each point of attachment. If an automated key exchange protocol, such as IKE, is used, setting up a new IPsec connection is costly in terms of computation and network latency, and may require a manual authentication phase (for instance, a one-time password). If IPSec connections are set up manually, there is considerable manual work involved in configuring the IPSec connection parameters.

Standard IPSec does e.g. not work through NAT devices at the moment. A standard IPSec NAT traversal protocol is

currently being specified, but the security gateway in the scenario might not support an IPSec protocol extended in this way. Furthermore, the current IPSec NAT traversal protocols are not well suited to mobility.

There are no provisions for improving quality of service over wireless links in the standard IPSec protocol. If the access network suffers from high packet drop rates, the applications running in the mobile host and a host that the mobile terminal is communicating with will suffer from packet drops.

A known method of solving some of these problems is based on having an intermediate host between the mobile terminal and the IPSec security gateway. The intermediate host might be a Mobile IP home agent, that provides mobility for the connection between the mobile terminal and the home agent, while the connection from the mobile node to the security gateway is an ordinary IPSec connection. In this case, packets sent by an application in the mobile client are first processed by IPSec, and then by Mobile IP.

In the general case, this implies both Mobile IP and IPSec header fields for packets exchanged by the mobile terminal and the home agent. The Mobile IP headers are removed by

the home agent prior to delivering packets to the security gateway, and added when delivering packets to the mobile terminal. Because of the use of two tunnelling protocols (Mobile IP and IPSec tunnelling), the solution is referred to as "double tunnelling" in this document.

The above method solves the mobility problem, at the cost of adding extra headers to packets. This may have a significant impact on networks that have low throughput such as the General Packet Radio System (GPRS).

Another known method is again to use an intermediate host between the mobile client and the IPSec security gateway. The intermediate host has an IPSec implementation that may support NAT traversal, and possibly some proprietary extensions for improving quality of service of the access network, for instance.

The mobile host would now establish an IPSec connection between itself and the intermediate host, and would also establish an IPSec connection between itself and the IPSec security gateway. This solution is similar to the first known method, except that two IPSec tunnels are used. It solves a different set of problems—for instance, NAT

traversal—but also adds packet size overhead because of double IPsec tunnelling.

A third known method is to use a similar intermediate host as in the second known method, but establish an IPSec connection between the mobile terminal and the intermediate host, and another, separate IPSec connection between the intermediate host and the security gateway. The IPSec connection between the mobile terminal and the intermediate host may support NAT traversal, for instance, while the second IPSec connection does not need to.

When packets are sent by an application in the mobile terminal, the packets are IPSec-processed using the IPSec connection shared by the mobile terminal and the intermediate host. Upon receiving these packets, the intermediate host undoes the IPSec-processing. For instance, if the packet was encrypted, the intermediate host decrypts the packet. The original packet would now be revealed in plaintext to the intermediate host. After this, the intermediate host IPSec-processes the packet using the IPSec connection shared by the intermediate host and the security gateway, and forwards the packet to the security gateway.

This solution allows the use of an IPSec implementation that support NAT traversal, and possibly a number of other (possibly vendor specific) improvements, addressing problems such as the access network quality of service variations. Regardless of these added features, the IPSec security gateway remains unaware of the improvements, and is not required to implement any of the protocols involved in improving service. However, the solution has a major drawback: the IPsec packets are decrypted in the intermediate host, and thus possibly sensitive data is unprotected in the intermediate host.

Consider a business scenario where a single intermediate host provides improved service to a number of separate customer networks, each having its own standard IPSec security gateway. Having decrypted packets of various customer networks in plaintext form in the intermediate host is clearly a major security problem.

To summarise, the known solutions either employ extra tunnelling, causing extra packet size overhead, or use separate tunnels, causing potential security problems in the intermediate host(s) that terminate such tunnels.

THE OBJECT OF THE INVENTION

The object of the invention is to develop a method for forwarding secure messages between two computers, especially, via an intermediate computer by avoiding the above mentioned disadvantages.

Especially, the object of the invention is to forward secure messages in a way that enables changes to be made in the secure connection

SUMMARY OF THE INVENTION

The method and system of the invention enable secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network. It is mainly characterized in that a message is formed in the first computer or in a computer that is served by the first computer, and in the latter case, sending the message to the first computer. In the first computer, a secure message is then formed by giving the message a unique identity and a destination address. The message is sent from the first computer to the intermediate computer, whereafter said destination address and the unique identity are used to find an address to the second computer. The current destination address is substituted with the found address to the second computer,

and the unique identity is substituted with another unique identity. Then the message is forwarded to the second computer.

Preferably, the first computer processes the formed message using a security protocol and encapsulates the message at least in an outer IP header. The outer IP header source address is the current address of the first computer, while the destination address is that of the intermediate computer. The message is then sent to the intermediate computer, which matches the outer IP header address fields together with a unique identifier used by the security protocol, and performs a translation of the outer addresses and the unique identity used by the security protocol. The translated packet is then sent to the second computer, which processes it using the standard security protocol in question. In the method of the invention, there is no extra encapsulation overhead as in the prior art methods. Also, the intermediate computer does not need to undo the security processing, e.g. decryption, and thus does not compromise security as in the prior art methods.

Corresponding steps are performed when the messages are sent in the reverse direction, i.e. from the second computer to the first computer.

Preferably, the secure message is formed by making use of the IPSec protocols, whereby the secure message is formed by using an IPsec connection between the first computer and the intermediate computer. The message sent from the first computer contains message data, an inner IP header containing actual sender and receiver addresses, an outer IP header containing the addresses of the first computer and the intermediate computer, a unique identity, and other security parameters. The unique identity is one or more SPI values and the other security parameters contain e.g. the IPsec sequence number(s). The number of SPI values depends on the SA bundle size (e.g. ESP+AH bundle would have two SPI values). In the following, when an SA is referred to, the same applies to an SA bundle. The other related security parameters, containing e.g. the algorithm to be used, a traffic description, and the lifetime of the SA, are not sent on the wire. Only SPI and sequence number are sent for each IPsec processed header (one SPI and one sequence number if e.g. ESP only is used; two SPIs and two sequence numbers if e.g. ESP+AH is used, etc.).

Thus, the unsecured data packet message is formed by the sending computer, which may or may not be the first computer. The IP header of this packet has IP source and

destination address fields (among other things). The packet is encapsulated e.g. wrapped inside a tunnel, and the resulting packet is secured. The secured packet has a new outer IP header, which contains another set of IP source and destination addresses (in the outer header—the inner header is untouched), i.e. there are two outer addresses (source and destination) and two inner addresses. The processed packet has a unique identity, the IPsec SPI value(s).

An essential idea of the invention is to use the standard protocol (IPSec) between the intermediate computer and the second computer and an "enhanced IPSec protocol" between the first computer and the intermediate computer. IPsec-protected packets are translated by the intermediate computer, without undoing the IPsec processing. This avoids both the overhead of double tunneling and the security problem involved in using separate tunnels.

The translation is performed e.g. by means of a translation table stored at the intermediate computer. The outer IP header address fields and/or the SPI-values are changed by the intermediate computer so that the message can be forwarded to the second computer.

By modifying the translation table and parameters associated to a given translation table entry, the properties of the connection between the first and the intermediate computers can be changed without establishing a new IPsec connection, or involving the second computer in any way.

One example of a change in the SA between the first computer and the intermediate computer is the change of addresses for enabling mobility. This can be accomplished in the invention simply by modifying the translation table entry address fields. Signaling messages may be used to request such a change. Such signalling messages may be authenticated and/or encrypted, or sent in plaintext. One method of doing authentication and/or encryption is to use an IPsec connection between the first computer and the intermediate computer. The second computer is unaware of this IPsec connection, and does not need to participate in the signalling protocol in any way. Several other methods of signalling exist, for instance, the IKE key exchange protocol maybe extended to carry such signalling messages.

In the signalling, e.g. a registration request is sent from the first computer to the intermediate computer which causes the intermediate computer to modify the addresses in

the mapping table and thus, the intermediate computer can identify the mobile next time a message is sent. Preferably, as a result of a registration request, a reply registration is sent from the intermediate computer back to the first computer.

Other examples of possible modifications to the SA—or in general, the packet processing behaviour—between the first computer and the intermediate computer are the following.

One example is the first computer and the intermediate computer performs some sort of retransmission protocol that ensures that the IPSec protected packets are not dropped in the route between the first and the intermediate computer. This may have useful applications when the first computer is connected using a network access method that has a high packet drop rate—for instance, GPRS.

Such a protocol can be easily based on e.g. IPsec sequence number field and the replay protection window, which provide a way to detect that packet(s) have been lost. When a receiving host detects missing packets, it can send a request message for those particular packets. The request can of course be piggy-backed on an existing data packet that is being sent to the other host. Another method of

doing the retransmissions may be based on using an extra protocol inside which the IPSec packets are wrapped for transmission between the first and intermediate computer. In any case, the second computer remains unaware of such a retransmission protocol.

Another example is performing a Network Address Translation (NAT) traversal encapsulation between the first and the intermediate computer. This method could be based on e.g. using UDP encapsulation for transmission of packets between the first and the intermediate computer. The second computer remains unaware about this processing and does not even need to support NAT traversal at all. This is beneficial because there are several existing IPSec products that have no support for NAT traversal.

The system of the invention is a telecommunication network for secure forwarding of messages and comprises at least a first computer, a second computer and an intermediate computer. It is characterized in that the first and the second computers have means to perform IPSec processing, and the intermediate computer have means to perform IPSec translation and possibly key exchange protocol, such as IKE, translation, preferably by means of mapping tables. The intermediate computer may perform IPSec processing

related to other features, such as mobility signalling described above or other enhancements.

The IPSec translation method is independent of the key exchange translation method. Also manual keying can be used instead of automatic keying. If automatic keying is used, any key exchange protocol can be modified for that purpose; however, the idea is to keep the second computer unaware of the interplay of the first and the intermediate computer.

An automatic key exchange protocol may be used in the invention in several ways. The essential idea is that the second computer sees a standard key exchange protocol run, while the first and the intermediate computer perform a modified key exchange. The modified key exchange protocol used between the first and the intermediate computer ensures that the IPsec translation table and other parameters required by the invention are set up as a side-effect of the key exchange protocol. One such modified protocol is presented in the application for the IKE key exchange protocol.

Each translation table consists of entries that are divided into two partitions. The first partition contains information fields related to the connection between the

first computer and the intermediate computer, while the second partition contains information fields related to the connection between the intermediate computer and the second computer.

The translation occurs by identifying the translation table entry by comparing against one partition, and mapping into the other. For traffic that is flowing from the first computer towards the second computer, through the intermediate computer, the entry is found by comparing the received packet against entries in the first partition, and then translating said fields using information found in the second partition of the same entry. For traffic flowing in the opposite direction, the second partition is used for finding the proper translation table entry, and the first partition for translating the packet fields.

The IPSec translation table partitions consist of the following information: the IP local address and the IP remote address (tunnel endpoint addresses) and SPIs for sending and receiving data.

As mentioned, a translation table entry consists of two such partitions, one for communication between first computer and the intermediate computer, and another for

communication between the intermediate computer and the second computer.

The invention described solves the above problems of prior art. The solution is based on giving the first computer, e.g. if it is mobile, an appearance of a standard computer for the second computer. Thus, the second computer will believe it is talking to a standard IPSec host, while the intermediate computer and the second computer will work together using a modified protocol, for instance a slightly modified IPSec and IKE that helps to accomplish this goal. There are, however, several other control protocols that could conceivably be used between the first and the intermediate computer.

In the following, the invention is described more in detail by using figures by means of some embodiment examples to carry out the invention. The invention is not restricted to the details of the figures and accompanying text, or any existing protocols, such as the currently standardised IPSec or IKE.

Especially, the invention can be concerned with other kinds of telecommunication networks wherein the method of the invention can be applied than that of the figures.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates an example of a telecommunication network of the invention.

FIG. 2 describes generally an example of the method of the invention.

FIG. 3 illustrates an example of an IPSec translation table used by the intermediate computer to change the outer IP address and SPI value.

FIG. 4 describes a detailed example of how the SA is formed in the invention.

FIG. 5 illustrates an example of translation tables for the modified key exchange of the invention.

FIG. 6 shows a mapping table for identification values of the user Security Gateway (SGW) addresses.

DETAILED DESCRIPTION OF THE INVENTION

An example of a telecommunication network of the invention is illustrated in FIG. 1, comprising a first computer, here a client computer **1** served by an intermediate computer,

here as a server **2**, and a host computer **4**, that is served by the second computer, here a security gateway (SGW) **3**. The security gateway supports the standard IPSec protocol and optionally the IKE key exchange protocol. The client computer and the server computer support a modified IPSec and IKE protocol.

The invention is not restricted to the topology of FIG. 1. In other embodiments, the first computer may e.g. be a router; or there might e.g. not be a host behind the second computer (in which case the first and the second computer are talking to each other directly), etc.

The IPSec translations taking place in the scenario of FIGS. 1, 2, and **3** are discussed first. The IPSec connections (such as SAs) in the scenario may be established manually, or using some key exchange protocol, such as the Internet Key Exchange (IKE). To illustrate how a key exchange protocol would be used in the scenario of FIG. 1, a modified IKE protocol based on IKE translation is also presented later.

In the invention, an IPSec connection is shared by the first computer and the second computer, while the intermediate computer holds information required to perform

address and IPSec SPI translations for the packets. These translations accomplish the effect of "double tunnelling" (described in the technical background section), but with the method of the invention the confidentiality of the packets is not compromised, while simultaneously having no extra overhead when compared to standard IPSec. The intermediate computer does not know the cryptographic keys used to encrypt and/or authenticate the packets, and can thus not reveal their contents.

The advantage of the invention is that the logical IPSec connection shared by the first and the second computer can be enhanced by the first and the intermediate computer without involvement of the second computer. In particular the so-called "ingress filtering" performed by some routers does not pose any problems when translations of addresses are used. In the example presented, each host also manages its own IPSec SPI space independently.

In the example of FIG. 1, an IPSec connection is formed between the client computer **1** (the first computer) and the security gateway **3** (the second computer). To create an IPSec tunnel, a SA (or usually a SA bundle) is formed between the respective computers with a preceding key exchange. The key exchange between the first and the second

computer can take place manually or it can be performed with an automatic key exchange protocol such as the IKE protocol. For performing said key exchange, a standard IKE protocol is used between the server **2** and the security gateway **3**, and a modified IKE protocol is used between the client computer **1** and the server **2**. An example of a modified IKE protocol that can be used in the invention is described in connection with FIG. 4.

Messages to be sent to the host terminal **4** from the client computer **1** are first sent to the server **2**, wherein an IPSec translation and an IKE translation takes place. After that the message can be sent to the security gateway **3**, which sends the message further in plain text to the host terminal **4**.

The method of the invention, wherein messages in packet form are sent by routing to the end destination, is generally described in connection with FIG. 2. It is assumed in the following description that the IPSec connection between the first and second computer already is formed. The IPSec connection can be set up manually or automatically by e.g. an IKE exchange protocol which is described later.

FIG. 2 illustrates the sequence of events that take place when the first computer, corresponding to the mobile terminal in FIG. 1, sends a packet to a destination host, labelled X in the figure, and when the host X sends a packet to the mobile terminal.

IP packets consist of different parts, such as a data payload and protocol headers. The protocol headers in turn consist of fields.

In step **1** of FIG. 2, the first computer, e.g. a mobile terminal, forms an IP packet that is to be sent to host X. Typically, this packet is created by an application running on the mobile terminal. The IP packet source address is the address of the mobile terminal, while the destination address is host X.

The packet is processed using an IPSec tunnel mode SA, which encapsulates the IP packet securely. The example assumes that IPSec encryption and/or authentication of ESP type is used for processing the-packet, although the invention is not limited to the use of only ESP; instead, an arbitrary IPsec connection may be used.

In said processing, a new IP header is constructed for the packet, with so-called outer IP addresses. The outer source

address of the packet can be the same as the inner IP address—i.e., the address of the mobile terminal—but can be different, if the mobile terminal is visiting a network. The outer source address corresponds to the care of address obtained by the mobile terminal from the visited network, in this case. The outer destination address is the address of the intermediate computer. In addition to the new IP header, an ESP header is added, when using IPSec ESP mode. The SPI field of the ESP header added by the IPSec processing is set to the SPI value that the intermediate computer uses for receiving packets from the mobile terminal. In general, there may be more than one SPI field in a packet.

The processing of packets in the intermediate computer is based on a translation table i.e. an IPSec translation table shown in FIG. 3. The table has been divided into two partitions. The left one, identified by the prefix "c-", refers to the network connection between the first computer (host **1** in FIG. 1) and the intermediate computer (host **2** in FIG. 1). The right one, identified by the prefix "s-", refers to the network connection between the intermediate computer and the second computer (computer **3** in FIG. 1). The postfix number ("-1", "-2", or "-3") identifies the

host in question. Thus, the address fields ("addr") refer to outer addresses of a packet, while the SPI fields ("SPI") refer to the receiver of packets, which packets were sent with this SPI. Thus, "c-SPI-2" is the SPI value used by host **2** (the intermediate computer) when receiving packets from host **1** (the first computer), and the SPI-value "c-SPI-1" is the SPI-value with which the first computer receives messages and the SPI-value with which the intermediate computer sends messages to the first computer and so on.

In terms of FIG. 3, the outer source address would be "c-addr-1" (195.1.2.3), the outer destination address "c-addr-2" (212.90.65.1), while the SPI field would be "c-SPI-2" (0×12341234). The notation 0×NNNNNNNN indicates a 32-bit unsigned integer value, encoded using a hexadecimal notation (base **16**). The inner source address is processed by IPSec in the first computer, and would typically be encrypted. In this example, the inner source address would be the static address of the mobile terminal, e.g. 10.0.0.1.

When the intermediate computer receives the packet sent in step **1** described above, it performs an address and SPI translation, ensuring that the security gateway (host **3** of

FIG. 1) can accept the packet. Most of the packet is secured using IPSec, and since the intermediate computer does not have the cryptographic keys to undo the IPSec processing done by the mobile terminal, it cannot decrypt any encrypted portions of the packet but is able to use the outer IP addresses and the incoming SPI value to determine how to modify the outer address and the SPI to suite the second computer, which is the next destination. SPI is now changed to 0×56785678 in the intermediate computer and the address is changed to the address of the second computer. This is done by means of the IPSec translation table of FIG. 3.

The first row of FIG. 3 is a row that the intermediate computer has found that matches the packet in the example, and thus the intermediate computer chooses it for translation. The new outer source address s-addr-**2** (212.90.65.1) is substituted for the outer source address c-addr-**1** (195.1.2.3), and the new outer destination address s-addr-**3** (103.6.5.4) is substituted for the outer destination address c-addr-**2** (212.90.65.1). The new SPI value, s-SPI-**3** (0×56785678), is substituted for the SPI value c-SPI-**2** (0×12341234). If more than one SPI values are used, all the SPI values are substituted similarly. In the

example, s-addr-**2** and c-addr-**2** happen to be the same on both partitions of the table. This is not necessarily so but the intermediate computer might use another address for sending.

In step **2** of FIG. 2, the translated packet is sent further to the second computer. The inner IP packet has not been modified after that the first computer sent the packet. The second computer processes the packet using standard IPSec algorithms. The security gateway (the second computer) can e.g. decipher and/or check the authenticity of the packet, then remove the IPSec tunnelling, and forward the original packet towards the destination host, X. Thus, the entire original packet was unaffected by the translation as the IP header, and thus the address fields, was covered by IPSec.

After uncovering the original packet from the IPsec tunnel, the second computer makes a routing decision based on the IP header of the original packet. In the example, the IP destination address is X (host X in FIG. 2), and thus the second computer delivers the packet either directly to X, or to the next hop router.

In step **3** of FIG. 2, the packet is sent from the second computer (corresponding to SGW in FIG. 1) to host X, having

now only the original source IP address 10.0.0.1 and the original destination IP address X in the IP header. Thus, in step **3**, host X receives the packet sent by the second computer. Usually, an application process running on host X would generate some return traffic. This would cause an IP packet to be generated and sent to the second computer.

If a packet is sent back from host X to the first computer (corresponding to the client computer in FIG. 1), steps analogous to steps **1-3** are performed. The packet is thus first sent to the second computer, with the source IP address being X and the destination IP address being 10.0.0.1, in step **4**. The generated packet is then received by the second computer. The IPSec policy of the second computer requires that the packet be IPSec-processed using a tunnel mode IPSec SA. This processing is similar to the one in steps **1** and **2**. A new, outer IP header is added to the packet in the second computer, after which the resulting packet is secured using the IPSec SA. The outer IP source address is set to s-addr-**3** (103.6.5.4) while the outer IP destination address is set to s-addr-**2** (212.90.65.1). The SPI field is set to s-SPI-**2** (0×c1230012). In step **5**, the resulting packet is sent to the address indicated by the new outer IP destination

address, s-addr-**2**, the intermediate computer. The intermediate computer receives the packet and performs a similar address and SPI translation.

The inner addresses are still the same, and are not modified by the intermediate computer. Since the packet intended to be sent to the first computer, the new, translated outer destination IP address indicate the address of the first computer.

The resulting packet is sent to the first computer in step **6**.

As a result of step **6**, the packet is received by the first computer. The IPSec processing is undone, i.e. decryption and/or authentication is performed, and the original packet is uncovered from the IPSec tunnel. The original packet is then delivered to the application running on the first computer. In case the first computer acts as a router, the packet may be delivered to a host in a subnet for which the first computer acts as a router.

The first computer may be a mobile terminal, the outer address of which changes from time to time. The translation table is then modified using some form of signalling messages, as described in the summary section. Upon

receiving a request for modifying a translation, the intermediate computer updates the related translation table entry to match the new information supplied by the first computer. The operation of the protocol then proceeds as discussed above.

The above discussion is a limited example for illustration purposes. In other embodiments e.g. more than one SA for the connection—for instance, ESP followed by AH, can be used. This introduces two SPI values that must be translated. More than two is also, of course, possible. Furthermore, the example was considered for IPsec ESP only. The changes required for an embodiment in which AH (or ESP+AH) is used, are discussed next.

Changes for Using AH:

If the Authentication Header (AH) IPSec security transform is to be used, there are more considerations than in the previous example. In particular, modifications of the packet fields—even the outer IP header—are detected if AH is used. Thus, the following nominal processing is required by the first computer. The second computer performs standard IPSec processing also in this case.

In step **1**, when sending a packet, the first computer must perform IPsec processing using the SPI values and addresses used in the connection between the intermediate computer and the second computer. For instance, the SPI value would be s-SPI-**3**, the outer source address s-addr-**2**, and the outer destination address s-addr-**3**. The AH integrity check value (ICV) must be computed using these values. ICV is a value, which authenticates most of the fields of the packet. In practice, all fields that are never modified by routers are authenticated.

After computing the AH integrity check value, the outer addresses and the SPI value are replaced with the values used between the first computer and the intermediate computer: c-addr-**1** for the outer source address, c-addr-**2** for the outer destination address, and c-SPI-**2** for the SPI.

In step **2**, the intermediate computer performs the address and SPI translations as in the example with ESP described above. The resulting packet is identical to the one used by the first computer for the AH integrity check value calculation, except possibly for fields not covered by AH (such as the Time-To-Live field, the header checksum, etc). Thus, the AH integrity check value is now correct.

In step **3**, the second computer performs standard IPSec processing of AH. The packet, which now is uncovered from the tunnel is sent to the host X. As in the previous example, an application in host X usually generates a return packet that is to be sent to the first computer. This packet is sent to the second computer in step **4**.

Upon receiving the packet, the processing of the second computer are the same as in the example with ESP. The second computer computes an AH integrity check value of the tunneled packet it is sending to the mobile terminal. The integrity check value is computed against the outer source address of s-addr-**3**, outer destination address of s-addr-**2**, and the SPI value of s-SPI-**2**.

In step **5**, when the intermediate computer receives the packet, it performs ordinary translation of the packet. The new outer source address is c-addr-**2**, the outer destination address is c-addr-**1**, and the SPI value is c-SPI-**1**. At this point the AH integrity check value is incorrect, which was caused by the translations.

When the mobile terminal receives the packet, it performs a translation of the current outer addresses and the SPI field for the original ones used by the second computer: s-

addr-**3** for the outer source address, s-addr-**2** for the outer destination address, and s-SPI-**2** for the SPI value. This reproduces the packet originally sent by the second computer, except possibly for fields not covered by AH. This operation restores the AH integrity check value to its original, correct value. The AH integrity check is then performed against these fields.

Key Exchange Considerations

The above example discussed the "steady state" IPSec translations performed by the intermediate computer. The IPSec SAs and the IPSec translation table entries may be set up manually, or using some automated protocol, such as the Internet Key Exchange (IKE) protocol.

Because the security gateway (the second computer) is a standard IPSec host, it implements some standard key exchange protocol, such as IKE. The first computer and the intermediate computer may use some modified version of IKE, or any other suitable automatic key exchange protocol.

The key exchange must appear as a standard key exchange according to the key exchange protocol supported by the security gateway (the second computer), such as IKE. Also, the overall key exchange performed by the first,

intermediate, and second computer must establish not only cryptographic keys, but also the IPSec translation table entries. The overall key exchange protocol should not reveal the IPSec cryptographic keys to the intermediate computer to avoid even the potential for security problems.

In the following, an example of a modified IKE protocol is presented to outline the functionality of such a protocol in the context of the invention. The protocol provides the functionality described above. In particular, the intermediate computer has no knowledge of the IPSec cryptographic keys established. The protocol is presented on a general level to simplify the presentation.

The automatic IKE protocol is used prior to other protocols to provide strongly authenticated cryptographic session keys for the IPSec protocols ESP and AH. IKE performs the following functions: (1) security policy negotiation (what algorithms shall be used, lifetimes etc.), (2) a Diffie-Hellman key exchange, and (3) strong user/host authentication (usually using either RSA-based signatures or pre-shared authentication keys). IKE is divided into two phases: phase **1** and phase **2**. Phase **1** negotiates and establishes cryptographic keys for internal use of the IKE protocol itself, and also performs the strong user or host

authentication. Phase **2** negotiates and establishes cryptographic keys for IPSec. If IPSec tunnel mode is used, phase **2** also negotiates the kind of traffic that may be sent using the tunnel (so-called traffic selectors).

The IKE framework supports several "sub-protocols" for phase **1** and phase **2**. The required ones are "main mode" for phase **1**, and "quick mode" for phase **2**. These are used as illustrations, but the invention is not limited to these sub-protocols of IKE.

For the security gateway (second computer), the IKE session seems to be coming from the address s-addr-**2** in FIG. 3. Since there may be any number of mobile terminals served by the intermediate computer, the intermediate computer should either (1) manage a pool of addresses to be used for the s-addr-**2** translation table address, thus providing each user with a separate "surrogate address", or (2) use the same address (or a limited set of addresses), and ensure that the mobile terminals are identified using some other means than their IP address (IKE provides for such identification types, so this is not a problem).

The modified IKE protocol specified is analogous to the IPSec translation table approach. However, instead of SPIs,

the so-called IKE cookies are used as translation indices instead. IKE cookies are essentially IKE session identifiers, and are thus analogous to the IPSec SPI values, which is another form of a session or context identifier. There are two cookies: the initiator cookie, chosen by the host that initiates the IKE session, and the responder cookie, chosen by the host that responds to a session initiation.

The essential features of the protocol are (1) that it appears to be an entirely ordinary IKE key exchange for the security gateway, (2) that the IPsec translation table entry is formed by the intermediate computer during the execution of the protocol, (3) that the first computer obtains all the necessary information for its packet processing, and (4) that the intermediate computer does not obtain the IPsec cryptographic session keys.

The overall steps of the protocol are:

- 1. The first computer initiates the key exchange protocol by sending a message to the intermediate computer. This message is essentially the IKE

main mode initiation message, with some modifications required for this application.

- 2. The intermediate computer determines which security gateway (second computer) to forward this IKE session to, and also establishes a preliminary IKE translation table entry based on the information available from the message.
- 3. The security gateway (the second computer) replies to the IKE main mode initiation message.
- 4. The intermediate computer completes the IKE mapping based on the reply message.
- 5. The modified IKE protocol run continues through IKE main mode (the phase **1** exchange), which is followed by quick mode (the phase **2** exchange). Extensions of standard IKE messages are used between the first computer and the intermediate computer to accomplish the extra goals required by this modified IKE protocol.

In FIG. 4, the IKE session is described message by message. The following text indicates the contents of each message, and how they are processed by the various hosts. There are six main mode messages in the protocol, named mm**1**, mm**2**, . .

. , mm**6**, and three quick mode messages, named qm**1**, qm**2**, and qm**3**.

FIG. 5 illustrates the IKE translation table entry related to the modified IKE key exchange being performed. The bolded entries in each step are added or changed in that step as a result of the processing described in the text.

The IKE translation table partition for the connection between the first computer and the intermediate computer is as follows (the field name in FIG. 5 is given in parentheses):

Local and remote IP address (c-addr-**1**, c-addr-**2**)

Initiator and responder cookie (c-icky, c-rcky)

IKE identification of the first computer (c-userid, e.g. joe@netseal.com)

The IKE translation table partition for the connection between the intermediate computer and the second computer is as follows (the field name in FIG. 5 is given in parentheses):

Local and remote IP address (s-addr-**2**, s-addr-**3**)

Initiator cookie and responder cookie (s-icky, s-rcky)

In addition to these entries, other data may be kept by the intermediate computer and/or the first computer.

The key exchange is initiated by generating an initiator cookie and sending a zero responder cookie to the second computer. A responder cookie is generated in the second computer and a mapping between IP addresses and IKE cookie values in the intermediate computer is established. A translation table to modify IKE packets in flight by modifying the external IP addresses and possibly IKE cookies of the IKE packets is used.

Either the modified IKE protocol between the first computer and the intermediate computer is modified such that the IKE keys are transmitted from the first computer to the intermediate computer for decryption and modification of IKE packets or, alternatively, the modified IKE protocol between the first computer and the intermediate computer is modified such that the IKE keys are not transmitted from the first computer to the intermediate computer for decryption and modification of IKE packets, and the modification of IKE packets is done by the first computer with the intermediate computer requesting such modifications. The latter alternative is discussed in the

example that follows, since it is more secure than the first alternative.

Extra information, such as user information and SPI change requests, to be sent between the first and the intermediate computer, is sent by appending the extra information to the standard IKE messages. The IKE standard has message encoding rules that indicate a definite length, thus the added extra information can be separated from the IKE message itself. The extra information fields are preferably encrypted and authenticated, for instance by using a secret shared by the first computer and the intermediate computer. The details of this process are not relevant to the invention.

The extra information slot in each IKE message is called the message "tail" in the following.

IKE messages consist of an IKE header, which includes the cookie fields and message ID field, and of a list of payloads. A payload has a type, and associated information.

FIG. 4 considers an example of the routing of packets according to the invention considering IPSec security association set-up for distribution of keys. As in the foregoing FIG. 2, the session begins with sending a packet

from the client (first computer) to the server (intermediate computer).

The key exchange is initiated by the first computer. Thus, in step **1** of FIG. 4, the first computer constructs mm**1**. The IP header of the message contains the following values:

- IP source address: 195.1.2.3 (c-addr-**1**)
- IP destination address: 212.90.65.1 (c-addr-**2**)

The IKE header contains the following values (step **1** in Figure X):

- Initiator cookie: CKY**1** (c-icky)
- Responder cookie: **0** (c-rcky)
- Message ID: **0**

The message contains the following payloads:

- A Security Association (SA) payload, which contains the IKE phase **1** security policy offers from the first computer.

- The message may contain additional payloads, such as Vendor Identification (VID) payloads, certificate requests/responses, etc.
- A VID payload can be used to indicate that the first computer supports the protocol described here.

The message tail contains the following information:

- User identification type and value—the c-userid field. These are used by the intermediate computer to choose a security gateway to forward this session to. The identification type may be any of the IKE types, but additional types can be defined. An alternative to this field is to directly indicate the security gateway for forwarding. There are other alternatives as well, but these are not essential to the invention.

In step **2**, the mm**1** is received by the intermediate computer. The intermediate computer examines the message, and forms the preliminary IKE translation table entry. FIG. 5, step **1** illustrates the contents of this preliminary entry. The c-userid field is sent in the mm**1** tail.

The intermediate computer then determines which security gateway to forward this IKE session to. The determination may be based on any available information, static configuration, load balancing, or availability requirements. The presented, simple method is to use the identification information in the mm**1** tail to look up the first matching identification type and value from a table. An example of such a table is presented in FIG. 6.

The identification mapping table of FIG. 6, is one method for choosing a security gateway that matches the incoming mobile terminal. The identification table would in this example be an ordered list of identification type/value entries, that match to a given security gateway address. When the incoming mobile terminal identification matches the identification in the table, the corresponding security gateway is used. For instance, john.smith@netseal.com would match the first row of the table, i.e., the security gateway 123.1.2.3, while joe@netseal.com matches the second row, i.e., the security gateway 103.6.5.4. The identification types include any identification types defined for the IKE protocol, and may contain other types as well, such as employee numbers, etc.

Other methods of determining the security gateway to be used may be employed. One such method is for the mobile terminal to directly indicate a given security gateway to be used. The mobile terminal may also indicate a group of security gateways, one of which is used. The exact details are not relevant to the invention.

In addition to determining the security gateway address, the intermediate computer determines which address its for communication between itself and the second computer. The same address as is used for the communication between the first and the intermediate computer may be used, but a new address may also be used. The address can be determined using a table similar to the one in FIG. 6, or the table of FIG. 6 may be extended to include this address.

The intermediate computer then generates its own initiator cookie. This is done to keep the two session identifier spaces entirely separate, although the same initiator cookie may be passed as is.

After these determinations, the preliminary translation table entry is modified. FIG. 5, step **2** illustrates the contents of the entry at this point.

The original IP header fields are modified as follows (step **2** in FIG. 4):

- IP source address: 212.90.65.1 (s-addr-**2**)
- IP destination address: 103.6.5.4 (s-addr-**3**)

The IKE header is modified as follows:

- Initiator cookie: CKY**2** (s-icky)
- Responder cookie: **0** (s-rcky)
- Message ID: **0**

The message tail is removed. The VID payload that identifies support for this modified protocol is also removed. The mm**1** is then forwarded to the second computer.

In step **3**, the second computer responds with mm**2**. The IP header of the message contains the following values (step **3** in FIG. 4):

- IP source address: 103.6.5.4 (s-addr-**3**)
- IP destination address: 212.90.65.1 (s-addr-**2**)

The IKE header contains the following values:

- Initiator cookie: CKY**2** (s-icky)
- Responder cookie: CKY**3** (s-rcky)
- Message ID: **0**

The message contains the following payloads:

- Security Association (SA) payload. This is a reply to the offer by the first computer, and indicates which security configuration is acceptable for the second computer (this scenario assumes success, so the case of an error reply is not considered).
- Possibly optional IKE payloads, such as VID payloads, certificate requests/replies, etc.

There is no message tail.

In step **4**, the mm**2** is received by the intermediate computer. The intermediate computer updates its IKE translation table based on the received message. Step **3** in

FIG. 5 illustrates the contents of the translation table entry at this point.

The intermediate computer generates its own responder cookie, CKY**4**, and updates the translation table yet again. Step **4** in FIG. 5 illustrates the entry at this point. After this step, the translation table entry is complete, and the address and cookie translations are performed as in steps **1-4** for the following messages.

The translated message contains the following IP header fields (FIG. 4, step **4**)

- IP source address: 212.90.65.1 (c-addr-**2**)
- IP destination address: 195.1.2.3 (c-addr-**1**)

The translated IKE header contains the following fields:

- Initiator cookie: CKY**1** (c-icky)
- Responder cookie: CKY**4** (c-rcky)

The message contains the following payloads:

- The SA payload sent by the second computer.
- Any optional payloads sent by the second computer.
- A VID payload may be added to indicate support of this modified protocol to the first computer.

A message tail is added, and contains the following information:

- Address and/or identification information of the chosen security gateway (the second computer). This information can be used by the client to choose proper authentication information, such as RSA keys.

The message is then forwarded to the first computer.

In step **5**, the first computer constructs mm**3**. The message contains the following payloads:

- A Key Exchange (KE) payload, that contains Diffie-Hellman key exchange data of the first computer.

- A Nonce (NONCE) payload, that contains a random number chosen by the first computer.
- Possibly optional IKE payloads.

The message is sent to the intermediate computer.

In step **6**, the mm**3** is forwarded to the second computer. The contents of the message are not changed, only the IP header addresses and the IKE cookies, in the manner described in steps **1-4**.

In step **7**, the second computer receives mm**3** and responds with mm**4**. The message contains the following payloads:

- A Key Exchange (KE) payload, that contains Diffie-Hellman key exchange data of the second computer.
- A Nonce (NONCE) payload, that contains a random number chosen by the second computer.
- Possibly optional IKE payloads.

In step **8**, the mm**4** is forwarded to the first computer.

In step **9**, the first computer constructs mm**5**, which is the first encrypted message in the session. All subsequent

messages are encrypted using the IKE session keys established from the previous Diffie-Hellman key exchange (the messages mm**3** and mm**4**) by means of hash operations, as described in the IKE specification. Note that the intermediate computer does not possess these keys, and can thus not examine the contents of any subsequent IKE messages. In fact, the intermediate computer has no advantage compared to a hostile attacker if it attempts to decipher the IKE traffic. Instead, the intermediate computer indirectly modifies some fields in the IKE messages by sending a modification request in the IKE message tail to the first computer, which does the requested modifications before IKE encryption processing.

The message contains the following payloads:

- An Identification (ID) payload, that identifies the first computer to the second computer. This identification may be the same as the identification sent in the mm**1** tail, but may differ from that. These two identifications serve different purposes: the mm**1** tail identification (c-userid) is used to select a security gateway

for IKE session forwarding (the second computer), while the ID payload in this message is used by the second computer for IKE authentication purposes, for instance, to select proper RSA authentication keys.

- A Signature (SIG) or Hash (HASH) payload, that serves as an authenticator. A signature payload is used if RSA- or DSS-based authentication is used, while a hash payload is used for pre-shared key authentication. There are other authentication methods in IKE, and IKE can also be extended with new authentication methods. These are not essential to the invention, and the following text assumes RSA authentication (i.e., use of the signature payload).
- Possibly optional IKE payloads.

The message tail contains the-following information:

- The SPI value that the first computer wants to use for receiving IPsec-protected messages from the intermediate computer, i.e., the c-SPI-**1** value of the IPsec translation table in FIG. 3.

More than one SPI value could be transmitted here, but for simplicity, the following discussion assumes that only a single SPI is necessary (i.e. only one SA is applied for IPsec traffic processing). Extending the scheme to multiple SPIs is straightforward.

In step **10**, the mm**5** is forwarded to the second computer.

The intermediate computer removes the message tail, and performs the IKE translation discussed previously, and then forwards the message to the second computer.

In step **11**, the second computer receives the mm**5** message, and authenticates the user (or the host, depending on what identification type is used). Assuming that the authentication succeeds, the second computer proceeds to authenticate itself to the first computer.

The mm**6** message contains the following payloads:

- An Identification (ID) payload, that identifies the second computer to the first computer.
- A Signature (SIG) payload (here RSA authentication is assumed).

- Possibly optional IKE payloads.

In step **12**, the mm**6** is received by the intermediate computer. The intermediate computer does not change the message itself, but adds a tail with the following information:

- The SPI value that the intermediate computer wants the first computer to offer to the second computer in the qm**1** message. Since the intermediate computer cannot access the contents of the IKE messages, this modification request is made using the message tail (see the discussion of step **9**). The SPI value sent matches the s-SPI-**2** field of the IPsec translation table of FIG. 3.
- The SPI value that the intermediate computer wants the first computer to use for messages sent to itself. This matches the c-SPI-**2** field of the IPsec translation table of FIG. 3.

The resulting message is forwarded to the first computer.

In step **13**, the first computer constructs qm**1**, which contains the following IKE payloads:

- A Hash (HASH) payload, that serves as an authenticator of the message.
- A Security Association (SA) payload, which contains the IKE phase **2** security policy offers from the first computer, i.e., the IPsec security policy offers. The SA payload contains the SPI value assigned to the first computer in the mm**6** message, i.e., s-SPI-**2** in FIG. 3.
- Optionally, a Key Exchange (KE) payload, if a new Diffie-Hellman key exchange is to be performed in phase **2** (this depends on the contents of the SA payload).
- A Nonce (NONCE) payload, which contains a random value chosen by the first computer.
- Optionally, two Identification (ID) payloads that indicate the IPsec traffic selectors that the first computer proposes for an IPsec tunnel mode SA. If IPsec transport mode is used, these are not necessary, but they may still be used. They may also be omitted if IPsec tunnel mode is used.

The IKE header is the same as previously, except that the Message ID field now contains a non-zero 32-bit value, that

serves as a phase **2** session identifier. This identifier remains constant for the entire quick mode exchange.

The message is sent to the intermediate computer.

In step **14**, the intermediate computer forwards the qm**1** message to the second computer.

In step **15**, the second computer inspects the security policy offers and other information contained in the qm**1** message, and determines which security policy offer matches its own security policy (the case when no security policies match results in an error notification message).

The second computer responds with qm**2** message that contains the following payloads:

- A Hash (HASH) payload, that serves as an authenticator of the message.
- A Security Association (SA) payload, which indicates the security policy offer chosen by the second computer. The message also contains the SPI value that the second computer wants to use when receiving IPsec-protected messages. The SPI

value matches s-SPI-**3** of the IPsec translation table in FIG. 3.

- Optionally, a Key Exchange (KE) payload, if a new Diffie-Hellman key exchange is to be performed in phase **2**.
- A Nonce (NONCE) payload, which contains a random value chosen by the second computer.
- If Identification (ID) payloads were sent by the first computer, the second computer also sends Identification payloads.

In step **16**, the intermediate computer forwards the qm**2** message to the first computer.

In step **17**, the first computer constructs qm**3** message, which contains the following payloads:

- A Hash (HASH) payload, that serves as an authenticator of the message.

The following information is sent in the message tail:

- The SPI value sent by the second computer in the qm**2** message. This is sent here, because the intermediate computer cannot decrypt the qm**2** message and look up the SPI from there. The SPI value matches s-SPI-**3** of the IPsec translation table in FIG. 3.

In step **18**, the intermediate computer receives the qm**3** and reads the s-SPI-**3** value from the message tail. All the information required to construct the IPsec translation table entry is now gathered, and the entry can be added to the translation table. In particular, the information fields are as follows:

- c-addr-**1**: same as c-addr-**1** of the IKE session (195.1.2.3).
- c-addr-**2**: same as c-addr-**2** of the IKE session (212.90.65.1).
- c-SPI-**1**: received in the mm**5** message tail from the first computer.
- c-SPI-**2**: chosen by the intermediate computer, sent to the first computer in the mm**6** message tail.

- s-addr-**2**: same as s-addr-**2** of the IKE session (212.90.65.1 in this example, may be different than c-addr-**2**).
- s-addr-**3**: same as s-addr-**3** of the IKE session (103.6.5.4).
- s-SPI-**2**: chosen by the intermediate computer, sent to the first computer in mm**6** message tail.
- s-SPI-**3**: sent by the second computer in qm**2** to the first computer, which sends it to the intermediate computer in qm**3** message tail.

The intermediate computer forwards the qm**3** message to the second computer, which completes the IKE key exchange, and the IPsec translation table set up.

The IPsec cryptographic keys established using the modified IKE key exchange presented above are either derived from the Diffie-Hellman key exchange performed in IKE main mode, or from the (optional) Diffie-Hellman key exchange performed in quick mode. In both cases, the intermediate computer has no access to the shared secret established using the Diffie-Hellman algorithm. In fact, the intermediate computer has no advantage when compared to a random, hostile attacker.

The above presentation was simplified and exemplified to increase clarity of the presentation. There are several issues not discussed, but these issues are not essential to the invention.

Some of these issues are the following:

- The phase **1** used main mode. Any other IKE phase **1** exchange can be used; this changes the details of the protocol but not the essential ideas.
- There are other approaches than the one presented here. One approach is for the first computer to reveal the IKE keys to the intermediate computer, so that the second computer is able to modify the required fields of the message (namely, SPI values).
- The discussion assumes that the first computer initiates the IKE exchange. The opposite direction is possible, too, but requires more considerations.
- The commit bit feature of IKE is not used. Adding that is simple.

- Security gateway selection is based on a table lookup indexed by an identification type/value pair sent by the first computer. Other mechanisms are easy to implement.
- The discussion assumes a successful IKE key exchange. Error cases are easy to handle.
- Phase **1** policy lookup (when processing mm**1** and mm**2** messages) is not based on the identity of the IKE counterpart. This is not a major issue, since the phase **1** security policy can be independent of the counterpart without limiting usability.
- Phase **1** is a pre-requisite for executing the protocol in the example. This can be easily changed by moving some of the "tail" items to phase **2**.
- The protocol establishes a pair of SAs, one for each direction, and manages the SPI value modifications of these SAs. It is easy to extend this to cover SA bundles with more than one SA, i.e., SAs applied in sequence (ESP followed by AH, for instance). This requires more than one SPI for each direction, but is easy to add to the protocol described.

The invention is not concerned with the details of the key exchange protocol. The presented outline for one such protocol is given as an example, several other alternatives exist. The invention is also not concerned with the IKE key exchange protocol: other key exchange protocols exist, and similar ideas can be applied in using them in the content of the invention.

While the present invention has been described in accordance with preferred compositions and embodiments, it is to be understood that certain substitutions and alterations may be made thereto without departing from the spirit and scope of the following claims.

We claim:

1. (New) An intermediate computer for secure forwarding of messages in a telecommunication network, comprising:

an intermediate computer configured to connect to a telecommunication network;

the intermediate computer configured to be assigned with a first network address in the telecommunication network;

the intermediate computer configured to receive from a mobile computer a secure message sent to the first network address having an encrypted data payload of a message and a unique identity;

the intermediate computer configured to read the unique identity from the secure message sent to the first network address; and

the intermediate computer configured to access a translation table, to find a destination address from the translation table using the unique identity, and

to forward the encrypted data payload to the destination address using a network address of the intermediate computer as a source address of a forwarded message containing the encrypted data payload.

2. (New) The intermediate computer of claim 1, wherein the intermediate computer is further configured to substitute the unique identity read from the secure message with

another unique identity prior to forwarding the encrypted data payload.

3. (New) The intermediate computer of claim 1, wherein the translation table is stored at the intermediate computer.

4. (New) The intermediate computer of claim 1, wherein the translation table includes two partitions, the first partition containing information fields related to the connection over which the secure message is sent to the first network address, the second partition containing information fields related to the connection over which the forwarded encrypted data payload is sent to the destination address.

5. (New) The intermediate computer of claim 1, wherein the intermediate computer is not configured to access cryptographic keys used to encrypt or authenticate the messages.

6. (New) The intermediate computer of claim 1, wherein the intermediate computer is configured to forward the encrypted data payload using SSL or TLS protocol.

7. (New) The intermediate computer of claim 1, wherein the intermediate computer is configured to receive secure

messages using SSL or TLS protocol.

8. (New) The intermediate computer of claim 1, wherein the unique identity read from the secure message includes one or more Security Parameter Index values.

9. (New) The intermediate computer of claim 1, wherein the intermediate computer is configured to modify the translation table entry address fields in response to a signaling message sent from the mobile computer when the mobile computer changes its address such that the intermediate computer can know that the address of the mobile computer is changed.

10. (New) The intermediate computer of claim 1, wherein the intermediate computer is a server.

11. (New) The intermediate computer of claim 1, wherein the source address of the forwarded message is the same as the first network address.

12. (New) A computer for sending secure messages, and for enabling secure forwarding of messages in a telecommunication network by an intermediate computer to a recipient computer, comprising:
a computer configured to connect to a telecommunication

network;

the computer configured to be assigned with a network address in the telecommunication network, wherein the computer is a mobile computer in that the address of the mobile computer changes;

the computer configured to form a secure message by encrypting the data payload of a message and giving the message a unique identity and a destination address of an intermediate computer, wherein the unique identity and the destination address are capable of being used by the intermediate computer to find an address to a recipient computer;

the computer configured to send the secure message to the intermediate computer for forwarding of the encrypted data payload to the recipient computer; and

the computer configured to set up a secure connection using a key exchange protocol.

13. (New) The computer of claim 12, wherein the computer is configured to form the secure message using a message received by the computer.

14. (New) The computer of claim 12, wherein the computer is configured to encapsulate the message in an outer IP header.

15. (New) The computer of claim 12, wherein the computer is

configured to form secure messages using IPSec protocols.

16. (New) The computer of claim 12, wherein the computer is configured to form secure messages containing data payload of a message, an inner IP header containing actual sender and receiver addresses, an outer IP header containing the addresses of the computer and the intermediate computer, and a unique identity.

17. (New) The computer of claim 12, wherein the unique identity is one or more Security Parameter Index values.

18. (New) The computer of claim 12, wherein the computer is configured to send a signaling message to the intermediate computer when the computer changes its address such that the intermediate computer can know that the address of the computer is changed.

19. (New) The computer of claim 18, wherein the computer is configured to send the signaling message encrypted.

20. (New) The computer of claim 19, wherein the computer is configured to send the signaling message authenticated.

21. (New) The computer of claim 12, wherein the computer is

configured to send the secure message using SSL or TLS protocol.

Abstract of Disclosure

The method and system enable secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network. A message is formed in the first computer or in a computer that is served by the first computer, and in the latter case, sending the message to the first computer. In the first computer, a secure message is then formed by giving the message a unique identity and a destination address. The message is sent from the first computer to the intermediate computer after which the destination address and the unique identity are used to find an address to the second computer. The current destination address is substituted with the found address to the second computer, and the unique identity is substituted with another unique identity. Then the message is forwarded to the second computer.

Attorney Ref. No. 664.1078CON2 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Sami Vaarala, Antti Nuopponen

Serial No. 15/372,208

Filed: 7 December 2016

For: METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION

Date: 8 December 2016

Confirmation No. 6275

CERTIFICATE OF MAILING

I HEREBY CERTIFY THAT THIS PAPER AND THE DOCUMENTS REFERRED TO AS BEING ATTACHED OR ENCLOSED HEREWITH ARE BEING FORWARDED TO THE COMMISSIONER FOR PATENTS, UNITED STATES PATENT OFFICE ELECTRONICALLY ON December 8, 2016

/rfasth/
Rolf Fasth
Attorney for Applicant

TRANSMITTAL LETTER

ELECTRONIC SUBMISSION

COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

Enclosed for filing in the above-referenced application are the following:

(X) Marked-up copy of Specification
(X) The Commissioner is hereby authorized to charge any additional fees which may be required in connection with the filing of this correspondence, or credit over-payment, to Account No. 06-0243.

Respectfully submitted,

FASTH LAW OFFICES

/rfasth/

Rolf Fasth
Registration No. 36,999

FASTH LAW OFFICES
1206 Stanridge Drive
Raleigh, North Carolina 27613-7063 USA
Tel: +1-910-687-0001
Fax: +1-919-882-1265

Attorney Ref. No. 664.1078CON2

Electronic Acknowledgement Receipt

EFS ID:	27731904
Application Number:	15372208
International Application Number:	
Confirmation Number:	6275
Title of Invention:	METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION
First Named Inventor/Applicant Name:	Sami Vaarala
Customer Number:	33369
Filer:	Rolf Fasth/Sloan Smith
Filer Authorized By:	Rolf Fasth
Attorney Docket Number:	664.1078CON2
Receipt Date:	08-DEC-2016
Filing Date:	
Time Stamp:	11:18:55
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	MARKED_UP.pdf	14018487 468c27790255fd593c6c68d13dac767520590284	no	76

Warnings:

Information:					
2	Miscellaneous Incoming Letter	TRX.pdf	237037 340481c751220a56f733b97129f9a994ad913af0	no	1
Warnings:					
Information:					
			Total Files Size (in bytes):	14255524	

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

PTO/AIA/15 (03-13)
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.	664.1078CON2
First Named Inventor	Sami Vaarala
Title	METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONN
Express Mail Label No.	Electronic Submission

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

1. ☐ **Fee Transmittal Form** (PTO/SB/17 or equivalent)
2. ☐ **Applicant asserts small entity status.** See 37 CFR 1.27
3. ☐ **Applicant certifies micro entity status.** See 37 CFR 1.29. Applicant must attach form PTO/SB/15A or B or equivalent.
4. ☑ **Specification** [*Total Pages* 76] Both the claims and abstract must start on a new page. *(See MPEP § 608.01(a) for information on the preferred arrangement)*
5. ☑ **Drawing(s)** (35 U.S.C. 113) [*Total Sheets* 6]
6. **Inventor's Oath or Declaration** [*Total Pages*] *(including substitute statements under 37 CFR 1.64 and assignments serving as an oath or declaration under 37 CFR 1.63(e))*
   a. ☐ Newly executed (original or copy)
   b. ☐ A copy from a prior application (37 CFR 1.63(d))
7. ☑ **Application Data Sheet** ** See note below.* See 37 CFR 1.76 (PTO/AIA/14 or equivalent)
8. **CD-ROM or CD-R** in duplicate, large table, or Computer Program (*Appendix*)
   ☐ Landscape Table on CD
9. **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 PAPERS

10. ☐ **Assignment Papers** (cover sheet & document(s))
    Name of Assignee
11. ☐ **37 CFR 3.73(c) Statement** (*when there is an assignee*) ☐ **Power of Attorney**
12. ☐ **English Translation Document** (*if applicable*)
13. ☐ **Information Disclosure Statement** (PTO/SB/08 or PTO-1449)
    ☐ Copies of citations attached
14. ☐ **Preliminary Amendment**
15. ☐ **Return Receipt Postcard** (*MPEP § 503*) (*Should be specifically itemized*)
16. ☐ **Certified Copy of Priority Document(s)** (*if foreign priority is claimed*)
17. ☐ **Nonpublication Request** Under 35 U.S.C. 122(b)(2)(B)(i). Applicant must attach form PTO/SB/35 or equivalent.
18. ☑ **Other:** UNSIGNED Inventors' Oath or Declaration
    Power of Attorney

Note*: (1) Benefit claims under 37 CFR 1.78 and foreign priority claims under 1.55 **must be included in an Application Data Sheet (ADS).
(2) For applications filed under 35 U.S.C. 111, the application must contain an ADS specifying the applicant if the applicant is an assignee, person to whom the inventor is under an obligation to assign, or person who otherwise shows sufficient proprietary interest in the matter. See 37 CFR 1.46(b).

19. CORRESPONDENCE ADDRESS

☑ The address associated with Customer Number: 33368 **OR** ☐ Correspondence address below

Name					
Address					
City		State		Zip Code	
Country		Telephone		Email	

Signature	/rfasth/	Date	7 December 2016
Name (Print/Type)	Rolf Fasth	Registration No. (Attorney/Agent)	36999

This collection of information is required by 37 CFR 1.53(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

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.

Abstract of Disclosure

The method and system enable secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network. A message is formed in the first computer or in a computer that is served by the first computer, and in the latter case, sending the message to the first computer. In the first computer, a secure message is then formed by giving the message a unique identity and a destination address. The message is sent from the first computer to the intermediate computer after which the destination address and the unique identity are used to find an address to the second computer. The current destination address is substituted with the found address to the second computer, and the unique identity is substituted with another unique identity. Then the message is forwarded to the second computer.

We claim:

1. (New) An intermediate computer for secure forwarding of messages in a telecommunication network, comprising:

an intermediate computer configured to connect to a telecommunication network;

the intermediate computer configured to be assigned with a first network address in the telecommunication network;

the intermediate computer configured to receive from a mobile computer a secure message sent to the first network address having an encrypted data payload of a message and a unique identity;

the intermediate computer configured to read the unique identity from the secure message sent to the first network address; and

the intermediate computer configured to access a translation table, to find a destination address from the translation table using the unique identity, and

to forward the encrypted data payload to the destination address using a network address of the intermediate computer as a source address of a forwarded message containing the encrypted data payload.

2. (New) The intermediate computer of claim 1, wherein the intermediate computer is further configured to substitute the unique identity read from the secure message with

another unique identity prior to forwarding the encrypted data payload.

3. (New) The intermediate computer of claim 1, wherein the translation table is stored at the intermediate computer.

4. (New) The intermediate computer of claim 1, wherein the translation table includes two partitions, the first partition containing information fields related to the connection over which the secure message is sent to the first network address, the second partition containing information fields related to the connection over which the forwarded encrypted data payload is sent to the destination address.

5. (New) The intermediate computer of claim 1, wherein the intermediate computer is not configured to access cryptographic keys used to encrypt or authenticate the messages.

6. (New) The intermediate computer of claim 1, wherein the intermediate computer is configured to forward the encrypted data payload using SSL or TLS protocol.

7. (New) The intermediate computer of claim 1, wherein the intermediate computer is configured to receive secure

messages using SSL or TLS protocol.

8. (New) The intermediate computer of claim 1, wherein the unique identity read from the secure message includes one or more Security Parameter Index values.

9. (New) The intermediate computer of claim 1, wherein the intermediate computer is configured to modify the translation table entry address fields in response to a signaling message sent from the mobile computer when the mobile computer changes its address such that the intermediate computer can know that the address of the mobile computer is changed.

10. (New) The intermediate computer of claim 1, wherein the intermediate computer is a server.

11. (New) The intermediate computer of claim 1, wherein the source address of the forwarded message is the same as the first network address.

12. (New) A computer for sending secure messages, and for enabling secure forwarding of messages in a telecommunication network by an intermediate computer to a recipient computer, comprising:
a computer configured to connect to a telecommunication

network;

the computer configured to be assigned with a network address in the telecommunication network, wherein the computer is a mobile computer in that the address of the mobile computer changes;

the computer configured to form a secure message by encrypting the data payload of a message and giving the message a unique identity and a destination address of an intermediate computer, wherein the unique identity and the destination address are capable of being used by the intermediate computer to find an address to a recipient computer;

the computer configured to send the secure message to the intermediate computer for forwarding of the encrypted data payload to the recipient computer; and

the computer configured to set up a secure connection using a key exchange protocol.

13. (New) The computer of claim 12, wherein the computer is configured to form the secure message using a message received by the computer.

14. (New) The computer of claim 12, wherein the computer is configured to encapsulate the message in an outer IP header.

15. (New) The computer of claim 12, wherein the computer is

configured to form secure messages using IPSec protocols.

16. (New) The computer of claim 12, wherein the computer is configured to form secure messages containing data payload of a message, an inner IP header containing actual sender and receiver addresses, an outer IP header containing the addresses of the computer and the intermediate computer, and a unique identity.

17. (New) The computer of claim 12, wherein the unique identity is one or more Security Parameter Index values.

18. (New) The computer of claim 12, wherein the computer is configured to send a signaling message to the intermediate computer when the computer changes its address such that the intermediate computer can know that the address of the computer is changed.

19. (New) The computer of claim 18, wherein the computer is configured to send the signaling message encrypted.

20. (New) The computer of claim 19, wherein the computer is configured to send the signaling message authenticated.

21. (New) The computer of claim 12, wherein the computer is

configured to send the secure message using SSL or TLS protocol.

METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION

PRIOR APPLICATIONS

This application is a U.S. Continuation Patent Application based on U.S. Continuation Patent Application No. 13/685,544, filed 26 November 2012 that claims priority from US Patent Application Serial No. 10/500,930, filed 19 October 2005, which claims priority from PCT/FI03/00045, filed 21 January 2003, that claims priority from Finnish Pat. App. No. 20020112, filed 22 January 2002.

TECHNICAL FIELD

The method and system of the invention are intended to secure connections in telecommunication networks. Especially, it is meant for wireless Internet Service Provider (ISP) connections.

TECHNICAL BACKGROUND

An internetwork is a collection of individual networks connected with intermediate networking devices that function as a single large network. Different networks can be interconnected by routers and other networking devices to create an internetwork.

A local area network (LAN) is a data network that covers a relatively small geographic area. It typically connects workstations, personal computers, printers and other devices. A wide area network (WAN) is a data communication network that covers a relatively broad geographic area. Wide area networks (WANS) interconnect LANs across normal telephone lines and, for instance, optical networks; thereby interconnecting geographically disposed users.

There is a need to protect data and resources from disclosure, to guarantee the authenticity of data, and to protect systems from network based attacks. More in detail, there is a need for confidentiality (protecting the contents of data from being read) integrity (protecting the data from being modified, which is a property that is independent of confidentiality), authentication (obtaining assurance about she actual sender of data), replay protection (guaranteeing that data is fresh, and not a copy of previously sent data), identity protection (keeping the identities of parties exchanging data secret from outsiders), high availability, i.e. denial-of-service protection (ensuring that the system functions even when under attack) and access control. IPSec is a technology providing most of these, but not all of them. (In

particulars identity protection is not completely handled by IPSec, and neither is denial-of-service protection.)

The IP security protocols (IPSec) provides the capability to secure communications between arbitrary hosts, e.g. across a LAN, across private and public wide area networks (WANs) and across the internet IPSec can be used in different ways, such as for building secure virtual private networks, to gain a secure access to a company network, or to secure communication with other organisations, ensuring authentication and confidentiality and providing a key exchange mechanism. IPSec ensures confidentiality integrity, authentication, replay protection, limited traffic flow confidentiality, limited identity protection, and access control based on authenticated identities. Even if some applications already have built in security protocols, the use of IPSec further enhances the security.

IPSec can encrypt and/or authenticate traffic at IP level. Traffic going in to a WAN is typically compressed and encrypted and traffic coming from a WAN is decrypted and decompressed. IPSec is defined by certain documents, which contain rules for the IPSec architecture. The documents that define IPSec, are, for the time being, the Request For

Comments (RFC) series of the Internet Engineering Task Force (IETF), in particular, RFCs 2401-2412.

Two protocols are used to provide security at the IP layer; an authentication protocol designated by the header of the protocol, Authentication Header (AH), and a combined encryption/authentication protocol designated by the format of the packet for that protocol, Encapsulating Security Payload (ESP) AH and ESP are however similar protocols, both operating by adding a protocol header. Both AH and ESP are vehicles for access control based on the distribution of cryptographic keys and the management of traffic flows related to these security protocols.

Security association (SA) is a key concept in the authentication and the confidentiality mechanisms for IP. A security association is a one-way relationship between a sender and a receiver that offers security services to the traffic carried on it if a secure two-way relationship is needed, then two security associations are required. If ESP and AH are combined, or if ESP and/or AH are applied more than once, the term SA bundle is used, meaning that two or more SAs are used. Thus, SA bundle refers to one or more SAs applied in sequence, e.g. by first performing an ESP

protection, and then an AH protection. The SA bundle is the combination of all SAs used to secure a packet.

The term IPsec connection is used in what follows in place of an IPSec bundle of one or more security associations, or a pair of IPSec bundles—one bundle for each direction—of one or more security associations. This term thus covers both unidirectional and bi-directional traffic protection. There is no implication of symmetry of the directions, i.e., the algorithms and IPSec transforms used for each direction may be different.

A security association is uniquely identified by three parameters. The first one, the Security Parameters Index (SPI), is a bit string assigned to this SA The SPI is carried in AH and ESP headers to enable the receiving system to select the SA under which a received packet will be processed. IP destination address is the second parameter, which is the address of the destination end point of the SA, which may be an end user system or a network system such as a firewall or a router. The third parameter, the security protocol identifier indicates whether the association is an AH or ESP security association.

In each IPSec implementation, there is a nominal security association data base (SADB) that defines the parameters associated with each SA. A security association is normally defined by the following parameters. The Sequence Number Counter is a 32-bit value used to generate the sequence number field in AH or ESP headers. The Sequence Counter Overflow is a flag indicating whether overflow of the sequence number counter should generate an auditable event and prevent further transmission of packets on this SA. An Anti-Replay Window is used to determine whether an inbound AH or ESP packet is a replay. AH information involves information about the authentication algorithm, keys and related parameters being used with AH. ESP information involves information of encryption and authentication algorithms, keys, initialisation vectors, and related parameters being used with IPSec. AH information consists of the authentication algorithm, keys and related parameters being used with AH. ESP information consists of encryption and authentication algorithms, keys, cryptographic initialisation vectors and related parameters being used with ESP. The sixth parameter, Lifetime of this Security Association, is a time-interval and/or byte-count after which this SA must be replaced with a new SA (and new SPI) or terminated plus an indication of which of these

actions should occur. IPSec Protocol Mode is either tunnel or transport mode. Maximum Transfer Unit (MTU), an optional feature, defines the maximum size of a packet that can be transmitted without fragmentation. Optionally an MTU discovery protocol may be used to determine the actual MTU for a given route, however, such a protocol is optional.

Both AH and ESP support two modes used, transport and tunnel mode.

Transport mode provides protection primarily for upper layer protocols and extends to the payload of an IP packet Typically, transport mode is used for end-to-end communication between two hosts. Transport mode may be used in conjunction with a tunnelling protocol, other than IPSec tunnelling, to provide a tunnelling capability.

Tunnel mode provides protection to the entire IP packet and is usually used for sending messages through more than two components, although tunnel mode may also be used for end-to-end communication between two hosts. Tunnel mode is often used when one or both ends of a SA is a security gateway, such as a firewall or a router that implements IPSec. With tunnel mode, a number of hosts on networks behind firewalls may engage in secure communications

without implementing IPSec. The unprotected packets generated by such hosts are tunnelled through external networks by tunnel mode SAs set up by the IPSec software in the firewall or secure router at boundary of the local network.

To achieve this, after the AH or ESP fields are added to the IP packet, the entire packet plus security fields are treated as the payload of a new outer IP packet with a new outer IP header. The entire original, or inner, packet travels through a tunnel from one point of an IP network to another: no routers along the way are able to examine the inner IP packet. Because the original packet is encapsulated, the new larger packet may have totally different source and destination addresses, adding to the security. In other words, the first step in protecting the packet using tunnel mode is to add a new IP header to the packet; thus the "IP|payload" packet becomes "IP|IP|payload". The next step is to secure the packet using ESP and/or AH. In case of ESP, the resulting packet is "IP|ESP|IP|payload". The whole inner packet is covered by the ESP and/or AH protection. AH also protects parts of the outer header, in addition to the whole inner packet.

The IPSec tunnel mode operates e.g. in such a way that if a host on a network generates an IP packet with a destination address of another host on another network, the packet is routed from the originating host to a security gateway (SGW), firewall or other secure router at the boundary of the first network. The SGW or the like filters all outgoing packets to determine the need for IPSec processing. If this packet from the first host to another host requires IPSec, the firewall performs IPSec processing and encapsulates the packet in an outer IP header. The source IP address of this outer IP header is this firewall and the destination address may be a firewall that forms the boundary to the other local network. This packet is now routed to the other host's firewall with intermediate routers examining only the outer IP header At the other host firewall, the outer IP header is stripped off and the inner packet is delivered to the other host.

ESP in tunnel mode encrypts and optionally authenticates the entire inner IP packet, including the inner IP header AH in tunnel mode authenticates the entire inner IP packet, including the inner IP header, and selected portions of the outer IP header.

The key management portion of IPSec involves the determination and distribution of secret keys. The default automated key management protocol for IPSec is referred to as ISAKMP/Oakley and consists of the Oakley key determination protocol and Internet Security Association and Key Management Protocol (ISAKMP). Internet key exchange (IKE) is a newer name for the ISAKMP/Oakley protocol. IKE is based on the Diffie-Hellman algorithm and supports RSA signature authentication among other modes. IKE is an extensible protocol, and allows future and vendor-specific features to be added without compromising functionality.

IPSec has been designed to provide confidentiality, integrity, and replay protection for IP packets. However, IPSec is intended to work with static network topology, where hosts are fixed to certain subnetworks. For instance, when an IPSec tunnel has been formed by using Internet Key Exchange (IKE) protocol, the tunnel endpoints are fixed and remain constant. If IPSec is used with a mobile host, the IKE key exchange will have to be redone from every new visited network. This is problematic, because IKE key exchanges involve computationally expensive Diffie-Hellman key exchange algorithm calculations and possibly RSA calculations. Furthermore, the key exchange requires at

least three round trips (six messages) if using the IKE aggressive mode followed by IKE quick mode, and nine messages if using IKE main mode followed by IKE quick mode. This may be a big problem in high latency networks, such as General Packet Radio Service (GPRS) regardless of the computational expenses.

In this text, the term mobility and mobile terminal does not only mean physical mobility, instead the term mobility is in the first hand meant moving from one network to another, which can be performed by a physically fixed terminal as well.

The problem with standard IPSec is thus that it has been designed for static connections. For instance, the end points of an IPSec tunnel mode SA are fixed. There is also no method for changing any of the parameters of an SA, other than by establishing a new SA that replaces the previous one. However, establishing SAs is costly in terms of both computation time and network latency.

An example of a specific scenario where these problems occur is described next in order to illustrate the problem.

In the scenario, there is a standard IPSec security gateway, which is used by a mobile terminal e.g. for remote

access. The mobile terminal is mobile in the sense that it changes its network point of attachment frequently. A mobile terminal can in this text thus be physically fixed or mobile. Because it may be connected to networks administered by third parties, it may also have a point of attachment that uses private addresses—i.e., the network is behind a router that performs network address translation (NAT). In addition, the networks used by the mobile terminal for access may be wireless, and may have poor quality of service in terms of throughput and e.g. packet drop rate.

Standard IPSec does not work well in the scenario. Since IPSec connections are bound to fixed addresses, the mobile terminal must establish a new IPSec connection from each point of attachment. If an automated key exchange protocol, such as IKE, is used, setting up a new IPsec connection is costly in terms of computation and network latency, and may require a manual authentication phase (for instance, a one-time password). If IPSec connections are set up manually, there is considerable manual work involved in configuring the IPSec connection parameters.

Standard IPSec does e.g. not work through NAT devices at the moment. A standard IPSec NAT traversal protocol is

currently being specified, but the security gateway in the scenario might not support an IPSec protocol extended in this way. Furthermore, the current IPSec NAT traversal protocols are not well suited to mobility.

There are no provisions for improving quality of service over wireless links in the standard IPSec protocol. If the access network suffers from high packet drop rates, the applications running in the mobile host and a host that the mobile terminal is communicating with will suffer from packet drops.

A known method of solving some of these problems is based on having an intermediate host between the mobile terminal and the IPSec security gateway. The intermediate host might be a Mobile IP home agent, that provides mobility for the connection between the mobile terminal and the home agent, while the connection from the mobile node to the security gateway is an ordinary IPSec connection. In this case, packets sent by an application in the mobile client are first processed by IPSec, and then by Mobile IP.

In the general case, this implies both Mobile IP and IPSec header fields for packets exchanged by the mobile terminal and the home agent. The Mobile IP headers are removed by

the home agent prior to delivering packets to the security gateway, and added when delivering packets to the mobile terminal. Because of the use of two tunnelling protocols (Mobile IP and IPSec tunnelling), the solution is referred to as "double tunnelling" in this document.

The above method solves the mobility problem, at the cost of adding extra headers to packets. This may have a significant impact on networks that have low throughput such as the General Packet Radio System (GPRS).

Another known method is again to use an intermediate host between the mobile client and the IPSec security gateway. The intermediate host has an IPSec implementation that may support NAT traversal, and possibly some proprietary extensions for improving quality of service of the access network, for instance.

The mobile host would now establish an IPSec connection between itself and the intermediate host, and would also establish an IPSec connection between itself and the IPSec security gateway. This solution is similar to the first known method, except that two IPSec tunnels are used. It solves a different set of problems—for instance, NAT

traversal—but also adds packet size overhead because of double IPsec tunnelling.

A third known method is to use a similar intermediate host as in the second known method, but establish an IPSec connection between the mobile terminal and the intermediate host, and another, separate IPSec connection between the intermediate host and the security gateway. The IPSec connection between the mobile terminal and the intermediate host may support NAT traversal, for instance, while the second IPSec connection does not need to.

When packets are sent by an application in the mobile terminal, the packets are IPSec-processed using the IPSec connection shared by the mobile terminal and the intermediate host. Upon receiving these packets, the intermediate host undoes the IPSec-processing. For instance, if the packet was encrypted, the intermediate host decrypts the packet. The original packet would now be revealed in plaintext to the intermediate host. After this, the intermediate host IPSec-processes the packet using the IPSec connection shared by the intermediate host and the security gateway, and forwards the packet to the security gateway.

This solution allows the use of an IPSec implementation that support NAT traversal, and possibly a number of other (possibly vendor specific) improvements, addressing problems such as the access network quality of service variations. Regardless of these added features, the IPSec security gateway remains unaware of the improvements, and is not required to implement any of the protocols involved in improving service. However, the solution has a major drawback: the IPsec packets are decrypted in the intermediate host, and thus possibly sensitive data is unprotected in the intermediate host.

Consider a business scenario where a single intermediate host provides improved service to a number of separate customer networks, each having its own standard IPSec security gateway. Having decrypted packets of various customer networks in plaintext form in the intermediate host is clearly a major security problem.

To summarise, the known solutions either employ extra tunnelling, causing extra packet size overhead, or use separate tunnels, causing potential security problems in the intermediate host(s) that terminate such tunnels.

THE OBJECT OF THE INVENTION

The object of the invention is to develop a method for forwarding secure messages between two computers, especially, via an intermediate computer by avoiding the above mentioned disadvantages.

Especially, the object of the invention is to forward secure messages in a way that enables changes to be made in the secure connection

SUMMARY OF THE INVENTION

The method and system of the invention enable secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network. It is mainly characterized in that a message is formed in the first computer or in a computer that is served by the first computer, and in the latter case, sending the message to the first computer. In the first computer, a secure message is then formed by giving the message a unique identity and a destination address. The message is sent from the first computer to the intermediate computer, whereafter said destination address and the unique identity are used to find an address to the second computer. The current destination address is substituted with the found address to the second computer,

and the unique identity is substituted with another unique identity. Then the message is forwarded to the second computer.

Preferably, the first computer processes the formed message using a security protocol and encapsulates the message at least in an outer IP header. The outer IP header source address is the current address of the first computer, while the destination address is that of the intermediate computer. The message is then sent to the intermediate computer, which matches the outer IP header address fields together with a unique identifier used by the security protocol, and performs a translation of the outer addresses and the unique identity used by the security protocol. The translated packet is then sent to the second computer, which processes it using the standard security protocol in question. In the method of the invention, there is no extra encapsulation overhead as in the prior art methods. Also, the intermediate computer does not need to undo the security processing, e.g. decryption, and thus does not compromise security as in the prior art methods.

Corresponding steps are performed when the messages are sent in the reverse direction, i.e. from the second computer to the first computer.

Preferably, the secure message is formed by making use of the IPSec protocols, whereby the secure message is formed by using an IPsec connection between the first computer and the intermediate computer. The message sent from the first computer contains message data, an inner IP header containing actual sender and receiver addresses, an outer IP header containing the addresses of the first computer and the intermediate computer, a unique identity, and other security parameters. The unique identity is one or more SPI values and the other security parameters contain e.g. the IPsec sequence number(s). The number of SPI values depends on the SA bundle size (e.g. ESP+AH bundle would have two SPI values). In the following, when an SA is referred to, the same applies to an SA bundle. The other related security parameters, containing e.g. the algorithm to be used, a traffic description, and the lifetime of the SA, are not sent on the wire. Only SPI and sequence number are sent for each IPsec processed header (one SPI and one sequence number if e.g. ESP only is used; two SPIs and two sequence numbers if e.g. ESP+AH is used, etc.).

Thus, the unsecured data packet message is formed by the sending computer, which may or may not be the first computer. The IP header of this packet has IP source and

destination address fields (among other things). The packet is encapsulated e.g. wrapped inside a tunnel, and the resulting packet is secured. The secured packet has a new outer IP header, which contains another set of IP source and destination addresses (in the outer header—the inner header is untouched), i.e. there are two outer addresses (source and destination) and two inner addresses. The processed packet has a unique identity, the IPsec SPI value(s).

An essential idea of the invention is to use the standard protocol (IPSec) between the intermediate computer and the second computer and an "enhanced IPSec protocol" between the first computer and the intermediate computer. IPsec-protected packets are translated by the intermediate computer, without undoing the IPsec processing. This avoids both the overhead of double tunneling and the security problem involved in using separate tunnels.

The translation is performed e.g. by means of a translation table stored at the intermediate computer. The outer IP header address fields and/or the SPI-values are changed by the intermediate computer so that the message can be forwarded to the second computer.

By modifying the translation table and parameters associated to a given translation table entry, the properties of the connection between the first and the intermediate computers can be changed without establishing a new IPsec connection, or involving the second computer in any way.

One example of a change in the SA between the first computer and the intermediate computer is the change of addresses for enabling mobility. This can be accomplished in the invention simply by modifying the translation table entry address fields. Signaling messages may be used to request such a change. Such signalling messages may be authenticated and/or encrypted, or sent in plaintext. One method of doing authentication and/or encryption is to use an IPsec connection between the first computer and the intermediate computer. The second computer is unaware of this IPsec connection, and does not need to participate in the signalling protocol in any way. Several other methods of signalling exist, for instance, the IKE key exchange protocol maybe extended to carry such signalling messages.

In the signalling, e.g. a registration request is sent from the first computer to the intermediate computer which causes the intermediate computer to modify the addresses in

the mapping table and thus, the intermediate computer can identify the mobile next time a message is sent. Preferably, as a result of a registration request, a reply registration is sent from the intermediate computer back to the first computer.

Other examples of possible modifications to the SA—or in general, the packet processing behaviour—between the first computer and the intermediate computer are the following.

One example is the first computer and the intermediate computer performs some sort of retransmission protocol that ensures that the IPSec protected packets are not dropped in the route between the first and the intermediate computer. This may have useful applications when the first computer is connected using a network access method that has a high packet drop rate—for instance, GPRS.

Such a protocol can be easily based on e.g. IPsec sequence number field and the replay protection window, which provide a way to detect that packet(s) have been lost. When a receiving host detects missing packets, it can send a request message for those particular packets. The request can of course be piggy-backed on an existing data packet that is being sent to the other host. Another method of

doing the retransmissions may be based on using an extra protocol inside which the IPSec packets are wrapped for transmission between the first and intermediate computer. In any case, the second computer remains unaware of such a retransmission protocol.

Another example is performing a Network Address Translation (NAT) traversal encapsulation between the first and the intermediate computer. This method could be based on e.g. using UDP encapsulation for transmission of packets between the first and the intermediate computer. The second computer remains unaware about this processing and does not even need to support NAT traversal at all. This is beneficial because there are several existing IPSec products that have no support for NAT traversal.

The system of the invention is a telecommunication network for secure forwarding of messages and comprises at least a first computer, a second computer and an intermediate computer. It is characterized in that the first and the second computers have means to perform IPSec processing, and the intermediate computer have means to perform IPSec translation and possibly key exchange protocol, such as IKE, translation, preferably by means of mapping tables. The intermediate computer may perform IPSec processing

related to other features, such as mobility signalling described above or other enhancements.

The IPSec translation method is independent of the key exchange translation method. Also manual keying can be used instead of automatic keying. If automatic keying is used, any key exchange protocol can be modified for that purpose; however, the idea is to keep the second computer unaware of the interplay of the first and the intermediate computer.

An automatic key exchange protocol may be used in the invention in several ways. The essential idea is that the second computer sees a standard key exchange protocol run, while the first and the intermediate computer perform a modified key exchange. The modified key exchange protocol used between the first and the intermediate computer ensures that the IPsec translation table and other parameters required by the invention are set up as a side-effect of the key exchange protocol. One such modified protocol is presented in the application for the IKE key exchange protocol.

Each translation table consists of entries that are divided into two partitions. The first partition contains information fields related to the connection between the

first computer and the intermediate computer, while the second partition contains information fields related to the connection between the intermediate computer and the second computer.

The translation occurs by identifying the translation table entry by comparing against one partition, and mapping into the other. For traffic that is flowing from the first computer towards the second computer, through the intermediate computer, the entry is found by comparing the received packet against entries in the first partition, and then translating said fields using information found in the second partition of the same entry. For traffic flowing in the opposite direction, the second partition is used for finding the proper translation table entry, and the first partition for translating the packet fields.

The IPSec translation table partitions consist of the following information: the IP local address and the IP remote address (tunnel endpoint addresses) and SPIs for sending and receiving data.

As mentioned, a translation table entry consists of two such partitions, one for communication between first computer and the intermediate computer, and another for

communication between the intermediate computer and the second computer.

The invention described solves the above problems of prior art. The solution is based on giving the first computer, e.g. if it is mobile, an appearance of a standard computer for the second computer. Thus, the second computer will believe it is talking to a standard IPSec host, while the intermediate computer and the second computer will work together using a modified protocol, for instance a slightly modified IPSec and IKE that helps to accomplish this goal. There are, however, several other control protocols that could conceivably be used between the first and the intermediate computer.

In the following, the invention is described more in detail by using figures by means of some embodiment examples to carry out the invention. The invention is not restricted to the details of the figures and accompanying text, or any existing protocols, such as the currently standardised IPSec or IKE.

Especially, the invention can be concerned with other kinds of telecommunication networks wherein the method of the invention can be applied than that of the figures.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates an example of a telecommunication network of the invention.

FIG. 2 describes generally an example of the method of the invention.

FIG. 3 illustrates an example of an IPSec translation table used by the intermediate computer to change the outer IP address and SPI value.

FIG. 4 describes a detailed example of how the SA is formed in the invention.

FIG. 5 illustrates an example of translation tables for the modified key exchange of the invention.

FIG. 6 shows a mapping table for identification values of the user Security Gateway (SGW) addresses.

DETAILED DESCRIPTION OF THE INVENTION

An example of a telecommunication network of the invention is illustrated in FIG. 1, comprising a first computer, here a client computer **1** served by an intermediate computer,

here as a server **2**, and a host computer **4**, that is served by the second computer, here a security gateway (SGW) **3**. The security gateway supports the standard IPSec protocol and optionally the IKE key exchange protocol. The client computer and the server computer support a modified IPSec and IKE protocol.

The invention is not restricted to the topology of FIG. 1. In other embodiments, the first computer may e.g. be a router; or there might e.g. not be a host behind the second computer (in which case the first and the second computer are talking to each other directly), etc.

The IPSec translations taking place in the scenario of FIGS. 1, 2, and **3** are discussed first. The IPSec connections (such as SAs) in the scenario may be established manually, or using some key exchange protocol, such as the Internet Key Exchange (IKE). To illustrate how a key exchange protocol would be used in the scenario of FIG. 1, a modified IKE protocol based on IKE translation is also presented later.

In the invention, an IPSec connection is shared by the first computer and the second computer, while the intermediate computer holds information required to perform

address and IPSec SPI translations for the packets. These translations accomplish the effect of "double tunnelling" (described in the technical background section), but with the method of the invention the confidentiality of the packets is not compromised, while simultaneously having no extra overhead when compared to standard IPSec. The intermediate computer does not know the cryptographic keys used to encrypt and/or authenticate the packets, and can thus not reveal their contents.

The advantage of the invention is that the logical IPSec connection shared by the first and the second computer can be enhanced by the first and the intermediate computer without involvement of the second computer. In particular the so-called "ingress filtering" performed by some routers does not pose any problems when translations of addresses are used. In the example presented, each host also manages its own IPSec SPI space independently.

In the example of FIG. 1, an IPSec connection is formed between the client computer **1** (the first computer) and the security gateway **3** (the second computer). To create an IPSec tunnel, a SA (or usually a SA bundle) is formed between the respective computers with a preceding key exchange. The key exchange between the first and the second

computer can take place manually or it can be performed with an automatic key exchange protocol such as the IKE protocol. For performing said key exchange, a standard IKE protocol is used between the server **2** and the security gateway **3**, and a modified IKE protocol is used between the client computer **1** and the server **2**. An example of a modified IKE protocol that can be used in the invention is described in connection with FIG. 4.

Messages to be sent to the host terminal **4** from the client computer **1** are first sent to the server **2**, wherein an IPSec translation and an IKE translation takes place. After that the message can be sent to the security gateway **3**, which sends the message further in plain text to the host terminal **4**.

The method of the invention, wherein messages in packet form are sent by routing to the end destination, is generally described in connection with FIG. 2. It is assumed in the following description that the IPSec connection between the first and second computer already is formed. The IPSec connection can be set up manually or automatically by e.g. an IKE exchange protocol which is described later.

FIG. 2 illustrates the sequence of events that take place when the first computer, corresponding to the mobile terminal in FIG. 1, sends a packet to a destination host, labelled X in the figure, and when the host X sends a packet to the mobile terminal.

IP packets consist of different parts, such as a data payload and protocol headers. The protocol headers in turn consist of fields.

In step **1** of FIG. 2, the first computer, e.g. a mobile terminal, forms an IP packet that is to be sent to host X. Typically, this packet is created by an application running on the mobile terminal. The IP packet source address is the address of the mobile terminal, while the destination address is host X.

The packet is processed using an IPSec tunnel mode SA, which encapsulates the IP packet securely. The example assumes that IPSec encryption and/or authentication of ESP type is used for processing the-packet, although the invention is not limited to the use of only ESP; instead, an arbitrary IPsec connection may be used.

In said processing, a new IP header is constructed for the packet, with so-called outer IP addresses. The outer source

address of the packet can be the same as the inner IP address—i.e., the address of the mobile terminal—but can be different, if the mobile terminal is visiting a network. The outer source address corresponds to the care of address obtained by the mobile terminal from the visited network, in this case. The outer destination address is the address of the intermediate computer. In addition to the new IP header, an ESP header is added, when using IPSec ESP mode. The SPI field of the ESP header added by the IPSec processing is set to the SPI value that the intermediate computer uses for receiving packets from the mobile terminal. In general, there may be more than one SPI field in a packet.

The processing of packets in the intermediate computer is based on a translation table i.e. an IPSec translation table shown in FIG. 3. The table has been divided into two partitions. The left one, identified by the prefix "c-", refers to the network connection between the first computer (host **1** in FIG. 1) and the intermediate computer (host **2** in FIG. 1). The right one, identified by the prefix "s-", refers to the network connection between the intermediate computer and the second computer (computer **3** in FIG. 1). The postfix number ("-1", "-2", or "-3") identifies the

host in question. Thus, the address fields ("addr") refer to outer addresses of a packet, while the SPI fields ("SPI") refer to the receiver of packets, which packets were sent with this SPI. Thus, "c-SPI-2" is the SPI value used by host **2** (the intermediate computer) when receiving packets from host **1** (the first computer), and the SPI-value "c-SPI-1" is the SPI-value with which the first computer receives messages and the SPI-value with which the intermediate computer sends messages to the first computer and so on.

In terms of FIG. 3, the outer source address would be "c-addr-1" (195.1.2.3), the outer destination address "c-addr-2" (212.90.65.1), while the SPI field would be "c-SPI-2" (0×12341234). The notation 0×NNNNNNNN indicates a 32-bit unsigned integer value, encoded using a hexadecimal notation (base **16**). The inner source address is processed by IPSec in the first computer, and would typically be encrypted. In this example, the inner source address would be the static address of the mobile terminal, e.g. 10.0.0.1.

When the intermediate computer receives the packet sent in step **1** described above, it performs an address and SPI translation, ensuring that the security gateway (host **3** of

FIG. 1) can accept the packet. Most of the packet is secured using IPSec, and since the intermediate computer does not have the cryptographic keys to undo the IPSec processing done by the mobile terminal, it cannot decrypt any encrypted portions of the packet but is able to use the outer IP addresses and the incoming SPI value to determine how to modify the outer address and the SPI to suite the second computer, which is the next destination. SPI is now changed to 0×56785678 in the intermediate computer and the address is changed to the address of the second computer. This is done by means of the IPSec translation table of FIG. 3.

The first row of FIG. 3 is a row that the intermediate computer has found that matches the packet in the example, and thus the intermediate computer chooses it for translation. The new outer source address s-addr-**2** (212.90.65.1) is substituted for the outer source address c-addr-**1** (195.1.2.3), and the new outer destination address s-addr-**3** (103.6.5.4) is substituted for the outer destination address c-addr-**2** (212.90.65.1). The new SPI value, s-SPI-**3** (0×56785678), is substituted for the SPI value c-SPI-**2** (0×12341234). If more than one SPI values are used, all the SPI values are substituted similarly. In the

example, s-addr-**2** and c-addr-**2** happen to be the same on both partitions of the table. This is not necessarily so but the intermediate computer might use another address for sending.

In step **2** of FIG. 2, the translated packet is sent further to the second computer. The inner IP packet has not been modified after that the first computer sent the packet. The second computer processes the packet using standard IPSec algorithms. The security gateway (the second computer) can e.g. decipher and/or check the authenticity of the packet, then remove the IPSec tunnelling, and forward the original packet towards the destination host, X. Thus, the entire original packet was unaffected by the translation as the IP header, and thus the address fields, was covered by IPSec.

After uncovering the original packet from the IPsec tunnel, the second computer makes a routing decision based on the IP header of the original packet. In the example, the IP destination address is X (host X in FIG. 2), and thus the second computer delivers the packet either directly to X, or to the next hop router.

In step **3** of FIG. 2, the packet is sent from the second computer (corresponding to SGW in FIG. 1) to host X, having

now only the original source IP address 10.0.0.1 and the original destination IP address X in the IP header. Thus, in step **3**, host X receives the packet sent by the second computer. Usually, an application process running on host X would generate some return traffic. This would cause an IP packet to be generated and sent to the second computer.

If a packet is sent back from host X to the first computer (corresponding to the client computer in FIG. 1), steps analogous to steps **1-3** are performed. The packet is thus first sent to the second computer, with the source IP address being X and the destination IP address being 10.0.0.1, in step **4**. The generated packet is then received by the second computer. The IPSec policy of the second computer requires that the packet be IPSec-processed using a tunnel mode IPSec SA. This processing is similar to the one in steps **1** and **2**. A new, outer IP header is added to the packet in the second computer, after which the resulting packet is secured using the IPSec SA. The outer IP source address is set to s-addr-**3** (103.6.5.4) while the outer IP destination address is set to s-addr-**2** (212.90.65.1). The SPI field is set to s-SPI-**2** (0×c1230012). In step **5**, the resulting packet is sent to the address indicated by the new outer IP destination

address, s-addr-**2**, the intermediate computer. The intermediate computer receives the packet and performs a similar address and SPI translation.

The inner addresses are still the same, and are not modified by the intermediate computer. Since the packet intended to be sent to the first computer, the new, translated outer destination IP address indicate the address of the first computer.

The resulting packet is sent to the first computer in step **6**.

As a result of step **6**, the packet is received by the first computer. The IPSec processing is undone, i.e. decryption and/or authentication is performed, and the original packet is uncovered from the IPSec tunnel. The original packet is then delivered to the application running on the first computer. In case the first computer acts as a router, the packet may be delivered to a host in a subnet for which the first computer acts as a router.

The first computer may be a mobile terminal, the outer address of which changes from time to time. The translation table is then modified using some form of signalling messages, as described in the summary section. Upon

receiving a request for modifying a translation, the intermediate computer updates the related translation table entry to match the new information supplied by the first computer. The operation of the protocol then proceeds as discussed above.

The above discussion is a limited example for illustration purposes. In other embodiments e.g. more than one SA for the connection—for instance, ESP followed by AH, can be used. This introduces two SPI values that must be translated. More than two is also, of course, possible. Furthermore, the example was considered for IPsec ESP only. The changes required for an embodiment in which AH (or ESP+AH) is used, are discussed next.

Changes for Using AH:

If the Authentication Header (AH) IPSec security transform is to be used, there are more considerations than in the previous example. In particular, modifications of the packet fields—even the outer IP header—are detected if AH is used. Thus, the following nominal processing is required by the first computer. The second computer performs standard IPSec processing also in this case.

In step **1**, when sending a packet, the first computer must perform IPsec processing using the SPI values and addresses used in the connection between the intermediate computer and the second computer. For instance, the SPI value would be s-SPI-**3**, the outer source address s-addr-**2**, and the outer destination address s-addr-**3**. The AH integrity check value (ICV) must be computed using these values. ICV is a value, which authenticates most of the fields of the packet. In practice, all fields that are never modified by routers are authenticated.

After computing the AH integrity check value, the outer addresses and the SPI value are replaced with the values used between the first computer and the intermediate computer: c-addr-**1** for the outer source address, c-addr-**2** for the outer destination address, and c-SPI-**2** for the SPI.

In step **2**, the intermediate computer performs the address and SPI translations as in the example with ESP described above. The resulting packet is identical to the one used by the first computer for the AH integrity check value calculation, except possibly for fields not covered by AH (such as the Time-To-Live field, the header checksum, etc). Thus, the AH integrity check value is now correct.

In step **3**, the second computer performs standard IPSec processing of AH. The packet, which now is uncovered from the tunnel is sent to the host X. As in the previous example, an application in host X usually generates a return packet that is to be sent to the first computer. This packet is sent to the second computer in step **4**.

Upon receiving the packet, the processing of the second computer are the same as in the example with ESP. The second computer computes an AH integrity check value of the tunneled packet it is sending to the mobile terminal. The integrity check value is computed against the outer source address of s-addr-**3**, outer destination address of s-addr-**2**, and the SPI value of s-SPI-**2**.

In step **5**, when the intermediate computer receives the packet, it performs ordinary translation of the packet. The new outer source address is c-addr-**2**, the outer destination address is c-addr-**1**, and the SPI value is c-SPI-**1**. At this point the AH integrity check value is incorrect, which was caused by the translations.

When the mobile terminal receives the packet, it performs a translation of the current outer addresses and the SPI field for the original ones used by the second computer: s-

addr-**3** for the outer source address, s-addr-**2** for the outer destination address, and s-SPI-**2** for the SPI value. This reproduces the packet originally sent by the second computer, except possibly for fields not covered by AH. This operation restores the AH integrity check value to its original, correct value. The AH integrity check is then performed against these fields.

Key Exchange Considerations

The above example discussed the "steady state" IPSec translations performed by the intermediate computer. The IPSec SAs and the IPSec translation table entries may be set up manually, or using some automated protocol, such as the Internet Key Exchange (IKE) protocol.

Because the security gateway (the second computer) is a standard IPSec host, it implements some standard key exchange protocol, such as IKE. The first computer and the intermediate computer may use some modified version of IKE, or any other suitable automatic key exchange protocol.

The key exchange must appear as a standard key exchange according to the key exchange protocol supported by the security gateway (the second computer), such as IKE. Also, the overall key exchange performed by the first,

intermediate, and second computer must establish not only cryptographic keys, but also the IPSec translation table entries. The overall key exchange protocol should not reveal the IPSec cryptographic keys to the intermediate computer to avoid even the potential for security problems.

In the following, an example of a modified IKE protocol is presented to outline the functionality of such a protocol in the context of the invention. The protocol provides the functionality described above. In particular, the intermediate computer has no knowledge of the IPSec cryptographic keys established. The protocol is presented on a general level to simplify the presentation.

The automatic IKE protocol is used prior to other protocols to provide strongly authenticated cryptographic session keys for the IPSec protocols ESP and AH. IKE performs the following functions: (1) security policy negotiation (what algorithms shall be used, lifetimes etc.), (2) a Diffie-Hellman key exchange, and (3) strong user/host authentication (usually using either RSA-based signatures or pre-shared authentication keys). IKE is divided into two phases: phase **1** and phase **2**. Phase **1** negotiates and establishes cryptographic keys for internal use of the IKE protocol itself, and also performs the strong user or host

authentication. Phase **2** negotiates and establishes cryptographic keys for IPSec. If IPSec tunnel mode is used, phase **2** also negotiates the kind of traffic that may be sent using the tunnel (so-called traffic selectors).

The IKE framework supports several "sub-protocols" for phase **1** and phase **2**. The required ones are "main mode" for phase **1**, and "quick mode" for phase **2**. These are used as illustrations, but the invention is not limited to these sub-protocols of IKE.

For the security gateway (second computer), the IKE session seems to be coming from the address s-addr-**2** in FIG. 3. Since there may be any number of mobile terminals served by the intermediate computer, the intermediate computer should either (1) manage a pool of addresses to be used for the s-addr-**2** translation table address, thus providing each user with a separate "surrogate address", or (2) use the same address (or a limited set of addresses), and ensure that the mobile terminals are identified using some other means than their IP address (IKE provides for such identification types, so this is not a problem).

The modified IKE protocol specified is analogous to the IPSec translation table approach. However, instead of SPIs,

the so-called IKE cookies are used as translation indices instead. IKE cookies are essentially IKE session identifiers, and are thus analogous to the IPSec SPI values, which is another form of a session or context identifier. There are two cookies: the initiator cookie, chosen by the host that initiates the IKE session, and the responder cookie, chosen by the host that responds to a session initiation.

The essential features of the protocol are (1) that it appears to be an entirely ordinary IKE key exchange for the security gateway, (2) that the IPsec translation table entry is formed by the intermediate computer during the execution of the protocol, (3) that the first computer obtains all the necessary information for its packet processing, and (4) that the intermediate computer does not obtain the IPsec cryptographic session keys.

The overall steps of the protocol are:

- 1. The first computer initiates the key exchange protocol by sending a message to the intermediate computer. This message is essentially the IKE

main mode initiation message, with some modifications required for this application.

- 2. The intermediate computer determines which security gateway (second computer) to forward this IKE session to, and also establishes a preliminary IKE translation table entry based on the information available from the message.
- 3. The security gateway (the second computer) replies to the IKE main mode initiation message.
- 4. The intermediate computer completes the IKE mapping based on the reply message.
- 5. The modified IKE protocol run continues through IKE main mode (the phase **1** exchange), which is followed by quick mode (the phase **2** exchange). Extensions of standard IKE messages are used between the first computer and the intermediate computer to accomplish the extra goals required by this modified IKE protocol.

In FIG. 4, the IKE session is described message by message. The following text indicates the contents of each message, and how they are processed by the various hosts. There are six main mode messages in the protocol, named mm**1**, mm**2**, . .

. , mm**6**, and three quick mode messages, named qm**1**, qm**2**, and qm**3**.

FIG. 5 illustrates the IKE translation table entry related to the modified IKE key exchange being performed. The bolded entries in each step are added or changed in that step as a result of the processing described in the text.

The IKE translation table partition for the connection between the first computer and the intermediate computer is as follows (the field name in FIG. 5 is given in parentheses):

Local and remote IP address (c-addr-**1**, c-addr-**2**)

Initiator and responder cookie (c-icky, c-rcky)

IKE identification of the first computer (c-userid, e.g. joe@netseal.com)

The IKE translation table partition for the connection between the intermediate computer and the second computer is as follows (the field name in FIG. 5 is given in parentheses):

Local and remote IP address (s-addr-**2**, s-addr-**3**)

Initiator cookie and responder cookie (s-icky, s-rcky)

In addition to these entries, other data may be kept by the intermediate computer and/or the first computer.

The key exchange is initiated by generating an initiator cookie and sending a zero responder cookie to the second computer. A responder cookie is generated in the second computer and a mapping between IP addresses and IKE cookie values in the intermediate computer is established. A translation table to modify IKE packets in flight by modifying the external IP addresses and possibly IKE cookies of the IKE packets is used.

Either the modified IKE protocol between the first computer and the intermediate computer is modified such that the IKE keys are transmitted from the first computer to the intermediate computer for decryption and modification of IKE packets or, alternatively, the modified IKE protocol between the first computer and the intermediate computer is modified such that the IKE keys are not transmitted from the first computer to the intermediate computer for decryption and modification of IKE packets, and the modification of IKE packets is done by the first computer with the intermediate computer requesting such modifications. The latter alternative is discussed in the

example that follows, since it is more secure than the first alternative.

Extra information, such as user information and SPI change requests, to be sent between the first and the intermediate computer, is sent by appending the extra information to the standard IKE messages. The IKE standard has message encoding rules that indicate a definite length, thus the added extra information can be separated from the IKE message itself. The extra information fields are preferably encrypted and authenticated, for instance by using a secret shared by the first computer and the intermediate computer. The details of this process are not relevant to the invention.

The extra information slot in each IKE message is called the message "tail" in the following.

IKE messages consist of an IKE header, which includes the cookie fields and message ID field, and of a list of payloads. A payload has a type, and associated information.

FIG. 4 considers an example of the routing of packets according to the invention considering IPSec security association set-up for distribution of keys. As in the foregoing FIG. 2, the session begins with sending a packet

from the client (first computer) to the server (intermediate computer).

The key exchange is initiated by the first computer. Thus, in step **1** of FIG. 4, the first computer constructs mm**1**. The IP header of the message contains the following values:

- IP source address: 195.1.2.3 (c-addr-**1**)
- IP destination address: 212.90.65.1 (c-addr-**2**)

The IKE header contains the following values (step **1** in Figure X):

- Initiator cookie: CKY**1** (c-icky)
- Responder cookie: **0** (c-rcky)
- Message ID: **0**

The message contains the following payloads:

- A Security Association (SA) payload, which contains the IKE phase **1** security policy offers from the first computer.

- The message may contain additional payloads, such as Vendor Identification (VID) payloads, certificate requests/responses, etc.
- A VID payload can be used to indicate that the first computer supports the protocol described here.

The message tail contains the following information:

- User identification type and value—the c-userid field. These are used by the intermediate computer to choose a security gateway to forward this session to. The identification type may be any of the IKE types, but additional types can be defined. An alternative to this field is to directly indicate the security gateway for forwarding. There are other alternatives as well, but these are not essential to the invention.

In step **2**, the mm**1** is received by the intermediate computer. The intermediate computer examines the message, and forms the preliminary IKE translation table entry. FIG. 5, step **1** illustrates the contents of this preliminary entry. The c-userid field is sent in the mm**1** tail.

The intermediate computer then determines which security gateway to forward this IKE session to. The determination may be based on any available information, static configuration, load balancing, or availability requirements. The presented, simple method is to use the identification information in the mm**1** tail to look up the first matching identification type and value from a table. An example of such a table is presented in FIG. 6.

The identification mapping table of FIG. 6, is one method for choosing a security gateway that matches the incoming mobile terminal. The identification table would in this example be an ordered list of identification type/value entries, that match to a given security gateway address. When the incoming mobile terminal identification matches the identification in the table, the corresponding security gateway is used. For instance, john.smith@netseal.com would match the first row of the table, i.e., the security gateway 123.1.2.3, while joe@netseal.com matches the second row, i.e., the security gateway 103.6.5.4. The identification types include any identification types defined for the IKE protocol, and may contain other types as well, such as employee numbers, etc.

Other methods of determining the security gateway to be used may be employed. One such method is for the mobile terminal to directly indicate a given security gateway to be used. The mobile terminal may also indicate a group of security gateways, one of which is used. The exact details are not relevant to the invention.

In addition to determining the security gateway address, the intermediate computer determines which address its for communication between itself and the second computer. The same address as is used for the communication between the first and the intermediate computer may be used, but a new address may also be used. The address can be determined using a table similar to the one in FIG. 6, or the table of FIG. 6 may be extended to include this address.

The intermediate computer then generates its own initiator cookie. This is done to keep the two session identifier spaces entirely separate, although the same initiator cookie may be passed as is.

After these determinations, the preliminary translation table entry is modified. FIG. 5, step **2** illustrates the contents of the entry at this point.

The original IP header fields are modified as follows (step **2** in FIG. 4):

- IP source address: 212.90.65.1 (s-addr-**2**)
- IP destination address: 103.6.5.4 (s-addr-**3**)

The IKE header is modified as follows:

- Initiator cookie: CKY**2** (s-icky)
- Responder cookie: **0** (s-rcky)
- Message ID: **0**

The message tail is removed. The VID payload that identifies support for this modified protocol is also removed. The mm**1** is then forwarded to the second computer.

In step **3**, the second computer responds with mm**2**. The IP header of the message contains the following values (step **3** in FIG. 4):

- IP source address: 103.6.5.4 (s-addr-**3**)
- IP destination address: 212.90.65.1 (s-addr-**2**)

The IKE header contains the following values:

- Initiator cookie: CKY**2** (s-icky)
- Responder cookie: CKY**3** (s-rcky)
- Message ID: **0**

The message contains the following payloads:

- Security Association (SA) payload. This is a reply to the offer by the first computer, and indicates which security configuration is acceptable for the second computer (this scenario assumes success, so the case of an error reply is not considered).
- Possibly optional IKE payloads, such as VID payloads, certificate requests/replies, etc.

There is no message tail.

In step **4**, the mm**2** is received by the intermediate computer. The intermediate computer updates its IKE translation table based on the received message. Step **3** in

FIG. 5 illustrates the contents of the translation table entry at this point.

The intermediate computer generates its own responder cookie, CKY**4**, and updates the translation table yet again. Step **4** in FIG. 5 illustrates the entry at this point. After this step, the translation table entry is complete, and the address and cookie translations are performed as in steps **1-4** for the following messages.

The translated message contains the following IP header fields (FIG. 4, step **4**)

- IP source address: 212.90.65.1 (c-addr-**2**)
- IP destination address: 195.1.2.3 (c-addr-**1**)

The translated IKE header contains the following fields:

- Initiator cookie: CKY**1** (c-icky)
- Responder cookie: CKY**4** (c-rcky)

The message contains the following payloads:

- The SA payload sent by the second computer.
- Any optional payloads sent by the second computer.
- A VID payload may be added to indicate support of this modified protocol to the first computer.

A message tail is added, and contains the following information:

- Address and/or identification information of the chosen security gateway (the second computer). This information can be used by the client to choose proper authentication information, such as RSA keys.

The message is then forwarded to the first computer.

In step **5**, the first computer constructs mm**3**. The message contains the following payloads:

- A Key Exchange (KE) payload, that contains Diffie-Hellman key exchange data of the first computer.

- A Nonce (NONCE) payload, that contains a random number chosen by the first computer.
- Possibly optional IKE payloads.

The message is sent to the intermediate computer.

In step **6**, the mm**3** is forwarded to the second computer. The contents of the message are not changed, only the IP header addresses and the IKE cookies, in the manner described in steps **1-4**.

In step **7**, the second computer receives mm**3** and responds with mm**4**. The message contains the following payloads:

- A Key Exchange (KE) payload, that contains Diffie-Hellman key exchange data of the second computer.
- A Nonce (NONCE) payload, that contains a random number chosen by the second computer.
- Possibly optional IKE payloads.

In step **8**, the mm**4** is forwarded to the first computer.

In step **9**, the first computer constructs mm**5**, which is the first encrypted message in the session. All subsequent

messages are encrypted using the IKE session keys established from the previous Diffie-Hellman key exchange (the messages mm**3** and mm**4**) by means of hash operations, as described in the IKE specification. Note that the intermediate computer does not possess these keys, and can thus not examine the contents of any subsequent IKE messages. In fact, the intermediate computer has no advantage compared to a hostile attacker if it attempts to decipher the IKE traffic. Instead, the intermediate computer indirectly modifies some fields in the IKE messages by sending a modification request in the IKE message tail to the first computer, which does the requested modifications before IKE encryption processing.

The message contains the following payloads:

- An Identification (ID) payload, that identifies the first computer to the second computer. This identification may be the same as the identification sent in the mm**1** tail, but may differ from that. These two identifications serve different purposes: the mm**1** tail identification (c-userid) is used to select a security gateway

for IKE session forwarding (the second computer), while the ID payload in this message is used by the second computer for IKE authentication purposes, for instance, to select proper RSA authentication keys.

- A Signature (SIG) or Hash (HASH) payload, that serves as an authenticator. A signature payload is used if RSA- or DSS-based authentication is used, while a hash payload is used for pre-shared key authentication. There are other authentication methods in IKE, and IKE can also be extended with new authentication methods. These are not essential to the invention, and the following text assumes RSA authentication (i.e., use of the signature payload).
- Possibly optional IKE payloads.

The message tail contains the-following information:

- The SPI value that the first computer wants to use for receiving IPsec-protected messages from the intermediate computer, i.e., the c-SPI-**1** value of the IPsec translation table in FIG. 3.

More than one SPI value could be transmitted here, but for simplicity, the following discussion assumes that only a single SPI is necessary (i.e. only one SA is applied for IPsec traffic processing). Extending the scheme to multiple SPIs is straightforward.

In step **10**, the mm**5** is forwarded to the second computer.

The intermediate computer removes the message tail, and performs the IKE translation discussed previously, and then forwards the message to the second computer.

In step **11**, the second computer receives the mm**5** message, and authenticates the user (or the host, depending on what identification type is used). Assuming that the authentication succeeds, the second computer proceeds to authenticate itself to the first computer.

The mm**6** message contains the following payloads:

- An Identification (ID) payload, that identifies the second computer to the first computer.
- A Signature (SIG) payload (here RSA authentication is assumed).

- Possibly optional IKE payloads.

In step **12**, the mm**6** is received by the intermediate computer. The intermediate computer does not change the message itself, but adds a tail with the following information:

- The SPI value that the intermediate computer wants the first computer to offer to the second computer in the qm**1** message. Since the intermediate computer cannot access the contents of the IKE messages, this modification request is made using the message tail (see the discussion of step **9**). The SPI value sent matches the s-SPI-**2** field of the IPsec translation table of FIG. 3.
- The SPI value that the intermediate computer wants the first computer to use for messages sent to itself. This matches the c-SPI-**2** field of the IPsec translation table of FIG. 3.

The resulting message is forwarded to the first computer.

In step **13**, the first computer constructs qm**1**, which contains the following IKE payloads:

- A Hash (HASH) payload, that serves as an authenticator of the message.
- A Security Association (SA) payload, which contains the IKE phase **2** security policy offers from the first computer, i.e., the IPsec security policy offers. The SA payload contains the SPI value assigned to the first computer in the mm**6** message, i.e., s-SPI-**2** in FIG. 3.
- Optionally, a Key Exchange (KE) payload, if a new Diffie-Hellman key exchange is to be performed in phase **2** (this depends on the contents of the SA payload).
- A Nonce (NONCE) payload, which contains a random value chosen by the first computer.
- Optionally, two Identification (ID) payloads that indicate the IPsec traffic selectors that the first computer proposes for an IPsec tunnel mode SA. If IPsec transport mode is used, these are not necessary, but they may still be used. They may also be omitted if IPsec tunnel mode is used.

The IKE header is the same as previously, except that the Message ID field now contains a non-zero 32-bit value, that

serves as a phase **2** session identifier. This identifier remains constant for the entire quick mode exchange.

The message is sent to the intermediate computer.

In step **14**, the intermediate computer forwards the qm**1** message to the second computer.

In step **15**, the second computer inspects the security policy offers and other information contained in the qm**1** message, and determines which security policy offer matches its own security policy (the case when no security policies match results in an error notification message).

The second computer responds with qm**2** message that contains the following payloads:

- A Hash (HASH) payload, that serves as an authenticator of the message.
- A Security Association (SA) payload, which indicates the security policy offer chosen by the second computer. The message also contains the SPI value that the second computer wants to use when receiving IPsec-protected messages. The SPI

value matches s-SPI-**3** of the IPsec translation table in FIG. 3.

- Optionally, a Key Exchange (KE) payload, if a new Diffie-Hellman key exchange is to be performed in phase **2**.
- A Nonce (NONCE) payload, which contains a random value chosen by the second computer.
- If Identification (ID) payloads were sent by the first computer, the second computer also sends Identification payloads.

In step **16**, the intermediate computer forwards the qm**2** message to the first computer.

In step **17**, the first computer constructs qm**3** message, which contains the following payloads:

- A Hash (HASH) payload, that serves as an authenticator of the message.

The following information is sent in the message tail:

- The SPI value sent by the second computer in the qm**2** message. This is sent here, because the intermediate computer cannot decrypt the qm**2** message and look up the SPI from there. The SPI value matches s-SPI-**3** of the IPsec translation table in FIG. 3.

In step **18**, the intermediate computer receives the qm**3** and reads the s-SPI-**3** value from the message tail. All the information required to construct the IPsec translation table entry is now gathered, and the entry can be added to the translation table. In particular, the information fields are as follows:

- c-addr-**1**: same as c-addr-**1** of the IKE session (195.1.2.3).
- c-addr-**2**: same as c-addr-**2** of the IKE session (212.90.65.1).
- c-SPI-**1**: received in the mm**5** message tail from the first computer.
- c-SPI-**2**: chosen by the intermediate computer, sent to the first computer in the mm**6** message tail.

- s-addr-**2**: same as s-addr-**2** of the IKE session (212.90.65.1 in this example, may be different than c-addr-**2**).
- s-addr-**3**: same as s-addr-**3** of the IKE session (103.6.5.4).
- s-SPI-**2**: chosen by the intermediate computer, sent to the first computer in mm**6** message tail.
- s-SPI-**3**: sent by the second computer in qm**2** to the first computer, which sends it to the intermediate computer in qm**3** message tail.

The intermediate computer forwards the qm**3** message to the second computer, which completes the IKE key exchange, and the IPsec translation table set up.

The IPsec cryptographic keys established using the modified IKE key exchange presented above are either derived from the Diffie-Hellman key exchange performed in IKE main mode, or from the (optional) Diffie-Hellman key exchange performed in quick mode. In both cases, the intermediate computer has no access to the shared secret established using the Diffie-Hellman algorithm. In fact, the intermediate computer has no advantage when compared to a random, hostile attacker.

The above presentation was simplified and exemplified to increase clarity of the presentation. There are several issues not discussed, but these issues are not essential to the invention.

Some of these issues are the following:

- The phase **1** used main mode. Any other IKE phase **1** exchange can be used; this changes the details of the protocol but not the essential ideas.
- There are other approaches than the one presented here. One approach is for the first computer to reveal the IKE keys to the intermediate computer, so that the second computer is able to modify the required fields of the message (namely, SPI values).
- The discussion assumes that the first computer initiates the IKE exchange. The opposite direction is possible, too, but requires more considerations.
- The commit bit feature of IKE is not used. Adding that is simple.

- Security gateway selection is based on a table lookup indexed by an identification type/value pair sent by the first computer. Other mechanisms are easy to implement.
- The discussion assumes a successful IKE key exchange. Error cases are easy to handle.
- Phase **1** policy lookup (when processing mm**1** and mm**2** messages) is not based on the identity of the IKE counterpart. This is not a major issue, since the phase **1** security policy can be independent of the counterpart without limiting usability.
- Phase **1** is a pre-requisite for executing the protocol in the example. This can be easily changed by moving some of the "tail" items to phase **2**.
- The protocol establishes a pair of SAs, one for each direction, and manages the SPI value modifications of these SAs. It is easy to extend this to cover SA bundles with more than one SA, i.e., SAs applied in sequence (ESP followed by AH, for instance). This requires more than one SPI for each direction, but is easy to add to the protocol described.

The invention is not concerned with the details of the key exchange protocol. The presented outline for one such protocol is given as an example, several other alternatives exist. The invention is also not concerned with the IKE key exchange protocol: other key exchange protocols exist, and similar ideas can be applied in using them in the content of the invention.

While the present invention has been described in accordance with preferred compositions and embodiments, it is to be understood that certain substitutions and alterations may be made thereto without departing from the spirit and scope of the following claims.

Rec'd PCT/PTO 08 JUL 2004
PCT/FI03/00045
10/500930

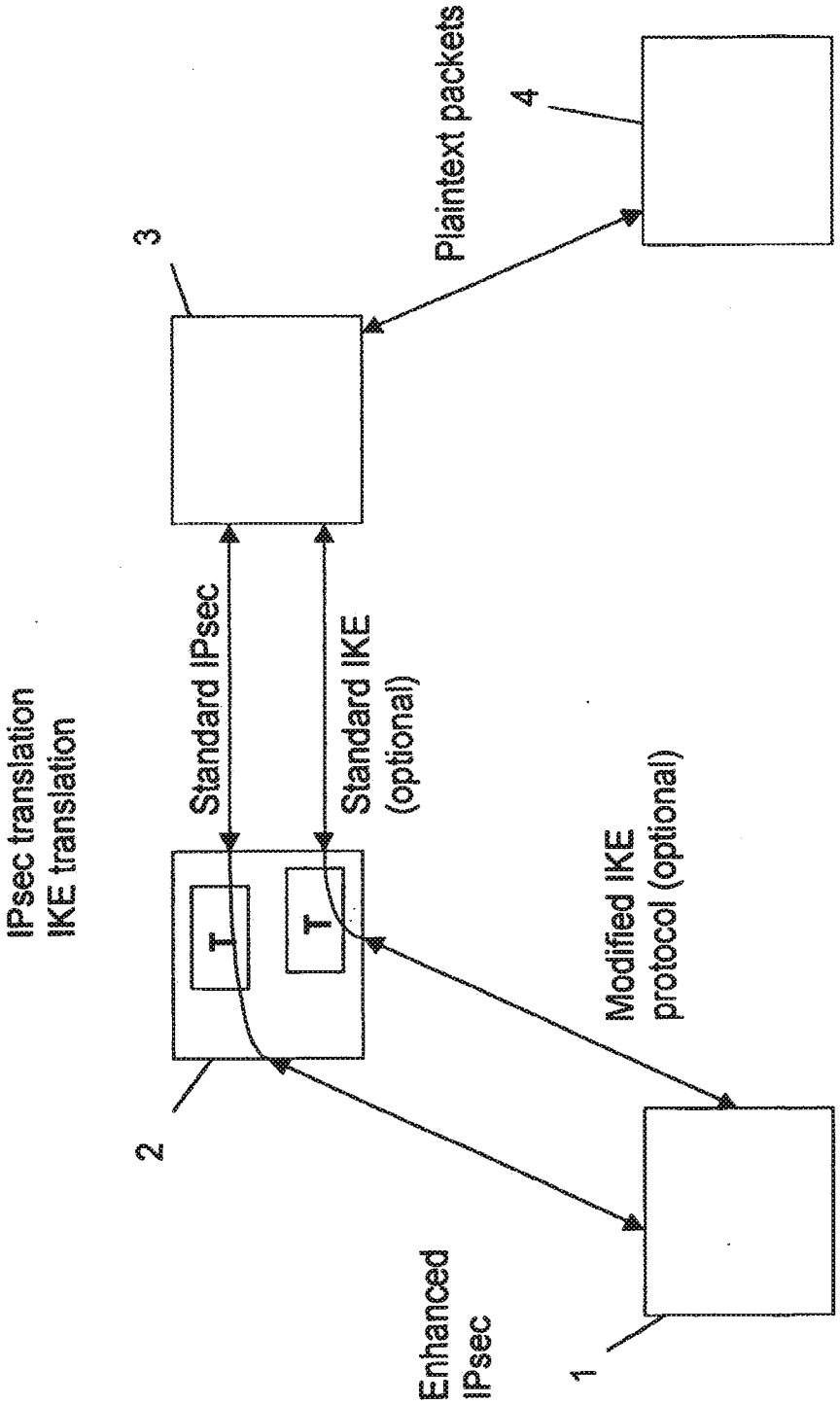

FIG. 1

Rec'd PCT/PTO 08 JUL 2004
PCT/FI03/00045
10/500930

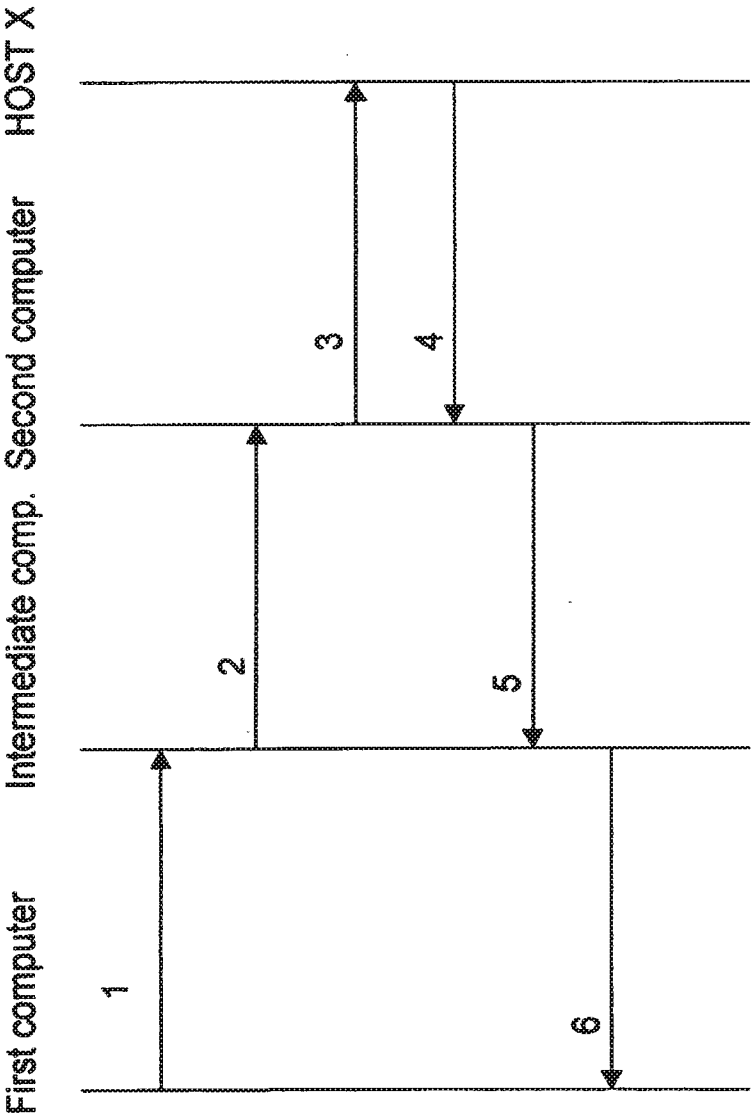

FIG. 2

Rec'd PCT/PTO 08 JUL 2004
PCT/FI03/00045
10/500930

c-addr-1	c-addr-2	c-SPI-1	c-SPI-2	s-addr-2	s-addr-3	s-SPI-2	s-SPI-3
195.1.2.3	212.90.65.1	0x80000001	0x12341234	212.90.65.1	103.6.5.4	0x1230012	0x56785678
...	...	...	...	...	...	...	...

FIG. 3

Rec'd PCT/PTO 08 JUL 2004
PCT/FI03/00045
10/500930

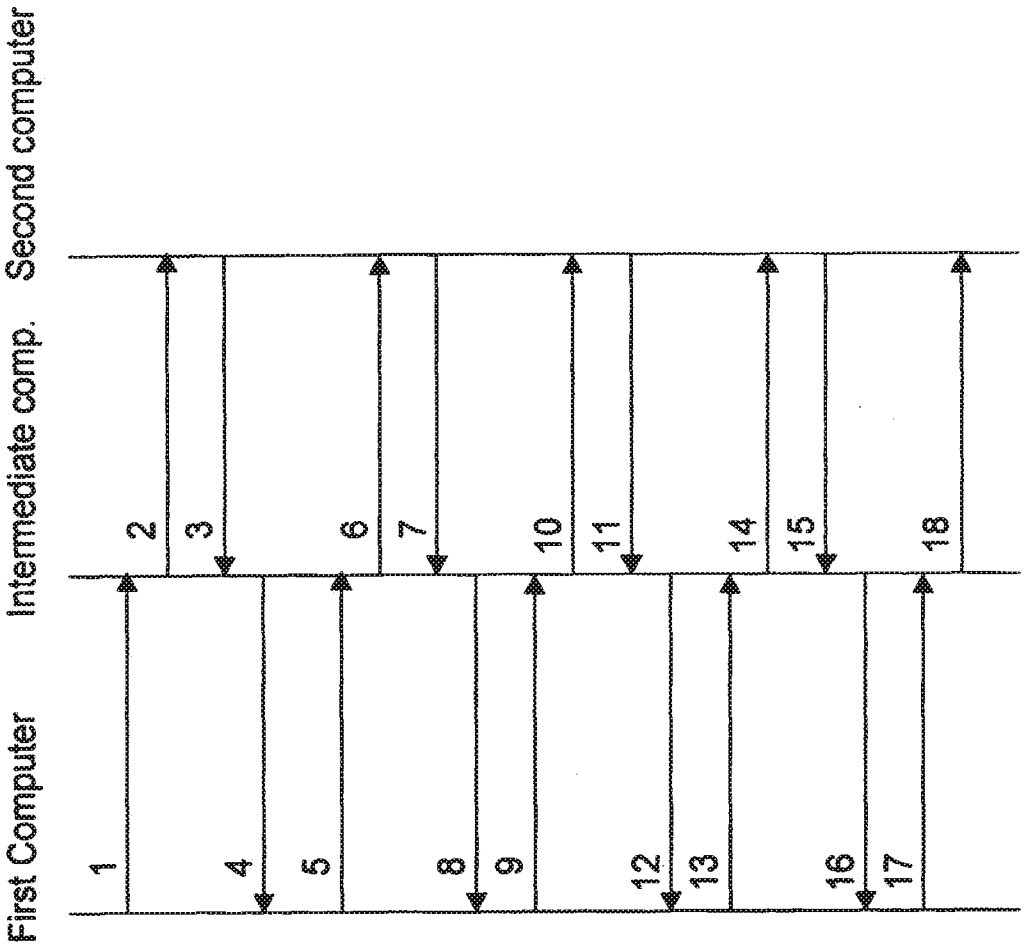

FIG. 4

Rec'd PCT/PTO 08 JUL 2004
PCT/FI03/00045
10/500930

Mapping field	Stage 1	Stage 2	Stage 3	Stage 4
c-addr-1	**195.1.2.3**	195.1.2.3	195.1.2.3	195.1.2.3
c-addr-2	**212.90.65.1**	212.90.65.1	212.90.65.1	212.90.65.1
c-icky	**CKY1**	CKY1	CKY1	CKY1
c-rcky	**0**	0	0	**CKY4**
c-userid	**joe@netseal.com**	joe@netseal.com	joe@netseal.com	joe@netseal.com
s-addr-2	n/a	**212.90.65.1**	212.90.65.1	212.90.65.1
s-addr-3	n/a	**103.6.5.4**	103.6.5.4	103.6.5.4
s-icky	n/a	**CKY2**	CKY2	CKY2
s-rcky	n/a	**0**	**CKY3**	CKY3

FIG. 5

Identification type	Identification value	SGW address
User@Fully-Qualified-Domain-Name	*.smith@netseal.com	123.1.2.3
user@Fully-Qualified-Domain-Name	*@netseal.com	103.6.5.4
Distinguished Name	"CN=Sami Vaarala, DC=netseal, DC=com"	122.4.3.2
Fully-Qualified-Domain-Name	host4.roammate.com	123.3.2.1
Employee number and company	"190170 / NetSeal Technologies"	123.4.3.2
...	...	...

FIG. 6

RF 12/7/16 664.1078CON2

POWER OF ATTORNEY BY APPLICANT FOR PATENT APPLICATION

I hereby revoke all previous powers of attorney given in the application identified in the attached transmittal letter. I am the applicant and the assignee to whom the inventors of the identified application are under an obligation to assign.

I hereby authorize Rolf Fasth, the U.S. attorney named herein, to accept and follow instructions from N/A as to any action to be taken in the U.S. Patent and Trademark Office regarding this application without direct communication between Rolf Fasth and the undersigned. In the event of a change in the persons from whom instructions may be taken, Rolf Fasth will be so notified by the undersigned.

I hereby appoint Rolf Fasth, Registration No. 36,999, to file and prosecute this application and to transact all business in the U.S. Patent and Trademark Office connected therewith.

Address all telephone calls to Rolf Fasth at telephone number (910) 687-0001; fax number (910) 295-2152.

Address all correspondence to:

PTO Customer No. 33369 (FASTH LAW OFFICES)

Date Dec 7TH, 2016

Signature

Name: Harri Yli-Kujala

Title and Company: CEO, MPH Technologies Oy.

ASSIGNMENT AND INVENTOR'S DECLARATION

WHEREAS, we, Sami Vaarala (Assignor 1) of Neljas Linja 22A, FIN-00503 Helsinki, Finland and Antti Nuopponen (Assignor 2) of Kaksoiskiventie 7-9 A1, FIN-02760 Espoo, Finland have invented a certain invention entitled METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION for which we are making application for Letters Patent of the United States, the specification of which is enclosed herewith; and

WHEREAS, MPH Technologies Oy (Assignee), a corporation organized under the laws of Finland, having an address at Keilaranta 1, FI-02150 Espoo, Finland, is desirous of acquiring the entire interest, title and interest in and to the application and invention, and to any United States patents to be obtained therefor:

NOW, THEREFORE, in consideration of good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, we, Sami Vaarala and Antti Nuopponen, hereby sell, assign and transfer to MPH Technologies Oy, its successors and assigns, the entire right, title and interest in and to said invention, patent application and patent rights in the United States including all rights of priority from the filing of the application; said invention, application and letters patent in the United States, all divisions, continuations, reissues and extensions thereof, including any right to bring or maintain an action for infringement under the provisional rights granted pursuant to Title 35, Section 154 of the United States Code or any other cause of action for acts which would constitute infringement occurring prior to this assignment, and including the right to claim priority under the International Convention of Paris (1883), as amended, or in any corresponding foreign patent application, and we request the Director of the U.S. Patent and Trademark Office to issue any Letters Patent granted upon the invention set forth in the application to MPH Technologies Oy,

its successors and assigns.

As a below named inventor, I hereby declare that this assignment and declaration is directed to the above-identified application having the title shown above. The above-identified application was made or was authorized to be made by me. I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby declare and acknowledge 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.

Legal name of first joint inventor: Sami Vaarala

Inventor's signature _____

Date _____, 2016

Residence: Helsinki, Finland

Citizenship: Finland

Post Office address: Neljas Linja 22A

FIN-00503 Helsinki, Finland

Legal name of second joint inventor: Antti Nuopponen

Inventor's signature _____

Date _____, 2016

Residence: Espoo, Finland

Citizenship: Finland

Post Office address: Kaksoiskiventie 7-9 A1

FIN-02760 Espoo, Finland

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION
First Named Inventor/Applicant Name:	Sami Vaarala
Filer:	Rolf Fasth/Sloan Smith
Attorney Docket Number:	664.1078CON2

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
UTILITY APPLICATION FILING	1011	1	280	280
UTILITY SEARCH FEE	1111	1	600	600
UTILITY EXAMINATION FEE	1311	1	720	720
Pages:				
Claims:				
CLAIMS IN EXCESS OF 20	1202	1	80	80
Miscellaneous-Filing:				
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**1680**

Electronic Acknowledgement Receipt

EFS ID:	27728204
Application Number:	15372208
International Application Number:	
Confirmation Number:	6275
Title of Invention:	METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION
First Named Inventor/Applicant Name:	Sami Vaarala
Customer Number:	33369
Filer:	Rolf Fasth/Sloan Smith
Filer Authorized By:	Rolf Fasth
Attorney Docket Number:	664.1078CON2
Receipt Date:	07-DEC-2016
Filing Date:	
Time Stamp:	18:46:22
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$1680
RAM confirmation Number	120816INTEFSW00007177060243
Deposit Account	060243
Authorized User	Sloan Smith

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

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

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	aia0014.pdf	1823528 4c096533ab081736d5be1a587963c7a037ff7a97	no	9
Warnings:					
Information:					
2	Transmittal of New Application	aia0015.pdf	276408 d46fb0dc7d61e03ab7068df32d0fddcc88ad15e3	no	2
Warnings:					
Information:					
3		APP.pdf	14018621 76809a318c144335245f9ed33dd34ef3d2a652c6	yes	76

Multipart Description/PDF files in .zip description

Document Description	Start	End
Abstract	76	76
Claims	70	75
Specification	1	69

Warnings:					
Information:					
4	Drawings-only black and white line drawings	FIGS.pdf	1726104 ae43ac2f790d9e7b00f5e1df89e3f2ccae0ed684	no	6
Warnings:					
Information:					
5	Power of Attorney	POA.pdf	866178 1eb57bf7bb5079e93075b5d52e4f2599d3b1de8a	no	1

Warnings:					
Information:					
6	Miscellaneous Incoming Letter	UNSIGNED_DECL.pdf	401056 4825448d67c8c57525eca8e7e9d21ddb459ea473	no	3
Warnings:					
Information:					
7	Fee Worksheet (SB06)	fee-info.pdf	36589 584917b275156ffd106da5ad4370a9152337be06	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	19148484		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

Electronic Acknowledgement Receipt

EFS ID:	27728204
Application Number:	15372208
International Application Number:	
Confirmation Number:	6275
Title of Invention:	METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION
First Named Inventor/Applicant Name:	Sami Vaarala
Customer Number:	33369
Filer:	Rolf Fasth/Sloan Smith
Filer Authorized By:	Rolf Fasth
Attorney Docket Number:	664.1078CON2
Receipt Date:	07-DEC-2016
Filing Date:	
Time Stamp:	18:46:22
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$1680
RAM confirmation Number	120816INTEFSW00007177060243
Deposit Account	060243
Authorized User	Sloan Smith

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

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

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	aia0014.pdf	1823528 4c096533ab081736d5be1a587963c7a037ff7a97	no	9
Warnings:					
Information:					
2	Transmittal of New Application	aia0015.pdf	276408 d46fb0dc7d61e03ab7068df32d0fddcc88ad15e3	no	2
Warnings:					
Information:					
3		APP.pdf	14018621 76809a318c144335245f9ed33dd34ef3d2a652c6	yes	76

Multipart Description/PDF files in .zip description

Document Description	Start	End
Abstract	76	76
Claims	70	75
Specification	1	69

Warnings:					
Information:					
4	Drawings-only black and white line drawings	FIGS.pdf	1726104 ae43ac2f790d9e7b00f5e1df89e3f2ccae0ed684	no	6
Warnings:					
Information:					
5	Power of Attorney	POA.pdf	866178 1eb57bf7bb5079e93075b5d52e4f2599d3b1de8a	no	1

Warnings:					
Information:					
6	Miscellaneous Incoming Letter	UNSIGNED_DECL.pdf	401056 4825448d67c8c57525eca8e7e9d21ddb459ea473	no	3
Warnings:					
Information:					
7	Fee Worksheet (SB06)	fee-info.pdf	36589 584917b275156ffd106da5ad4370a9152337be06	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	19148484		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	664.1078CON2
	Application Number	
Title of Invention	METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2:

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Sami		Vaarala	

Residence Information (Select One) US Residency ● Non US Residency Active US Military Service

City	Helsinki	Country of Residence [i]	FI

Mailing Address of Inventor:

Address 1	Neljas Linja 22A
Address 2	
City	FIN-00503 Helsinki
State/Province	
Postal Code	FI
Country [i]	FI

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Antti		Nuopponen	

Residence Information (Select One) US Residency ◉ Non US Residency Active US Military Service

City	Espoo	Country of Residence [i]	FI

Mailing Address of Inventor:

Address 1	Kaksoiskiventie 7-9 A1
Address 2	
City	FIN-02760 Espoo
State/Province	
Postal Code	FI
Country [i]	FI

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	664.1078CON2
	Application Number	
Title of Invention	METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION	

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	33369		
Email Address	sloan.smith@fasthlaw.com	Add Email	Remove Email

Application Information:

Title of the Invention	METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION		
Attorney Docket Number	664.1078CON2	**Small Entity Status Claimed**	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	6	**Suggested Figure for Publication (if any)**	

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	● Customer Number	US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	33369		

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	664.1078CON2
	Application Number	
Title of Invention	METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION	

Domestic Benefit/National Stage Information:

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

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Continuation of	13685544	2012-11-26
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13685544	Continuation of	10500930	2005-10-19
Prior Application Status	Patented		Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
10500930	a 371 of international	PCTFI0300045	2003-01-21	8346949	2013-01-01

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)[i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Remove

Application Number	Country[i]	Filing Date (YYYY-MM-DD)	Access Code[i] (if applicable)
20020112	FI	2002-01-22	

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

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

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	664.1078CON2
	Application Number	
Title of Invention	METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION	

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	664.1078CON2
	Application Number	
Title of Invention	METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION	

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	664.1078CON2
	Application Number	
Title of Invention	METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION	

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1 — Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

● Assignee	Legal Representative under 35 U.S.C. 117	Joint Inventor
Person to whom the inventor is obligated to assign.	Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor:

If the Applicant is an Organization check here. ☒

Organization Name	MPH Technologies Oy		
Mailing Address Information For Applicant:			
Address 1	Keilaranta 1		
Address 2			
City	FI-02150 Espoo	**State/Province**	
Country	FI	Postal Code	FI
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	664.1078CON2
	Application Number	
Title of Invention	METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION	

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). **However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).**

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/rfasth/			Date (YYYY-MM-DD)	2016-12-07
First Name	Rolf	Last Name	Fasth	Registration Number	36999

Additional Signature may be generated within this form by selecting the Add button. Add

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	664.1078CON2
	Application Number	
Title of Invention	METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION	

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

Document code: WFEE

United States Patent and Trademark Office
Sales Receipt for Accounting Date: 12/15/2016

ASAHLE SALE #00000031 Mailroom Dt: 12/07/2016 060243 15372208
01 FC : 1051 140.00 DA