



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

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
10/500,930 10/19/2005 Sami Vaarala 290.1078USN 1571

33369 7590 11/21/2017
FASTH LAW OFFICES (ROLF FASTH)
1206 Stanridge Drive
Raleigh, NC 27613-7063

EXAMINER

TOWFIGHI, AFSHAWN M

ART UNIT PAPER NUMBER

2469

NOTIFICATION DATE DELIVERY MODE

11/21/2017

ELECTRONIC

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

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

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

sloan.smith@fasthlaw.com



UNITED STATES PATENT AND TRADEMARK OFFICE

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

Patent No.: 8346949
Issue Date: 01 January 2013
Appl. No.: 10/500,930
Filed: 19 October 2005

PART (A) RESPONSE FOR CERTIFICATES OF CORRECTION

This is a decision on the Certificate of Correction request filed 12 October 2017.

The request for issuance of Certificate of Correction for the above-identified correction(s) under the provisions of 37 CFR 1.322 and/or 1.323 is hereby:

(Check one)

Approved Approved in Part Denied

Comments: _____

PART (B) PETITION UNDER 37 CFR 1.324 OR 37 CFR 1.48

This is a decision on the petition filed _____ to correct inventorship under 37 CFR 1.324.

This is a decision on the request under 37 CFR 1.48, petition filed _____. In view of the fact that the patent has already issued, the request under 37 CFR 1.48 has been treated as a petition to correct inventorship under 37 CFR 1.324.

The petition is hereby: Granted Dismissed

Comment: _____

The patented filed is being forwarded to Certificate of Corrections Branch for issuance of a certificate naming only the actual inventor or inventors.

/Ian N Moore/
Supervisory Patent Examiner, Art Unit 2469
Technology Center 2400
Phone: (571)272-3085

Certificates of Correction Branch email: CustomerServiceCoC@uspto.gov CoC Central Phone Number: (703) 756-1814

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 8,346,949 B2
APPLICATION NO. : 10/500930
DATED : January 1, 2013
INVENTOR(S) : Sami Vaarala and Antti Nuopponen

Page 1 of 1

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

In the Claims

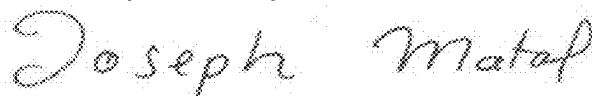
Column 22, Line 10: delete “the first computer and the second computer” negotiating and exchanging keys with one another,

Column 22, Line 20: delete “in the first computer” forming a secure message,

Column 22, Line 33: delete “the intermediate computer” substituting, at the intermediate computer,

Column 22, Line 36: delete “the intermediate computer” forwarding, at the intermediate computer,

Signed and Sealed this
Twenty-first Day of November, 2017



Joseph Matal
*Performing the Functions and Duties of the
Under Secretary of Commerce for Intellectual Property and
Director of the United States Patent and Trademark Office*

**UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION**Page 1 of 1

PATENT NO. : 8,346,949

APPLICATION NO.: 10/500,930

ISSUE DATE : 1 January 2013

INVENTOR(S) : Sami Vaarala, Antti Nuopponen

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

Col. 22, line 10: delete "the first computer and the second computer" negotiating and exchanging keys with one another,

Col. 22, line 20: delete "in the first computer" forming a secure message,

Col. 22, line 33: delete "the intermediate computer" substituting, at the intermediate computer,

Col. 22, line 36: delete "the intermediate computer" forwarding, at the intermediate computer,

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

FASTH LAW OFFICES
1206 Stanridge Drive
Raleigh, NC 27613

This collection of information is required by 37 CFR 1.322, 1.323, and 1.324. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1.0 hour to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Attention Certificate of Corrections Branch, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Privacy Act Statement

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

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

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
Attorney Ref. No. 290.1078USN

In re application of
 Sami Vaarala, Antti Nuopponen
 Serial No. 10/500,930

Art Unit 2469
 Confirmation No. 1571

CERTIFICATE OF MAILING

Filed: 19 October 2005

I HEREBY CERTIFY THAT THIS PAPER AND THE DOCUMENTS
 REFERRED TO AS BEING ATTACHED OR ENCLOSED HERewith
 ARE BEING SUBMITTED ELECTRONICALLY TO THE UNITED
 STATES PATENT AND TRADEMARK OFFICE ON **12 October**
2017.

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

/rfasth/

Examiner: Afshawn M. Towfighi

 Rolf Fasth
 Attorney for Applicant

Date: 12 October 2017

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) Request for Certificate of Correction due to USPTO error
- (X) The Commissioner is hereby authorized to charge any 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. 290.1078USN

Electronic Acknowledgement Receipt

EFS ID:	30634917
Application Number:	10500930
International Application Number:	
Confirmation Number:	1571
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:	290.1078USN
Receipt Date:	12-OCT-2017
Filing Date:	19-OCT-2005
Time Stamp:	11:43:25
Application Type:	U.S. National Stage under 35 USC 371

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	Request for Certificate of Correction	sb0044.pdf	170774 c98c25f0c4989e3a38daa5590b0a53f4d8f9c424	no	2

Warnings:

Information:					
2	Transmittal Letter	TRX.pdf	246703	no	1
			dc2aa54b0fbd4938b85f6deeaac617f8437c65fa		
Warnings:					
Information:					
Total Files Size (in bytes):				417477	
<p>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.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					



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

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
10/500,930 10/19/2005 Sami Vaarala 290.1078USN 1571

33369 7590 09/22/2017
FASTH LAW OFFICES (ROLF FASTH)
1206 Stanridge Drive
Raleigh, NC 27613-7063

EXAMINER

TOWFIGHI, AFSHAWN M

ART UNIT PAPER NUMBER

2469

NOTIFICATION DATE DELIVERY MODE

09/22/2017

ELECTRONIC

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

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

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

sloan.smith@fasthlaw.com

Applicant-Initiated Interview Summary	Application No. 10/500,930	Applicant(s) VAARALA ET AL.	
	Examiner AFSHAWN TOWFIGHI	Art Unit 2469	

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

(1) AFSHAWN TOWFIGHI. (3)_____.

(2) Rolf Fasth. (4)_____.

Date of Interview: 18 September 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: 1-29.

Identification of prior art discussed: _____.

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...)

Mr. Fasth pointed out that the issued patent does not contain the examiner's amendment from 1/12/12. Examiner confirmed, and informed Mr. Fasth that the best course of action at this time would be to file a certificate of correction.

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

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

Attachment

/AFSHAWN TOWFIGHI/
Primary Examiner, Art Unit 2469

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record

A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews

Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.

All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:

- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:

- 1) A brief description of the nature of any exhibit shown or any demonstration conducted,
- 2) an identification of the claims discussed,
- 3) an identification of the specific prior art discussed,
- 4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
- 5) a brief identification of the general thrust of the principal arguments presented to the examiner,
(The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
- 6) a general indication of any other pertinent matters discussed, and
- 7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Sami Vaarala, Antti Nuopponen Art Unit 2469

Patent No. 8,346,949

5 Issued: 1 January 2013
METHOD AND SYSTEM FOR SENDING A

MESSAGE THROUGH A SECURE CONNECTION

Examiner: Afshawn M. Towfighi Date: 3 January 2013

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

15 **LOSS OF SMALL ENTITY STATUS**

This is a notice of LOSS OF SMALL ENTITY STATUS under 37 CFR
1.28 for the above issued patent. Applicant was notified on
28 September 2012 that the assignor had not been entitled to
20 small entity status since June 2010. The issue fee and
publication fee have been paid at the large entity rate.
Applicant was unintentionally deficient in the following
payments:

25 8 April 2011	RCE	\$405 paid,	<u>\$525 due</u>
7 Nov 2011	2-month EXT	\$635 paid,	<u>\$655 due</u>
18 Jan 2012	RCE	\$465 paid,	<u>\$465 due</u>

30 The Commissioner is hereby authorized to charge **\$1645** in
deficient fees itemized above and any additional fees which
may be required in connection with the filing of this
correspondence, or credit over-payment, to Account
No. 06-0243.

35 Respectfully submitted,

FASTH LAW OFFICES

/rfasth/

Rolf Fasth

Registration No. 36,999

40 FASTH LAW OFFICES
26 Pinecrest Plaza, Suite 2
Southern Pines, NC 28387-4301
Telephone: (910) 687-0001
Facsimile: (910) 295-2152
45 Email: rolf.fasth@fasthlaw.com

Electronic Acknowledgement Receipt

EFS ID:	14609619
Application Number:	10500930
International Application Number:	
Confirmation Number:	1571
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:	290.1078USN
Receipt Date:	03-JAN-2013
Filing Date:	19-OCT-2005
Time Stamp:	16:28:23
Application Type:	U.S. National Stage under 35 USC 371

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	Post Allowance Communication - Incoming	LOSS_ENTITY.pdf	62744 e964f67c45e3501c9f04b52f740a0ba1edfa d05f	no	1

Warnings:

Information:

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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



APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/500,930	01/01/2013	8346949	290.1078USN	1571

33369 7590 12/12/2012
FASTH LAW OFFICES (ROLF FASTH)
26 PINECREST PLAZA, SUITE 2
SOUTHERN PINES, NC 28387-4301

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 959 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, Espoo, FINLAND;
Antti Nuopponen, Espoo, FINLAND;

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

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 06/29/2012
 FASTH LAW OFFICES (ROLF FASTH)
 26 PINECREST PLAZA, SUITE 2
 SOUTHERN PINES, NC 28387-4301

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)
29 Nov. 2012	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/500,930	10/19/2005	Sami Vaarala	290.1078USN	1571

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

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES NO	\$870 \$1770	\$300	\$0	\$170 \$2070	11/29/2012
EXAMINER		ART UNIT	CLASS-SUBCLASS			
TOWEIGHI, AFSHAWN M		2469	709-229000			

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

(B) RESIDENCE (CITY AND STATE OR COUNTRY)

MPH TECHNOLOGIES OY

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 credit any overpayment, to Deposit Account Number 060243 (enclose an extra copy of this form).

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

- a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27. b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature /rfasth/

Date 29 November 2012

Typed or printed name Rolf Fasth

Registration No. 36,999

This collection of information 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.

Electronic Patent Application Fee Transmittal

Application Number:	10500930
Filing Date:	19-Oct-2005
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:	290.1078USN

Filed as Large Entity

U.S. National Stage under 35 USC 371 Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl issue fee	1501	1	1770	1770
Publ. Fee- early, voluntary, or normal	1504	1	300	300

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				2070

Electronic Acknowledgement Receipt

EFS ID:	14322959
Application Number:	10500930
International Application Number:	
Confirmation Number:	1571
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:	290.1078USN
Receipt Date:	28-NOV-2012
Filing Date:	19-OCT-2005
Time Stamp:	09:28:54
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$2070
RAM confirmation Number	8919
Deposit Account	060243
Authorized User	

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

Charge any Additional Fees required under 37 C.F.R. 1.492 (National application filing, search, and examination fees)

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

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

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

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	TRX.pdf	66512 ff2f92ee4b0f33016f94213a1559e63d68bfd5bd	no	1

Warnings:

Information:

2	Issue Fee Payment (PTO-85B)	PART_B.pdf	1881195 0e02380cd4b2ad0e120626da7649181c4802e83a	no	1
---	-----------------------------	------------	---	----	---

Warnings:

Information:

3	Fee Worksheet (SB06)	fee-info.pdf	31946 30a92d0789195f8b6c7a3e51d3cd13ce50a47fcd	no	2
---	----------------------	--------------	---	----	---

Warnings:

Information:

Total Files Size (in bytes):

1979653

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of
Sami Vaarala, Antti Nuopponen

Art Unit 2469
Confirmation No. 1571

Serial No. 10/500,930

Filed: 19 October 2005

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

CERTIFICATE OF MAILING

I HEREBY CERTIFY THAT THIS PAPER AND THE DOCUMENTS
REFERRED TO AS BEING ATTACHED OR ENCLOSED HERewith
ARE BEING ELECTRONICALLY SUBMITTED TO THE
COMMISSIONER FOR PATENTS, P.O. BOX 1450,
ALEXANDRIA, VA 22313-1450 ON 28 November 2012.

/rfasth/

Rolf Fasth
Attorney for Applicant

Examiner: Afshawn M.
Towfighi

Date: 28 November 2012

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 and Publication Fee (\$1170;)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
26 Pinecrest Plaza, Suite 2
Southern Pines, NC 28387-4301
Telephone: 910-687-0001
Facsimile: 910-295-2152
Attorney Ref. No. 290.1078USN

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)
26 PINECREST PLAZA, SUITE 2
SOUTHERN PINES, NC 28387-4301



**Courtesy Reminder for
Application Serial No: 10/500,930**

Attorney Docket No: 290.1078USN

Customer Number: 33369

Date of Electronic Notification: 08/29/2012

This is a courtesy reminder that new correspondence is available for this application. 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

nan_russell@fasthlaw.com

Please verify that these email addresses are correct.

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.



NOTICE OF ALLOWANCE AND FEE(S) DUE

33369 7590 08/29/2012
FASTH LAW OFFICES (ROLF FASTH)
26 PINECREST PLAZA, SUITE 2
SOUTHERN PINES, NC 28387-4301

EXAMINER
TOWFIGHI, AFSHAWN M
ART UNIT
PAPER NUMBER

2469

DATE MAILED: 08/29/2012

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.

10/500,930 10/19/2005 Sami Vaarala 290.1078USN 1571

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

Table with 7 columns: APPLN. TYPE, SMALL ENTITY, ISSUE FEE DUE, PUBLICATION FEE DUE, PREV. PAID ISSUE FEE, TOTAL FEE(S) DUE, DATE DUE

nonprovisional YES \$870 \$300 \$0 \$1170 11/29/2012

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 SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

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)

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.

33369 7590 08/29/2012
FASTH LAW OFFICES (ROLF FASTH)
 26 PINECREST PLAZA, SUITE 2
 SOUTHERN PINES, NC 28387-4301

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.
-----------------	-------------	----------------------	---------------------	------------------

10/500,930 10/19/2005 Sami Vaarala 290.1078USN 1571

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

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
-------------	--------------	---------------	---------------------	----------------------	------------------	----------

nonprovisional YES \$870 \$300 \$0 \$1170 11/29/2012

EXAMINER	ART UNIT	CLASS-SUBCLASS
----------	----------	----------------

TOWFIGHI, AFSHAWN M 2469 709-229000

<p>1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).</p> <p><input type="checkbox"/> Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.</p> <p><input type="checkbox"/> "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.</p>	<p>2. For printing on the patent front page, list</p> <p>(1) the names of up to 3 registered patent attorneys or agents OR, alternatively, 1 _____</p> <p>(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. 2 _____</p> <p>3 _____</p>
---	---

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

<p>4a. The following fee(s) are submitted:</p> <p><input type="checkbox"/> Issue Fee</p> <p><input type="checkbox"/> Publication Fee (No small entity discount permitted)</p> <p><input type="checkbox"/> Advance Order - # of Copies _____</p>	<p>4b. Payment of Fee(s); (Please first reapply any previously paid issue fee shown above)</p> <p><input type="checkbox"/> A check is enclosed.</p> <p><input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached.</p> <p><input type="checkbox"/> The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).</p>
---	--

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

a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27. b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information 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.



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

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
10/500,930 10/19/2005 Sami Vaarala 290.1078USN 1571

33369 7590 08/29/2012
FASTH LAW OFFICES (ROLF FASTH)
26 PINECREST PLAZA, SUITE 2
SOUTHERN PINES, NC 28387-4301

EXAMINER

TOWFIGHI, AFSHAWN M

ART UNIT PAPER NUMBER

2469

DATE MAILED: 08/29/2012

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)

(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 746 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 746 day(s).

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 Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

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.

10/500,930

Examiner

AFSHAWN TOWFIGHI

Applicant(s)

VAARALA ET AL.

Art Unit

2469

-- 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 1/18/12.
- 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 1-29.
- 4. Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some* c) None of 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. A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 - 6. CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) hereto or 2) to Paper No./Mail Date _____.
 - (b) 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).**
- 7. 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. Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3. Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 1/18/2012
- 4. Examiner's Comment Regarding Requirement for Deposit of Biological Material
- 5. Notice of Informal Patent Application
- 6. Interview Summary (PTO-413), Paper No./Mail Date _____ .
- 7. Examiner's Amendment/Comment
- 8. Examiner's Statement of Reasons for Allowance
- 9. Other _____.

/A. T./
Examiner, Art Unit 2469

/IAN N. MOORE/
Supervisory Patent Examiner, Art Unit 2469

DETAILED ACTION

Information Disclosure Statement

1. The information disclosure statement (IDS) submitted on 1/18/12 has been considered by the examiner.

Allowable Subject Matter

2. Claims 1-29 (amended) are allowed.
3. The following is an examiner's statement of reasons for allowance:
Amended claims 1-29 are allowable for the same reasons indicated in the Notice of Allowance mailed on 1/12/12 and are allowable over prior art since the prior art reference(s) taken individually or in combination fails to particularly disclose, fairly suggests, or render obvious as argued by the applicant which examiner considers as persuasive as set forth above.

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

Art Unit: 2469

(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.

/A. T./
Examiner, Art Unit 2469

/IAN N. MOORE/
Supervisory Patent Examiner, Art Unit 2469




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. 1571

SERIAL NUMBER 10/500,930	FILING or 371(c) DATE 10/19/2005 RULE	CLASS 709	GROUP ART UNIT 2469	ATTORNEY DOCKET NO. 290.1078USN	
APPLICANTS Sami Vaarala, Espoo, FINLAND; Antti Nuopponen, Espoo, FINLAND; ** CONTINUING DATA ***** This application is a 371 of PCT/FI03/00045 01/21/2003 ** FOREIGN APPLICATIONS ***** FINLAND 20020112 01/22/2002 ** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** ** SMALL ENTITY **					
Foreign Priority claimed <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No 35 USC 119(a-d) conditions met <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Verified and /AFSHAWN M TOWFIGHI/ Acknowledged Examiner's Signature _____	<input type="checkbox"/> Met after Allowance _____ Initials	STATE OR COUNTRY FINLAND	SHEETS DRAWINGS 6	TOTAL CLAIMS 26	INDEPENDENT CLAIMS 2
ADDRESS FASTH LAW OFFICES (ROLF FASTH) 26 PINECREST PLAZA, SUITE 2 SOUTHERN PINES, NC 28387-4301 UNITED STATES					
TITLE METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION					
FILING FEE RECEIVED 657	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:		<input type="checkbox"/> All Fees <input type="checkbox"/> 1.16 Fees (Filing) <input type="checkbox"/> 1.17 Fees (Processing Ext. of time) <input type="checkbox"/> 1.18 Fees (Issue) <input type="checkbox"/> Other _____ <input type="checkbox"/> Credit		

Search Notes 	Application/Control No. 10500930	Applicant(s)/Patent Under Reexamination VAARALA ET AL.
	Examiner Afshawn Towfighi	Art Unit 2469

SEARCHED			
Class	Subclass	Date	Examiner
709	236, 229, 245	11-5-2008	JS
ABOVE	UPDATED	12/28/2011	AT
ABOVE	UPDATED	8/12/2012	AT

SEARCH NOTES		
Search Notes	Date	Examiner
Limited classification of 709/229, 245	11-5-2008	JS
Inventor search	11-5-2008 (Updated 12/28/11) (Updated 8/12/12)	JS
Text search of EAST (US Pat, US PG Pub, JPO, EPO, Derwent)	11-5-2008	JS
Updated Text search of EAST (see attached history)	5-28-2009	JS
Updated text search of EAST (see attached history)	9-8-09	JS
EAST search with previous examiner's classes and focus on new limitations	3/15/2010	AT
Conf with B.Bruckart and J.Avellino - Reopen and search IPsec/tunneling/gateway/proxy	8/21/2010	AT
Updated EAST search - see attached	8/21/2010	AT
EAST (USPAT, USPGPUB) - see search history printout (Updated 4/28/11)	1/17/2011 (Updated 4/28/11) (Updated 12/28/11)	AT

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner
	Interference Search - see search history printout	12/28/2011	AT

--	--

Receipt date: 01/18/2012

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)

Approved for use through 07/31/2012. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		10500930
	Filing Date		2005-10-19
	First Named Inventor	Sami Vaarala	
	Art Unit	2469	
	Examiner Name	Afshawn M. Towfigh	
	Attorney Docket Number	290.1078USN	

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6732269		2004-05-04	Baskey, Michael Edward et al.	
	2	6718388		2004-04-06	Yarborough, William Jordan et al.	
	3	6957346		2005-10-18	Kivinen, Tero et al.	
	4	6795917		2004-09-21	Ylonen, Tatu	

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

U.S.PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

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

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

Receipt date: 01/18/2012 INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		10500930	
	Filing Date		2005-10-19	
	First Named Inventor	Sami Vaarala		
	Art Unit	2469		
	Examiner Name	Afshawn M. Towfighi		
	Attorney Docket Number	290.1078USN		

1								<input type="checkbox"/>
---	--	--	--	--	--	--	--	--------------------------

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

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	ARI LUOTONEN, "Tunneling SSL Through a WWW Proxy" Internet draft memo, March 26, 1997.	<input type="checkbox"/>
	2	ARI LUOTONEN, "Tunneling TCP based protocols through Web proxy servers" Internet draft memo, August 1998.	<input type="checkbox"/>
	3		<input type="checkbox"/>

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

EXAMINER SIGNATURE

Examiner Signature	/Afshawn Towfighi/	Date Considered	08/12/2012
--------------------	--------------------	-----------------	------------

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		10500930
	Filing Date		2005-10-19
	First Named Inventor	Sami Vaarala	
	Art Unit		2469
	Examiner Name	Afshawn M. Towfighi	
	Attorney Docket Number		290.1078USN

CERTIFICATION STATEMENT

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

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

OR

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

- See attached certification statement.
- The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.
- A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/rfasth/	Date (YYYY-MM-DD)	2012-01-17
Name/Print	Rolf Fasth	Registration Number	36999

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

Privacy Act Statement

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

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

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.T./

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L2	5426	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L3	15	L2 and secure near10 key near10 exchang\$3	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L4	544	ipsec same tunnel\$3 same IKE	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L5	170	ipsec same tunnel\$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L6	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2012/08/12 17:25
L7	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
L8	21	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L9	3132	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L10	2700	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L11	2700	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L12	2068	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L13	2068	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L14	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L15	5426	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L16	15	L15 and secure near10 key near10 exchang\$3	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L17	544	ipsec same tunnel\$3 same IKE	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L18	170	ipsec same tunnel\$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L19	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2012/08/12 17:25
L20	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

L21	21	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L22	3132	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L23	2700	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L24	2700	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L25	2068	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L26	2068	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L27	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L28	5426	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L29	15	L28 and secure near10 key near10 exchang\$3	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L30	544	ipsec same tunnel\$3 same IKE	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L31	170	ipsec same tunnel\$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L32	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2012/08/12 17:25
L33	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
L34	21	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L35	3132	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L36	2700	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L37	2700	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L38	2068	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L39	2068	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L40	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L41	5426	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L42	15	L41 and secure near10 key near10 exchang\$3	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L43	544	ipsec same tunnel\$3 same IKE	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L44	170	ipsec same tunnel\$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L45	2	"US 20060173968"	US-PGPUB; USPAT; USOCR;	OR	OFF	2012/08/12 17:25

			DERWENT			
L46	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
L47	21	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L48	3132	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L49	2700	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L50	2700	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L51	2068	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L52	2068	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L53	4	"7882538"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L54	20	"6744741"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L55	19	"7055027"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L56	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L57	5426	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L58	15	L57 and secure near10 key near10 exchang\$3	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L59	544	ipsec same tunnel\$3 same IKE	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L60	170	ipsec same tunnel\$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L61	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2012/08/12 17:25
L62	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
L63	21	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L64	3132	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L65	2700	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L66	2700	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L67	2068	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L68	2068	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L69	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L70	5426	709/236.ccls. or 709/245.ccls.	US-PGPUB;	OR	OFF	2012/08/12

			USPAT			17:25
L71	15	L70 and secure near10 key near10 exchang\$3	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L72	544	ipsec same tunnel\$3 same IKE	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L73	170	ipsec same tunnel\$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L74	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2012/08/12 17:25
L75	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
L76	21	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L77	3132	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L78	2700	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L79	2700	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L80	2068	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L81	2068	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L82	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L83	5426	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L84	15	L83 and secure near10 key near10 exchang\$3	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L85	544	ipsec same tunnel\$3 same IKE	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L86	170	ipsec same tunnel\$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L87	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2012/08/12 17:25
L88	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
L89	21	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L90	3132	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L91	2700	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L92	2700	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L93	2068	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L94	2068	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25

L95	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L96	5426	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L97	15	L96 and secure near10 key near10 exchang\$3	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L98	544	ipsec same tunnel\$3 same IKE	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L99	170	ipsec same tunnel\$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L100	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2012/08/12 17:25
L101	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
L102	21	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L103	3132	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L104	2700	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L105	2700	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L106	2068	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L107	2068	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L108	4	"7882538"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L109	20	"6744741"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L110	19	"7055027"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L111	9	((SAMI) near2 (VAARALA)).INV.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L112	9	((ANTTI) near2 (NUOPPONEN)).INV.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L113	9	L111 or L112	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L114	8	L113 and (secure adj connection).clm.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L115	7	L113 and (secure adj connection with address).clm.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L116	1	L113 and (secure adj connection with intermediate with address).clm.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:25
L120	107613	("6732269" "6718388" "6957346" "6795917").pn"	US-PGPUB; USPAT; EPO; JPO	OR	ON	2012/08/12 17:47
L121	4	("6732269" "6718388" "6957346" "6795917").pn.	US-PGPUB; USPAT; EPO; JPO	OR	ON	2012/08/12 17:47
L122	5426	709/236.ccls. or 709/245.ccls.	US-PGPUB;	OR	OFF	2012/08/12

			USPAT			17:57
L123	3132	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L124	2700	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L125	2700	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L126	2068	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L127	5426	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L128	3132	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L129	2700	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L130	2700	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L131	2068	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L132	5426	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L133	3132	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L134	2700	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L135	2700	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L136	2068	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L137	5426	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L138	3132	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L139	2700	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L140	2700	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L141	2068	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L142	4	"7882538"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L143	5426	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L144	3132	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L145	2700	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L146	2700	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L147	2068	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L148	5426	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L149	3132	ipsec same (ssl or tls)	US-PGPUB;	OR	OFF	2012/08/12

			USPAT			17:57
L150	2700	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L151	2700	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L152	2068	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L153	5426	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L154	3132	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L155	2700	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L156	2700	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L157	2068	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L158	5426	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L159	3132	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L160	2700	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L161	2700	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L162	2068	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L163	4	"7882538"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L164	9	L111 or L112	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L165	8	L113 and (secure adj connection).clm.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L166	7	L113 and (secure adj connection with address).clm.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L167	1	L113 and (secure adj connection with intermediate with address).clm.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L171	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L172	15	L2 and secure near10 key near10 exchang\$3	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L173	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2012/08/12 17:57
L174	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
L175	21	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L176	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L177	15	L15 and secure near10 key near10 exchang\$3	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57

L178	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2012/08/12 17:57
L179	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
L180	21	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L181	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L182	15	L28 and secure near10 key near10 exchang\$3	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L183	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2012/08/12 17:57
L184	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
L185	21	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L186	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L187	15	L41 and secure near10 key near10 exchang\$3	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L188	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2012/08/12 17:57
L189	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
L190	21	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L191	20	"6744741"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L192	19	"7055027"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L193	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L194	15	L57 and secure near10 key near10 exchang\$3	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L195	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2012/08/12 17:57
L196	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
L197	21	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L198	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L199	15	L70 and secure near10 key near10 exchang\$3	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L200	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2012/08/12 17:57

L201	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
L202	21	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L203	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L204	15	L83 and secure near10 key near10 exchang\$3	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L205	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2012/08/12 17:57
L206	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
L207	21	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L208	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L209	15	L96 and secure near10 key near10 exchang\$3	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L210	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2012/08/12 17:57
L211	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
L212	21	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L213	20	"6744741"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L214	19	"7055027"	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L215	9	((SAMI) near2 (VAARALA)).INV.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L216	9	((ANTTI) near2 (NUOPPONEN)).INV.	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L217	170	ipsec same tunnel\$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L218	170	ipsec same tunnel\$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L219	170	ipsec same tunnel\$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L220	170	ipsec same tunnel\$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L221	170	ipsec same tunnel\$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L222	170	ipsec same tunnel\$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L223	170	ipsec same tunnel\$3 same IKE	US-PGPUB;	OR	OFF	2012/08/12

		same (gateway or proxy or intermediate)	USPAT			17:57
L224	170	ipsec same tunnel\$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L225	544	ipsec same tunnel\$3 same IKE	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L226	544	ipsec same tunnel\$3 same IKE	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L227	544	ipsec same tunnel\$3 same IKE	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L228	544	ipsec same tunnel\$3 same IKE	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L229	544	ipsec same tunnel\$3 same IKE	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L230	544	ipsec same tunnel\$3 same IKE	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L231	544	ipsec same tunnel\$3 same IKE	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L232	544	ipsec same tunnel\$3 same IKE	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L233	2068	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L234	2068	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L235	2068	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L236	2068	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L237	2068	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L238	2068	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L239	2068	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L240	2068	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2012/08/12 17:57
L241	107613	("6732269" "6718388" "6957346" "6795917").pn	US-PGPUB; USPAT; EPO; JPO	OR	ON	2012/08/12 17:57
L242	4	("6732269" "6718388" "6957346" "6795917").pn.	US-PGPUB; USPAT; EPO; JPO	OR	ON	2012/08/12 17:57


EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L117	1	(secure adj connection with intermediate with address).clm.	USPAT; UPAD	OR	OFF	2012/08/12 17:25
L118	14	(secure adj connection with (intermediate or gateway or proxy) with address).clm.	USPAT; UPAD	OR	OFF	2012/08/12 17:25
L119	1	(secure adj connection with (intermediate or gateway or proxy) with (key or token) with address).clm.	USPAT; UPAD	OR	OFF	2012/08/12 17:25

L168	1	(secure adj connection with intermediate with address).clm.	USPAT; UPAD	OR	OFF	2012/08/12 17:57
L169	14	(secure adj connection with (intermediate or gateway or proxy) with address).clm.	USPAT; UPAD	OR	OFF	2012/08/12 17:57
L170	1	(secure adj connection with (intermediate or gateway or proxy) with (key or token) with address).clm.	USPAT; UPAD	OR	OFF	2012/08/12 17:57

8/ 12/ 2012 6:15:08 PM


C:\Users\atowfighi\Documents\EAST\Workspaces\jeff930.wsp

Issue Classification 	Application/Control No. 10500930	Applicant(s)/Patent Under Reexamination VAARALA ET AL.
	Examiner AFSHAWN TOWFIGHI	Art Unit 2469

ORIGINAL					INTERNATIONAL CLASSIFICATION												
CLASS		SUBCLASS			CLAIMED					NON-CLAIMED							
709		229			G	0	6	F	15 / 16 (2006.01.01)								
CROSS REFERENCE(S)																	
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)																
726	3																

<input checked="" type="checkbox"/> Claims renumbered in the same order as presented by applicant <input type="checkbox"/> CPA <input type="checkbox"/> T.D. <input type="checkbox"/> R.1.47															
Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original

/AFSHAWN TOWFIGHI/ Examiner.Art Unit 2469 (Assistant Examiner)	8/12/12 (Date)	Total Claims Allowed: 29	
/IAN N MOORE/ Supervisory Patent Examiner.Art Unit 2469 (Primary Examiner)	08/15/2012 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 1

Index of Claims 	Application/Control No. 10500930	Applicant(s)/Patent Under Reexamination VAARALA ET AL.
	Examiner AFSHAWN TOWFIGHI	Art Unit 2469

✓	Rejected
=	Allowed

-	Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

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

CLAIM		DATE									
Final	Original	10/28/2008	05/28/2009	09/08/2009	03/15/2010	08/21/2010	01/17/2011	04/28/2011	12/28/2011	08/12/2012	
	1	✓	✓	✓	✓	✓	✓	✓	=	=	
	2	✓	✓	✓	✓	✓	✓	✓	=	=	
	3	✓	✓	✓	✓	✓	✓	✓	=	=	
	4	✓	✓	✓	✓	✓	✓	✓	=	=	
	5	✓	✓	✓	✓	✓	✓	✓	=	=	
	6	✓	✓	✓	✓	✓	✓	✓	=	=	
	7	✓	✓	✓	✓	✓	✓	✓	=	=	
	8	✓	✓	✓	✓	✓	✓	✓	=	=	
	9	✓	✓	✓	✓	✓	✓	✓	=	=	
	10	✓	✓	✓	✓	✓	✓	✓	=	=	
	11	✓	✓	✓	✓	✓	✓	✓	=	=	
	12	✓	✓	✓	✓	✓	✓	✓	=	=	
	13	✓	✓	✓	✓	✓	✓	✓	=	=	
	14	✓	✓	✓	✓	✓	✓	✓	=	=	
	15	✓	✓	✓	✓	✓	✓	✓	=	=	
	16	✓	✓	✓	✓	✓	✓	✓	=	=	
	17	✓	✓	✓	✓	✓	✓	✓	=	=	
	18	✓	✓	✓	✓	✓	✓	✓	=	=	
	19	✓	✓	✓	✓	✓	✓	✓	=	=	
	20	✓	✓	✓	✓	✓	✓	✓	=	=	
	21	✓	✓	✓	✓	✓	✓	✓	=	=	
	22	✓	✓	✓	✓	✓	✓	✓	=	=	
	23	✓	✓	✓	✓	✓	✓	✓	=	=	
	24	✓	✓	✓	✓	✓	✓	✓	=	=	
	25	✓	✓	✓	✓	✓	✓	✓	=	=	
	26	✓	✓	✓	✓	✓	✓	✓	=	=	
	27	✓	✓	✓	✓	✓	✓	✓	=	=	
	28							✓	=	=	
	29							✓	=	=	

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

Request for Continued Examination (RCE) Transmittal

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

Application Number	10500930
Filing Date	19 October 2005
First Named Inventor	Sami Vaarala
Art Unit	2469
Examiner Name	Afshawn M. Towfighi
Attorney Docket Number	290.1078USN

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.

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

1. **Submission required under 37 CFR 1.114** Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).
- a. Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.
- i. Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
- ii. Other _____
- b. Enclosed
- i. Amendment/Reply
- ii. Affidavit(s)/ Declaration(s)
- iii. Information Disclosure Statement (IDS)
- iv. Other Copy of non-patent literature cited
2. **Miscellaneous**
- a. Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of _____ months. (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)
- b. Other _____
3. **Fees** The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.
- The Director is hereby authorized to charge the following fees, or credit any overpayments, to
- a. Deposit Account No. 06-0243. I have enclosed a duplicate copy of this sheet.
- i. RCE fee required under 37 CFR 1.17(e)
- ii. Extension of time fee (37 CFR 1.136 and 1.17)
- iii. Other Supplemental IDS fee
- b. Check in the amount of \$ _____ enclosed
- c. Payment by credit card (Form PTO-2038 enclosed)

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

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Signature	/rfasth/	Date	17 January 2012
Name (Print/Type)	ROLF FASTH	Registration No.	36,999

CERTIFICATE OF MAILING OR TRANSMISSION

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

Signature	Electronic Submission	Date	17 January 2012
Name (Print/Type)	Rolf Fasth /rfasth/	Date	17 January 2012

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop RCE, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

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.

Instruction Sheet for RCEs

(not to be submitted to the USPTO)

NOTES:

An RCE is not a new application, and filing an RCE will not result in an application being accorded a new filing date.

Filing Qualifications:

The application must be a utility or plant application filed on or after June 8, 1995. The application cannot be a provisional application, a utility or plant application filed before June 8, 1995, a design application, or a patent under reexamination. See 37 CFR 1.114(e).

Filing Requirements:

Prosecution in the application must be closed. Prosecution is closed if the application is under appeal, or the last Office action is a final action, a notice of allowance, or an action that otherwise closes prosecution in the application (e.g., an Office action under *Ex parte Quayle*). See 37 CFR 1.114(b).

A submission and a fee are required at the time the RCE is filed. If reply to an Office action under 35 U.S.C. 132 is outstanding (e.g., the application is under final rejection), the submission must meet the reply requirements of 37 CFR 1.111. If there is no outstanding Office action, the submission can be an information disclosure statement, an amendment, new arguments, or new evidence. See 37 CFR 1.114(c). The submission may be a previously filed amendment (e.g., an amendment after final rejection).

WARNINGS:

Request for Suspension of Action:

All RCE filing requirements must be met before suspension of action is granted. A request for a suspension of action under 37 CFR 1.103(c) does not satisfy the submission requirement and does not permit the filing of the required submission to be suspended.

Improper RCE will NOT toll Any Time Period:

Before Appeal - If the RCE is improper (e.g., prosecution in the application is not closed or the submission or fee has not been filed) and the application is not under appeal, the time period set forth in the last Office action will continue to run and the application will be abandoned after the statutory time period has expired if a reply to the Office action is not timely filed. No additional time will be given to correct the improper RCE.

Under Appeal - If the RCE is improper (e.g., the submission or the fee has not been filed) and the application is under appeal, the improper RCE is effective to withdraw the appeal. Withdrawal of the appeal results in the allowance or abandonment of the application depending on the status of the claims. If there are no allowed claims, the application is abandoned. If there is at least one allowed claim, the application will be passed to issue on the allowed claim(s). See MPEP 1215.01.

See MPEP 706.07(h) for further information on the RCE practice.

PATENT

Attorney Matter No. 290.1078USN

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Date: 17 January 2012

Sami Vaarala, Antti Nuopponen

Serial No. 10/500,930

Filed: 19 October 2005

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

Examiner: Afshawn M. Towfighi

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT PURSUANT TO CFR §
1.17(c)

TO: COMMISSIONER FOR PATENTS

This Information Disclosure Statement and the enclosed references listed on Form PTO/SB/08 are being filed to comply with the Applicant's duty of disclosure. The related fee is submitted concurrently.

It is requested that the Examiner review the enclosed information and cite this information as having been considered in connection with this present application.

Respectfully submitted,

FASTH LAW OFFICES

/rfasth/

Rolf Fasth

Registration No. 36,999

FASTH LAW OFFICES
26 Pinecrest Plaza, Suite 2
Southern Pines, NC 28387-4301
Telephone: 910-687-0001
Facsimile: 910-295-2152

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
Attorney Ref. No. 290.1078USN

In re application of
 Sami Vaarala, Antti Nuopponen

Art Unit 2469
 Confirmation No. 1571

Serial No. 10/500,930

CERTIFICATE OF MAILING

Filed: 19 October 2005

I HEREBY CERTIFY THAT THIS PAPER AND THE DOCUMENTS
 REFERRED TO AS BEING ATTACHED OR ENCLOSED HERewith
 ARE BEING SUBMITTED ELECTRONICALLY TO THE UNITED
 STATES PATENT AND TRADEMARK OFFICE ON 18 January
 2012.

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

/rfasth/

Examiner: Afshawn M. Towfighi

 Rolf Fasth
 Attorney for Applicant

Date: 18 January 2012

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) Supplemental IDS and fee.
- (X) RCE and fee
- (X) Copies of non-patent literature cited
- (X) The Commissioner is hereby authorized to charge any 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
 26 Pinecrest Plaza, Suite 2
 Southern Pines, North Carolina 28387-4301

Telephone: 910-687-0001
 Facsimile: 910-295-2152
Attorney Ref. No. 290.1078USN

Electronic Patent Application Fee Transmittal

Application Number:	10500930
Filing Date:	19-Oct-2005
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:	290.1078USN

Filed as Small Entity

U.S. National Stage under 35 USC 371 Filing Fees

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

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Request for continued examination	2801	1	465	465
Submission- Information Disclosure Stmt	1806	1	180	180
Total in USD (\$)				645

Electronic Acknowledgement Receipt

EFS ID:	11858269
Application Number:	10500930
International Application Number:	
Confirmation Number:	1571
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:	290.1078USN
Receipt Date:	18-JAN-2012
Filing Date:	19-OCT-2005
Time Stamp:	09:10:10
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$645
RAM confirmation Number	9725
Deposit Account	060243
Authorized User	

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

Charge any Additional Fees required under 37 C.F.R. 1.492 (National application filing, search, and examination fees)

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

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

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

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS.PDF	66625	no	4
			31f490db890793769e7fe41fcee1b65ec715148		

Warnings:

Information:

This is not an USPTO supplied IDS fillable form

2	Non Patent Literature	NPL.PDF	22389	no	6
			28e1ba21864776cfff0cb28d8d253090c629584e		

Warnings:

Information:

3	Non Patent Literature	NPL_B.PDF	28801	no	10
			efada3ca14a2172f580d1075b228cb7c660e314a		

Warnings:

Information:

4	Request for Continued Examination (RCE)	RCE.PDF	145141	no	2
			82c4fb0ac246cd7b6a5a2b33c2fa351bb1508c1		

Warnings:

This is not a USPTO supplied RCE SB30 form.

Information:

5	Transmittal Letter	SUPP_IDS_LTR.PDF	55097	no	1
			20708cfc04532ea0c8a0fb83e573c22e730b6773		

Warnings:

Information:

6	Transmittal Letter	TRX.pdf	58279	no	1
			002737baf3fbb972cf730c284b62648d3d04919f		

Warnings:

Information:

7	Fee Worksheet (SB06)	fee-info.pdf	31855	no	2
			6ffee20096366edf84e4561c4d9d41317dcd a55f		

Warnings:

Information:

Total Files Size (in bytes):			408187		
-------------------------------------	--	--	--------	--	--

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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		10500930
	Filing Date		2005-10-19
	First Named Inventor	Sami Vaarala	
	Art Unit	2469	
	Examiner Name	Afshawn M. Towfigh	
	Attorney Docket Number	290.1078USN	

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6732269		2004-05-04	Baskey, Michael Edward et al.	
	2	6718388		2004-04-06	Yarborough, William Jordan et al.	
	3	6957346		2005-10-18	Kivinen, Tero et al.	
	4	6795917		2004-09-21	Ylonen, Tatu	

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

U.S.PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

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

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

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

Application Number	10500930
Filing Date	2005-10-19
First Named Inventor	Sami Vaarala
Art Unit	2469
Examiner Name	Afshawn M. Towfighi
Attorney Docket Number	290.1078USN

1									<input type="checkbox"/>
---	--	--	--	--	--	--	--	--	--------------------------

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

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	ARI LUOTONEN, "Tunneling SSL Through a WWW Proxy" Internet draft memo, March 26, 1997.	<input type="checkbox"/>
	2	ARI LUOTONEN, "Tunneling TCP based protocols through Web proxy servers" Internet draft memo, August 1998.	<input type="checkbox"/>
	3		<input type="checkbox"/>

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

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

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

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

Application Number	10500930		
Filing Date	2005-10-19		
First Named Inventor	Sami Vaarala		
Art Unit	2469		
Examiner Name	Afshawn M. Towfighi		
Attorney Docket Number	290.1078USN		

CERTIFICATION STATEMENT

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

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

OR

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

- See attached certification statement.
- The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.
- A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/rfasth/	Date (YYYY-MM-DD)	2012-01-17
Name/Print	Rolf Fasth	Registration Number	36999

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

Privacy Act Statement

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

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

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



NOTICE OF ALLOWANCE AND FEE(S) DUE

33369 7590 01/12/2012
FASTH LAW OFFICES (ROLF FASTH)
26 PINECREST PLAZA, SUITE 2
SOUTHERN PINES, NC 28387-4301

EXAMINER
TOWFIGHI, AFSHAWN M
ART UNIT
PAPER NUMBER

2469
DATE MAILED: 01/12/2012

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.

10/500,930 10/19/2005 Sami Vaarala 290.1078USN 1571
TITLE OF INVENTION: METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION

Table with 7 columns: APPLN. TYPE, SMALL ENTITY, ISSUE FEE DUE, PUBLICATION FEE DUE, PREV. PAID ISSUE FEE, TOTAL FEE(S) DUE, DATE DUE

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 SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

- A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.
B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

- A. Pay TOTAL FEE(S) DUE shown above, or
B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

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)

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.

33369 7590 01/12/2012
FASTH LAW OFFICES (ROLF FASTH)
 26 PINECREST PLAZA, SUITE 2
 SOUTHERN PINES, NC 28387-4301

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.
10/500,930	10/19/2005	Sami Vaarala	290.1078USN	1571

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

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	\$870	\$300	\$0	\$1170	04/12/2012

EXAMINER	ART UNIT	CLASS-SUBCLASS
TOWFIGHI, AFSHAWN M	2469	709-229000

<p>1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).</p> <p><input type="checkbox"/> Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.</p> <p><input type="checkbox"/> "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.</p>	<p>2. For printing on the patent front page, list</p> <p>(1) the names of up to 3 registered patent attorneys or agents OR, alternatively, 1 _____</p> <p>(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. 2 _____</p> <p>3 _____</p>
---	---

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

<p>4a. The following fee(s) are submitted:</p> <p><input type="checkbox"/> Issue Fee</p> <p><input type="checkbox"/> Publication Fee (No small entity discount permitted)</p> <p><input type="checkbox"/> Advance Order - # of Copies _____</p>	<p>4b. Payment of Fee(s); (Please first reapply any previously paid issue fee shown above)</p> <p><input type="checkbox"/> A check is enclosed.</p> <p><input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached.</p> <p><input type="checkbox"/> The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).</p>
---	--

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

a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27. b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information 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.



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

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
Values: 10/500,930, 10/19/2005, Sami Vaarala, 290.1078USN, 1571

33369 7590 01/12/2012
FASTH LAW OFFICES (ROLF FASTH)
26 PINECREST PLAZA, SUITE 2
SOUTHERN PINES, NC 28387-4301

EXAMINER

TOWFIGHI, AFSHAWN M

ART UNIT PAPER NUMBER

2469

DATE MAILED: 01/12/2012

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)

(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 643 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 643 day(s).

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 Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

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.

<i>Examiner-Initiated Interview Summary</i>	Application No. 10/500,930	Applicant(s) VAARALA ET AL.	
	Examiner AFSHAWN TOWFIGHI	Art Unit 2469	

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

(1) AFSHAWN TOWFIGHI. (3)_____.

(2) Rolf Fasth. (4)_____.

Date of Interview: 03 January 2011.

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...)

Applicant's representative gave permission for the examiner to place the "action" terms at the beginning of each limitation in claim 1.

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

/A. T./
Examiner, Art Unit 2469

Notice of Allowability

Application No.

10/500,930

Examiner

AFSHAWN TOWFIGHI

Applicant(s)

VAARALA ET AL.

Art Unit

2469

-- 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 11/7/11.
- 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 1-29.
- 4. Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some* c) None of 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. A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
- 6. CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) hereto or 2) to Paper No./Mail Date _____.
 - (b) 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).
- 7. 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. Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3. Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
- 4. Examiner's Comment Regarding Requirement for Deposit of Biological Material
- 5. Notice of Informal Patent Application
- 6. Interview Summary (PTO-413), Paper No./Mail Date 1/3/11.
- 7. Examiner's Amendment/Comment
- 8. Examiner's Statement of Reasons for Allowance
- 9. Other _____.

/A. T./
Examiner, Art Unit 2469

/IAN N. MOORE/
Supervisory Patent Examiner, Art Unit 2469

EXAMINER'S AMENDMENT

1. 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 a telephone interview with Rolf Fasth on 1/3/11.

The application has been amended as follows:

Lines 5-6 of claim 1 should be replaced with "negotiating and exchanging keys with one another, by the first and second computer, according to a key exchange".

Line 14 of claim 1 should be replaced with "forming a secure message, in the first computer, by giving the".

Line 26 of claim 1 should be replaced with "substituting, at the intermediate computer, the first unique".

Line 29 of claim 1 should be replaced with "forwarding, at the intermediate computer, the secure message with".

Response to Arguments

2. Applicant's arguments, see pages 9-20, filed 11/7/2011, with respect to claims 1-29 have been fully considered and are persuasive. The rejection of claims 1-29 has been withdrawn.

Allowable Subject Matter

3. Claims 1-29 (amended) are allowed.
4. The following is an examiner's statement of reasons for allowance:

Amended claims 1-29 are allowable over prior art since the prior art reference(s) taken individually or in combination fails to particularly disclose, fairly suggests, or render obvious as argued by the applicant which examiner considers as persuasive as set forth above.

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.

Art Unit: 2469

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.

/A. T./
Examiner, Art Unit 2469

/IAN N. MOORE/
Supervisory Patent Examiner, Art Unit 2469

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L2	5125	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L3	13	L2 and secure near10 key near10 exchang\$3	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L4	501	ipsec same tunnel\$3 same IKE	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L5	152	ipsec same tunnel\$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L6	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2011/12/28 20:07
L7	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
L8	20	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L9	2794	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L10	2398	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L11	2398	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L12	1829	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L13	1829	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L14	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L15	5125	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L16	13	L15 and secure near10 key near10 exchang\$3	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07

L17	501	ipsec same tunnel\$3 same IKE	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L18	152	ipsec same tunnel\$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L19	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2011/12/28 20:07
L20	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
L21	20	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L22	2794	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L23	2398	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L24	2398	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L25	1829	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L26	1829	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L27	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L28	5125	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L29	13	L28 and secure near10 key near10 exchang\$3	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L30	501	ipsec same tunnel\$3 same IKE	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L31	152	ipsec same tunnel\$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L32	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2011/12/28 20:07

L33	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
L34	20	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L35	2794	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L36	2398	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L37	2398	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L38	1829	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L39	1829	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L40	2	"20010047487"	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L41	5125	709/236.ccls. or 709/245.ccls.	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L42	13	L41 and secure near10 key near10 exchang\$3	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L43	501	ipsec same tunnel\$3 same IKE	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L44	152	ipsec same tunnel\$3 same IKE same (gateway or proxy or intermediate)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L45	2	"US 20060173968"	US-PGPUB; USPAT; USOCR; DERWENT	OR	OFF	2011/12/28 20:07
L46	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
L47	20	ike with responder with cookie	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L48	2794	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L49	2398	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L50	2398	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07


L51	1829	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L52	1829	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L53	1	"7882538"	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L54	18	"6744741"	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L55	13	"7055027"	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:07
L56	9	((SAMI) near2 (VAARALA)).INV.	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:09
L57	9	((ANTTI) near2 (NUOPPONEN)).INV.	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:10
L58	9	l56 or l57	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:11
L59	8	l58 and (secure adj connection).clm.	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:11
L60	7	l58 and (secure adj connection with address).clm.	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:11
L61	1	l58 and (secure adj connection with intermediate with address).clm.	US-PGPUB; USPAT	OR	OFF	2011/12/28 20:12

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L62	1	(secure adj connection with intermediate with address).clm.	USPAT; UPAD	OR	OFF	2011/12/28 20:12
L63	13	(secure adj connection with (intermediate or gateway or proxy) with address).clm.	USPAT; UPAD	OR	OFF	2011/12/28 20:12
L64	1	(secure adj connection with (intermediate or gateway or proxy) with (key or token) with address).clm.	USPAT; UPAD	OR	OFF	2011/12/28 20:13

12/ 28/ 2011 8:26:53 PM

H:\ EAST Workspaces\ jeff930.wsp


Search Notes 	Application/Control No. 10500930	Applicant(s)/Patent Under Reexamination VAARALA ET AL.
	Examiner Afshawn Towfighi	Art Unit 2469

SEARCHED			
Class	Subclass	Date	Examiner
709	236, 229, 245	11-5-2008	JS
ABOVE	UPDATED	12/28/2011	AT

SEARCH NOTES		
Search Notes	Date	Examiner
Limited classification of 709/229, 245	11-5-2008	JS
Inventor search	11-5-2008 (Updated 12/28/11)	JS
Text search of EAST (US Pat, US PG Pub, JPO, EPO, Derwent)	11-5-2008	JS
Updated Text search of EAST (see attached history)	5-28-2009	JS
Updated text search of EAST (see attached history)	9-8-09	JS
EAST search with previous examiner's classes and focus on new limitations	3/15/2010	AT
Conf with B.Bruckart and J.Avellino - Reopen and search IPsec/tunneling/gateway/proxy	8/21/2010	AT
Updated EAST search - see attached	8/21/2010	AT
EAST (USPAT, USPGPUB) - see search history printout (Updated 4/28/11)	1/17/2011 (Updated 4/28/11) (Updated 12/28/11)	AT

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner
	Interference Search - see search history printout	12/28/2011	AT

--	--

Index of Claims 	Application/Control No. 10500930	Applicant(s)/Patent Under Reexamination VAARALA ET AL.
	Examiner AFSHAWN TOWFIGHI	Art Unit 2469

✓	Rejected
=	Allowed

-	Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

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


CLAIM		DATE									
Final	Original	10/28/2008	05/28/2009	09/08/2009	03/15/2010	08/21/2010	01/17/2011	04/28/2011	12/28/2011		
	1	✓	✓	✓	✓	✓	✓	✓	=		
	2	✓	✓	✓	✓	✓	✓	✓	=		
	3	✓	✓	✓	✓	✓	✓	✓	=		
	4	✓	✓	✓	✓	✓	✓	✓	=		
	5	✓	✓	✓	✓	✓	✓	✓	=		
	6	✓	✓	✓	✓	✓	✓	✓	=		
	7	✓	✓	✓	✓	✓	✓	✓	=		
	8	✓	✓	✓	✓	✓	✓	✓	=		
	9	✓	✓	✓	✓	✓	✓	✓	=		
	10	✓	✓	✓	✓	✓	✓	✓	=		
	11	✓	✓	✓	✓	✓	✓	✓	=		
	12	✓	✓	✓	✓	✓	✓	✓	=		
	13	✓	✓	✓	✓	✓	✓	✓	=		
	14	✓	✓	✓	✓	✓	✓	✓	=		
	15	✓	✓	✓	✓	✓	✓	✓	=		
	16	✓	✓	✓	✓	✓	✓	✓	=		
	17	✓	✓	✓	✓	✓	✓	✓	=		
	18	✓	✓	✓	✓	✓	✓	✓	=		
	19	✓	✓	✓	✓	✓	✓	✓	=		
	20	✓	✓	✓	✓	✓	✓	✓	=		
	21	✓	✓	✓	✓	✓	✓	✓	=		
	22	✓	✓	✓	✓	✓	✓	✓	=		
	23	✓	✓	✓	✓	✓	✓	✓	=		
	24	✓	✓	✓	✓	✓	✓	✓	=		
	25	✓	✓	✓	✓	✓	✓	✓	=		
	26	✓	✓	✓	✓	✓	✓	✓	=		
	27	✓	✓	✓	✓	✓	✓	✓	=		
	28							✓	=		
	29							✓	=		


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. 1571

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.		
10/500,930	10/19/2005	709	2469	290.1078USN		
APPLICANTS Sami Vaarala, Espoo, FINLAND; Antti Nuopponen, Espoo, FINLAND; ** CONTINUING DATA ***** This application is a 371 of PCT/FI03/00045 01/21/2003 ** FOREIGN APPLICATIONS ***** FINLAND 20020112 01/22/2002 ** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** ** SMALL ENTITY **						
Foreign Priority claimed <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	35 USC 119(a-d) conditions met <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
Verified and /AFSHAWN M TOWFIGHI/	Examiner's Signature	Initials	FINLAND	6	26	2
ADDRESS FASTH LAW OFFICES (ROLF FASTH) 26 PINECREST PLAZA, SUITE 2 SOUTHERN PINES, NC 28387-4301 UNITED STATES						
TITLE Method and system for sending a message through a secure connection						
FILING FEE RECEIVED 657	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:			<input type="checkbox"/> All Fees		
				<input type="checkbox"/> 1.16 Fees (Filing)		
				<input type="checkbox"/> 1.17 Fees (Processing Ext. of time)		
				<input type="checkbox"/> 1.18 Fees (Issue)		
				<input type="checkbox"/> Other _____		
				<input type="checkbox"/> Credit		

Issue Classification 	Application/Control No. 10500930	Applicant(s)/Patent Under Reexamination VAARALA ET AL.
	Examiner AFSHAWN TOWFIGHI	Art Unit 2469

ORIGINAL						INTERNATIONAL CLASSIFICATION														
CLASS			SUBCLASS			CLAIMED					NON-CLAIMED									
709			229			G	0	6	F	15 / 16 (2006.01.01)										
CROSS REFERENCE(S)																				
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)																			
726	3																			

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

/AFSHAWN TOWFIGHI/ Examiner.Art Unit 2469 (Assistant Examiner)	12/28/11 (Date)	Total Claims Allowed: 29	
	/IAN N MOORE/ Supervisory Patent Examiner.Art Unit 2469 (Primary Examiner)	01/06/2012 (Date)	O.G. Print Claim(s) O.G. Print Figure 1 1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Art Unit 2458

5 Sami Vaarala and Antti Nuopponen

Serial No. 10/500,930

10 Filed: 19 October 2005

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

15 Examiner: Afshawn M. Towfighi

Date: 7 November 2011

20 Attorney Docket No. 290.1078USN

AMENDMENT

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

30 This is in response to the Office action of 10 May
2011. Please amend the above-identified patent application as
follows:

In the Claims:

Amend the claims as follows:

5

1. (Currently amended) A method for secure forwarding of a message from a first computer to a second computer using a secure connection via an intermediate computer in a telecommunication network, comprising:

10

the first computer and the second computer negotiating and exchanging keys with one another according to a key exchange protocol to establish [[a]] the secure connection between the first computer and the second computer via the intermediate computer,

15

the secure connection having a source address of the first computer as a first end point and a destination address of the second computer as a second end point of the secure connection,

20

in the first computer, forming a secure message by giving the secure message a first unique identity and a first destination address to the intermediate computer,

25

sending the secure message, using the secure connection, containing the first unique identity and the first destination address from the first computer to the intermediate computer, the intermediate computer receiving the secure message and performing a translation by using the first unique identity to find a second destination address to the second computer, the intermediate computer substituting the first destination address with the second destination address to the second computer,

30

the intermediate computer substituting the first unique identity with a second unique identity of the secure connection, and

35

the intermediate computer forwarding the secure message with the second destination address and the second unique identity

to the second computer in the secure connection.

2. (Previously presented) The method of claim 1 wherein the method further comprises forming the secure message by using
5 an IPsec connection between the first computer and the second computer.

3. (Previously presented) The method of claim 1 wherein the method further comprises performing a secure forwarding of the
10 message by making use of SSL or TLS protocols.

4. (Previously presented) The method of claim 2 wherein the method further comprises manually performing a preceding
15 distribution of keys to components for forming the IPsec connection.

5. (Previously presented) The method of claim 2 wherein the method further comprises performing a preceding distribution
20 of keys for forming the IPsec connection by an automated key exchange protocol.

6. (Previously presented) The method of claim 5 wherein the method further comprises performing the automated key exchange
25 protocol used for the preceding distribution of keys for forming the IP Sec connection by means of a modified IKE key exchange protocol between the first computer and the intermediate computer and by means of a standard IKE key exchange protocol between the intermediate computer and the second computer.

30
7. (Previously presented) The method of claim 2 wherein the method further comprises sending the message that is sent from the first computer as a packet that contains message data, an inner IP header containing the actual sender and receiver
35 addresses, an outer IP header containing the addresses of the

first computer and the intermediate computer, the unique identity.

5 8. (Previously presented) The method of claim 1 wherein the method further comprises the IPsec connection being one or more security associations (SA) and the unique identity being one or more SPI values.

10 9. (Previously presented) The method of claim 1 wherein the method further comprises performing the matching by using a translation table stored at the intermediate computer.

15 10. (Previously presented) The method of claim 1 wherein the method further comprises changing both the address and the SPI-value by the intermediate computer.

20 11. (Previously presented) The method of claim 1 wherein the method further comprises the first computer being a mobile terminal so that the mobility is enabled by modifying the translation table at the intermediate computer.

25 12. (Previously presented) The method of claim 11 wherein the method further comprises performing the modification of the translation tables by sending a request for registration of the new address from the first computer to the intermediate computer.

30 13. (Previously presented) The method of claim 12 wherein the method further comprises sending a reply to the request for registration from the intermediate computer to the first computer.

35 14. (Previously presented) The method of claim 12 wherein the method further comprises authenticating or encrypting by IPsec the request for registration and/or reply.

15. (Previously presented) The method of claim 4 wherein the method further comprises establishing the key distribution for the secure connections by establishing an IKE protocol translation table, and using the translation table to modify
5 IP addresses and cookie values of IKE packets in the intermediate computer.

16. (Previously presented) The method of claim 15 wherein the
10 method further comprises establishing the key exchange distribution by:
generating an initiator cookie and sending a zero responder cookie to the second computer,
generating a responder cookie in the second computer,
15 establishing a mapping between IP addresses and IKE cookie values in the intermediate computer, and
using the translation table to modify IKE packets in flight by modifying the external IP addresses and possibly IKE cookies of the IKE packets.

20
17. (Previously presented) The method of claim 15 wherein the method further comprises modifying a modified IKE protocol between the first computer and the intermediate computer by transmitting the IKE keys from the first computer to the
25 intermediate computer in order to decrypt and modify IKE packets.

18. (Previously presented) The method of claim 15 wherein the method further comprises carrying out in a modified IKE
30 protocol between the first computer and the intermediate computer the modification of the IKE packets by the first computer with the intermediate computer requesting such modifications.

35 19. (Previously presented) The method of claim 17 wherein the

method further comprises defining the address so that the first computer is identified for the second computer by the intermediate computer by means of an IP address taken from a pool of user IP addresses when forming the translation table.

5

20. (Previously presented) The method of claim 1 wherein the method further comprises sending the secure message by using an IPSec transport mode.

10 21. (Previously presented) The method of claim 1 wherein the method further comprises sending the secure message by using an IPSec tunnel mode.

15 22. (Previously presented) A telecommunication network for secure forwarding of messages, comprising:
a first computer, a second computer and an intermediate computer,
means for directly negotiating and exchanging keys, according to a key exchange protocol, between the first computer and the
20 second computer to establish a security association having a source address of the first computer as a first end point and an IP destination address of the second computer as a second end point,
the first and the second computers having means for performing
25 an IPSec processing,
the intermediate computer having translation means for using translation tables to perform IPsec and IKE translation and for changing a destination address of the intermediate computer of a secure message, containing a unique identity, to
30 a destination address of the second computer without decrypting the secure message, and
the intermediate computer having means for using the unique identity when forwarding the secure message received from the first computer to the second computer in the security
35 association.

23. (Previously presented) The telecommunication network of claim 22 wherein the translation table for IPsec translation has IP addresses of the intermediate computer to be matched with IP addresses of the second computer.

24. (Previously presented) The telecommunication network of claim 22 wherein the translation tables for IKE translation consists of two partitions, one for the communication between the first computer and the intermediate computer and another for the communication between the intermediate computer and the second computer.

25. (Previously presented) The telecommunication network of claim 24 wherein both partitions of the mapping table for IKE translation contains translation fields for a source IP address, a destination IP address, initiator and responder cookies between respective computers.

26. (Previously presented) The telecommunication network of claim 22 wherein there is another translation table for IKE translation containing fields for matching a given user to a given computer.

27. (Previously presented) A telecommunication network for secure forwarding of messages, comprising:
a first computer,
a second computer,
an intermediate computer electronically connected to the first computer and the second computer,
a negotiating and key exchanging module between the first computer and the second computer to establish a secure connection having a source address of the first computer as a first end point and a destination address of the second computer as a second end point, and

the intermediate computer performing translation between destination addresses and secure identities for forwarding a secure message, containing a unique identity, received from the first computer and using the unique identity when
5 forwarding the secure message to the second computer in the secure connection without decrypting the secure message and being aware of the keys to encrypt and/or authenticate the secure message and without establishing a new secure connection.

10

28. (Original) The method of claim 1 wherein the method further comprises the intermediate computer substituting the first unique identity with the second unique identity of the secure connection without establishing a new secure connection
15 and without involving the second computer.

29. (Original) The method of claim 1 wherein the packets between the first computer and intermediate computers are sent using a UDP protocol.

20

REMARKS/ARGUMENTS

5 Reconsideration of the application is respectfully
requested. Claims 1-2, 4-29 were rejected under Section 103
as being obvious over Kunzinger in view of Gunter. This
rejection is respectfully traversed.

 Claim 1 has now been amended to clarify that the
10 secure forwarding if the message is from the first computer to
the second computer using a secure connection and that the
secure message is sent by using the same secure connection.
No new matter has been added. Support may, for example, be
found in paragraphs 0073-0083 of the corresponding US
15 2006/0173968.

 Kunzinger merely teaches the use of two tunnels. He
explains that the security gateway 420 (intermediary computer)
serves as a point of entry into the intranet (paragraph 0050)
and that the security gateway retains the ability to provide
20 of the type of services available in the environment of Fig.
3. These services include access control and network address
translation that require content inspection. In other words,
the gateway protects the intranet from undesirable
communication from the open Internet by inspecting the content
25 of incoming packets before the packets enter into the
intranet. This requires the gateway (intermediate computer)
to decrypt the incoming packet in order to be able to inspect

the content of the incoming packet. In other words, Kunzinger expressly teaches away from any modification that would not allow the intermediate computer to decrypt the incoming packet to inspect the content (which would happen if Kunzinger is
5 modified to include Gunter's extended tunnel, as proposed by the Examiner).

Fig. 4 of Kunzinger clearly shows that a first tunnel extends between the first computer (client) and the intermediate computer (boundary device or gateway) and a
10 second tunnel extends between the intermediate computer and a second computer (server). The first tunnel provides security through the Internet and the second tunnel provides security through an intranet (see paragraph [0051] of Kunzinger). Kunzinger explains in paragraph [0047] that the "use of
15 cascaded tunnels (as opposed to one tunnel or SA extending from the client to the server) allows security protection to be tailored to the requirements of a particular network segment."

Applicant fails to see why the skilled person would
20 look to Gunter to modify Kunzinger to include a single tunnel extending from the client to the server when Kunzinger expressly teaches that such a modification should not be made because this would mean that the gateway would not be able to inspect the content of the incoming packets to protect the
25 intranet from the outside public Internet.

In the current invention, the intermediate computer

does not need to know the cryptographic keys or read the content but is able to use the outer IP addresses and the incoming SPI value (= unique identity) to determine how to modify the outer address and the SPI to suite the second
5 computer, which is the next destination.

In paragraph [0013], Kunzinger explains that the security associations are negotiated between the tunnel endpoints i.e. a first negotiation is between the endpoints of tunnel 1 and a second negotiation is between the endpoints of
10 tunnel 2. This means the client 405 negotiates with the gateway 420 to establish tunnel 1 (but not with the server 440). Similarly, the gateway 420 negotiates with the server 440 to establish tunnel 2.

In summary, Kunzinger clearly teaches the use of
15 cascade tunnels which provide the tailoring features (see paragraph [0047]) "as opposed to a tunnel or SA extending from the client to the server." In other words, he expressly teaches away from using a single tunnel from the client to the server. Also, in paragraphs [0012-0014] Kunzinger explains
20 that each tunnel is a separate connection. In paragraphs 0067-0068 Kunzinger explains if there is no existing cascaded tunnel available between the gateway 420 and the server 440 then a pair of IKE and IPSsec security associations are established to provide the next tunnel (which again indicates
25 that there are two separate tunnels and not one tunnel).

On page 5 of the Office action, the Examiner states

that Kunzinger teaches "the intermediate computer forwarding the secure message with the second destination address and the second unique identity to the second computer in the secure connection." (emphasis added). Applicant strongly disagrees.

5 Kunzinger forwards the message in the second tunnel which is different from the first tunnel discussed on page 4 of the Office action. The current claim 1 requires that the message is sent in the same secure connection that extends from the first computer to the second computer.

10 On page 6, the Examiner states that it would have been obvious to combine the teachings of Kunzinger and Gunter to have endpoints directly negotiate a key to establish a secure connection. Applicant respectfully and strongly disagrees.

15 Kunzinger expressly states that the intermediate computer must be able to decrypt the message to protect the intranet (see paragraph 0050). If the secure connection is established by the endpoints of the tunnel, as suggested by Gunter, then the intermediate computer could not intervene and
20 decrypt the message, as expressly required by Kunzinger. The Examiner is respectfully requested to better explain why the skilled person would modify Kunzinger to have one extended tunnel when Kunzinger expressly teaches away from this modification even if such an extended tunnel may be shown in
25 Gunter.

Additionally, it is submitted that the secure tunnel

(Tunnel 1) in Fig. 3 could not extend between the client and the server because in Kunzinger, the gateways must have clear text access to datagrams as explained in paragraph [0027], lines 13-15. As indicated above, if the tunnel would be
5 between the client and the server, then the gateway could not have clear text access to the datagrams. In paragraph [0017], Kunzinger explains that there are several disadvantages in providing an end-to-end security association between the two end-points (i.e. between the client and server, see paragraph
10 0017) because any "intermediate system in the network path are prevented from accessing the clear-text data content of the transmitted packets, because only the two endpoints are able to encrypt and decrypt the packets on this SA." In other words, Kunzinger expressly teaches away from a security
15 association that extends between the client (first computer) and the server (the second computer) when the flag is set which is the only time the gateway would be using the id to identify the second computer. A secure connection that extends between the first computer and the second computer is
20 exactly what is required by the amended claim 1 and that the intermediate computer uses the unique identity contained in the secure message to find the address to the second computer.

In order for the gateway (intermediate computer) of Kuntzinger to forward a packet it has to decrypt it (see
25 paragraph 0068, lines 6-7. A key is needed for decryption which of course cannot be transmitted in the packet to be

decrypted. The key has been sent to the gateway in advance since a key is something used to encrypt and decrypt with (lock and unlock). A key is never sent in the same message as the encrypted message. It would be the same thing as leaving
5 the key in a door when leaving your house.

There is a difference between encryption and hashing. Encryption transforms data from a cleartext to ciphertext and back (given the right keys), and the two texts should roughly correspond to each other in size: big cleartext
10 yields big ciphertext, and so on. "Encryption" is a two-way operation. Hashes, on the other hand, compile a stream of data into a small digest (a summarized form: think "Reader's Digest"), and it is strictly a one way operation. A hash value is thus a unique and extremely compact numerical
15 representation of a piece of data. Hashing is a one way function and a hash cannot be read by a receiver.

The Examiner states that "the key is the value id". It is respectfully submitted that this does not make sense. A key is a tool that is used to decrypt (remove encryption)
20 from an encrypted message. If a key is sent together with an encrypted message, the encryption would be meaningless, since then anyone would have the key and be able to read the message. If again, the key would be sent as data in the encrypted message, the recipient could not take out the key
25 from the message (being without a key to open the message). Thus, the key in Kunzinger is not an id and is not sent with

the message.

Gunter does not cure these deficiencies. Gunter is merely concerned with an ordinary key exchange (which is done to form a secure connection), but when the connection has been
5 formed a device in an internal network send the keys to a firewall so that the fire wall could follow the connection. The forming of the connection takes place without the fire wall being present in the negotiation (see Fig. 4, reference numbers 200 and 202). The packets in the key exchange go
10 through the firewall in the same way as through other routers (which are between the negotiating parties). The fire wall sends the packets to the internal network without decryption.

This operation does not differ at all from ordinary router operation. The firewall of Gunter is able to decrypt the
15 packets and store them but otherwise, it is just like an ordinary router.

Applicants fail to see why a person of ordinary skill in the art would look to Kunzinger and Gunter to learn about the steps of the present invention when Kunzinger
20 expressly teaches away from this feature when the flag is set since Kunzinger's intermediate computer would be prevented from accessing the clear-text data content described in paragraph [0017]. When the flag is not set the gateway would not use any unique identity contained in the secure message to
25 find an address for the second computer.

It is also noted that the Examiner has not commented

on all the arguments presented in the previous response. The Examiner is respectfully requested to review and consider all the arguments presented.

Also, paragraphs [0067] and [0068] of Kunzinger explain that the gateway decrypts that incoming data packet by using the decryption key that corresponds to the particular secure association i.e. Tunnel 1 extending between the client and the gateway. Kunzinger then explains that whether the message is intended to be forwarded further in the secured form (to the endpoint) then a Tunnel 2 has to be used and if there is no Tunnel 2 then it has to be established by means of a key exchange (IKE) procedure. Kunzinger explains that the policy "will direct the gateway to either use an existing cascaded tunnel, or if one is not available, to establish a pair of IKE and IPsec security associations that will provide this next cascaded tunnel. Kunzinger is here referring to Tunnel 2. This again confirms that Kunzinger requires two separate tunnels (secure connections) and it is submitted that it would not have been possible for Kunzinger's gateway to have decrypted the packet had the tunnel extended all the way between Kunzinger's client and server.

It is submitted that Kunzinger would require extensive modifications that are not taught or suggested to arrive at the features of the present invention. It is even submitted that Kunzinger would be inoperable by modifying it with Gunter's extended tunnel because Kunzinger's gateway

could not inspect the content of incoming packets.

In view thereof, claim 1 is submitted to be allowable.

Claims 2, 4-21 are submitted to be allowable because
5 they depend upon the allowable base claim 1 and because each claim includes limitations that are not taught or suggested in the cited references.

Independent claim 22 is submitted to be allowable for reasons similar to the reasons put forth above. Claim 22
10 has been amended to now require that the secure message contains the unique identity and that the intermediate computer has a module performing the IPsec and IKE translation etc. without decrypting the secure message.

In contrast, the intermediate computer in Kunzinger
15 decrypts the incoming secured message, as explained above. An important function of Kunzinger's gateways is to function as a port of entry into an intranet and to inspect the content of incoming secure packets which requires decryption of the packets before forwarding them to the server (the second
20 computer) in the intranet. In other words, the decryption is an important function of Kunzinger's invention because the security gateway (intermediate computer) must be able to decrypt the packet so that it can provide the important services of access control, network address translation etc.
25 that require content inspection, as explained in for example, paragraph [0050] of Kunzinger. Throughout the Kunzinger

patent, the feature of content inspection is emphasized and it is submitted it would be contrary to the spirit of Kunzinger to modify his system to prevent the security gateway from being able to inspect the content of the incoming packets. It is submitted that Kunzinger expressly teaches away from extending the tunnel from the client to the server so that the gateway could not decrypt the incoming packet. The proposed modification is therefore not obvious even if another reference such as Gunter shows a tunnel that has an intermediary computer that cannot decrypt the incoming packet.

Claims 23-26 are submitted to be allowable because they depend upon the allowable base claim 22 and because each claim includes limitations that are not taught or suggested in the cited references.

Independent claim 27 is submitted to be allowable for the same reasons as those put forth for the patentability of claim 22. In addition, the amended claim 27 requires a module for performing the IPsec and IKE translation etc. without undoing the IPsec processing and being aware of the keys to encrypt and/or authenticate the secure message and without establishing a new IPsec connection and that the secure message contains the unique identity. It is submitted that Kunzinger expressly teaches away from extending the tunnel from the client to the server so that the gateway could not decrypt the incoming packet. The proposed modification of Kunzinger is therefore not obvious.

Claims 28-29 are submitted to be allowable because they depend upon the allowable base claim 1 and because the claims include limitations that are not taught or suggested in the cited references.

5 Claim 3 was rejected under Section 103 as being obvious over Kunzinger in view of Patel. This rejection is respectfully traversed.

10 Claim 3 is submitted to be allowable because it depends upon the allowable base claim 1 and because the claim includes limitations that are not taught or suggested in the cited references.

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

Respectfully submitted,

10 FASTH LAW OFFICES

15 /rfasth/
Rolf Fasth
Registration No. 36,999

20 **ATTORNEY DOCKET NO. 290.1078USN**

FASTH LAW OFFICES
26 Pinecrest Plaza, Suite 2
Southern Pines, NC 28387-4301

25 Telephone: (910) 687-0001
Facsimile: (910) 295-2152

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
Attorney Ref. No. 290.1078USN

In re application of

Sami Vaarala, Antti Nuopponen

Art Unit 2458
 Confirmation No. 1571

Serial No. 10/500,930

CERTIFICATE OF MAILING

Filed: 19 October 2005

I HEREBY CERTIFY THAT THIS PAPER AND THE DOCUMENTS
 REFERRED TO AS BEING ATTACHED OR ENCLOSED HERewith
 ARE BEING SUBMITTED ELECTRONICALLY TO THE UNITED
 STATES PATENT AND TRADEMARK OFFICE ON **7 November**
2011.

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

/rfasth/

Examiner: Afshawn M. Towfighi

 Rolf Fasth

Date: 7 November 2011

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) Response to Office Action dated 10 May 2011.
- (X) **Applicant hereby petitions to obtain a three month extension
 to respond to the outstanding Office Action.**
- (X) The Commissioner is hereby authorized to charge any 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
 26 Pinecrest Plaza, Suite 2
 Southern Pines, North Carolina 28387-4301

Telephone: 910-687-0001
 Facsimile: 910-295-2152
Attorney Ref. No. 290.1078USN

Electronic Patent Application Fee Transmittal

Application Number:	10500930
Filing Date:	19-Oct-2005
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:	290.1078USN

Filed as Small Entity

U.S. National Stage under 35 USC 371 Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 3 months with \$0 paid	2253	1	635	635

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				635

Electronic Acknowledgement Receipt

EFS ID:	11346935
Application Number:	10500930
International Application Number:	
Confirmation Number:	1571
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:	290.1078USN
Receipt Date:	07-NOV-2011
Filing Date:	19-OCT-2005
Time Stamp:	11:46:36
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$635
RAM confirmation Number	19786
Deposit Account	060243
Authorized User	

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

Charge any Additional Fees required under 37 C.F.R. 1.492 (National application filing, search, and examination fees)

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

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

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

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	AMD.PDF	91639 13497a2c2149d6a05a21b035d28f3eaf5a0f1a4f	no	20

Warnings:

Information:

2	Miscellaneous Incoming Letter	TRX.PDF	63352 b3e324a4fb0ffa615645b151271deccda3014745f	no	1
---	-------------------------------	---------	--	----	---

Warnings:

Information:

3	Fee Worksheet (SB06)	fee-info.pdf	30004 403312c96cf95d9832125079987820aeca029963	no	2
---	----------------------	--------------	---	----	---

Warnings:

Information:

Total Files Size (in bytes): 184995

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.

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 10/500,930	Filing Date 10/19/2005	<input type="checkbox"/> To be Mailed
---	---	----------------------------------	---------------------------------------

APPLICATION AS FILED – PART I			OTHER THAN SMALL ENTITY			
	(Column 1)	(Column 2)	SMALL ENTITY <input checked="" type="checkbox"/>	OR		
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	RATE (\$)	FEE (\$)
<input type="checkbox"/> BASIC FEE <small>(37 CFR 1.16(a), (b), or (c))</small>	N/A	N/A	N/A		N/A	
<input type="checkbox"/> SEARCH FEE <small>(37 CFR 1.16(k), (j), or (m))</small>	N/A	N/A	N/A		N/A	
<input type="checkbox"/> EXAMINATION FEE <small>(37 CFR 1.16(o), (p), or (q))</small>	N/A	N/A	N/A		N/A	
TOTAL CLAIMS <small>(37 CFR 1.16(j))</small>	minus 20 =	*	X \$ =	OR	X \$ =	
INDEPENDENT CLAIMS <small>(37 CFR 1.16(h))</small>	minus 3 =	*	X \$ =		X \$ =	
<input type="checkbox"/> APPLICATION SIZE FEE <small>(37 CFR 1.16(s))</small>	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).					
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT <small>(37 CFR 1.16(j))</small>						
			TOTAL		TOTAL	

* If the difference in column 1 is less than zero, enter "0" in column 2.

APPLICATION AS AMENDED – PART II					OTHER THAN SMALL ENTITY			
	(Column 1)	(Column 2)	(Column 3)					
AMENDMENT	11/07/2011	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)
	Total <small>(37 CFR 1.16(i))</small>	* 29	Minus ** 29	= 0	X \$30 =	0	OR	X \$ =
	Independent <small>(37 CFR 1.16(h))</small>	* 3	Minus *** 3	= 0	X \$125 =	0	OR	X \$ =
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>						OR	
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>						OR	
					TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE

	(Column 1)	(Column 2)	(Column 3)					
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)
	Total <small>(37 CFR 1.16(i))</small>	*	Minus **	=	X \$ =		OR	X \$ =
	Independent <small>(37 CFR 1.16(h))</small>	*	Minus ***	=	X \$ =		OR	X \$ =
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>						OR	
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>						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".

Legal Instrument Examiner:
 /PAUL STANBACK/

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

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

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



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.
10/500,930	10/19/2005	Sami Vaarala	290.1078USN	1571
33369	7590	05/10/2011	EXAMINER	
FASTH LAW OFFICES (ROLF FASTH) 26 PINECREST PLAZA, SUITE 2 SOUTHERN PINES, NC 28387-4301			TOWFIGHI, AFSHAWN M	
			ART UNIT	PAPER NUMBER
			2469	
			NOTIFICATION DATE	DELIVERY MODE
			05/10/2011	ELECTRONIC

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

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

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

sloan.smith@fasthlaw.com
nan_russell@fasthlaw.com

Office Action Summary	Application No. 10/500,930	Applicant(s) VAARALA ET AL.	
	Examiner AFSHAWN TOWFIGHI	Art Unit 2469	

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

Period for Reply

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

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

Status

- 1) Responsive to communication(s) filed on 4/8/11.
- 2a) This action is **FINAL**.
- 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-29 is/are pending in the application.
 - 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-29 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 - Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 - Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 - 1. Certified copies of the priority documents have been received.
 - 2. Certified copies of the priority documents have been received in Application No. _____.
 - 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

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

Attachment(s)

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

DETAILED ACTION

1. Claims 1-29 are pending.
2. Claims 28 and 29 are new.

Continued Examination Under 37 CFR 1.114

3. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 4/8/11 has been entered.

Response to Arguments

4. Applicant's arguments with respect to claims 1-29 have been considered but some are not persuasive and some are moot in view of the new ground(s) of rejection.

On page 4 of the applicant's response, the applicant states that the key in Kunzinger does not correspond to the unique identity of the present invention.

The examiner respectfully disagrees, but has provided clarification. The messages exchanged in Kunzinger are part of the IPSec protocol. The protocol uses messages that are encrypted and have a value associated them that is used by a key to read the

Art Unit: 2469

messages. Kunzinger [0067] shows that the messages have ID's associated them, in addition, IPsec uses a hash value that is transmitted with each packet. The "key" is the value that is transmitted with the packet so that it can be read by the receiving device. Therefore, as the claim language reads, the new combination of references does teach the argued limitations.

The examiner invites the applicant to contact the examiner to discuss the claim language and help further advance prosecution of the case.

Claim Rejections - 35 USC § 103

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

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

4. Claims 1,2, 4-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kunzinger (Pub No: 2002/0091921)., and further in view of Gunter et al (Patent No: 7,055,027).

As to claim 1, Kunzinger teaches a method for secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network (*Kunzinger, [0047] L1-13, end to end data sending via an intermediate gateway using secure tunnels*), comprising:

Art Unit: 2469

in the first computer, forming a secure message by giving the secure message a first unique identity and a first destination address to the intermediate computer, (Kunzinger, [0068] L1-3, the hash value of IPSec used by the key is the id and [0013] the outer header has the address of the endpoint of the tunnel, i.e. gateway), sending the secure message containing the first unique identity and the first destination address from the first computer to the intermediate computer message (Kunzinger, [0068] L1-3, the message is sent from the client and received by the gateway [0068] L1-3, the hash value of IPSec used by the key is the id and [0013] the outer header has the address of the endpoint of the tunnel, i.e. gateway),

the intermediate computer receiving the secure message (Kunzinger, [0068] L1-3, the message is sent from the client and received by the gateway) and performing a translation by using the first unique identity to find a second destination address to the second computer (Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel and the data is then forwarded/send the over the second tunnel and [0013] the new packet has the address of the second computer),

the intermediate computer substituting the first destination address with the second destination address to the second computer (Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel and the data is then forwarded/send the over the second tunnel and [0013] the new packet has the address of the second computer),

Art Unit: 2469

the intermediate computer substituting the first unique identity with a second unique identity of the secure connection (Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel and the data is then forwarded/send the over the second tunnel and [0013] the new packet has the address of the second computer), and the intermediate computer forwarding the secure message with the second destination address and the second unique identity to the second computer in the secure connection (Kunzinger, [0074] forwarding the IPSec datagram and [0013] and [0068] the id and address are in the packet of data).

Kunzinger does not expressly the first computer and the second computer negotiating and exchanging keys with one another according to a key exchange protocol to establish a secure connection between the first computer and the second computer via the intermediate computer, the secure connection having a source address of the first computer as a first end point and a destination address of the second computer as a second end point of the secure connection.

However, Gunter teaches the first computer and the second computer negotiating and exchanging keys with one another according to a key exchange protocol to establish a secure connection between the first computer and the second computer via the intermediate computer (Gunter, Fig 4 and Col 6 L36-40, external client 42 and internal client 44 establish a secure connection via the intermediate firewall using a key exchange protocol) the secure connection having a source address of the first computer as a first end point and a destination address of the second computer as

Art Unit: 2469

a second end point of the secure connection (Gunter, Fig 4, the external client 42 is the source of the secure connection and the internal client 44 is the destination)

It would have been obvious to one of ordinary skill in the art at the time of invention to combine the teachings of Kunzinger and Gunter to have the endpoints directly negotiate a key to establish a secure connection, because Gunter teaches that direct key negotiation is a well know method for two endpoints to communicate securely with an intermediary involved (Gunter Col 3 L50-57).

As to claim 2, Kunzinger and Gunter teaches wherein the method further comprises forming the secure message by using an IPSec connection between the first computer and the second computer (Kunzinger, [0067], IPSec protection).

As to claim 4, Kunzinger and Gunter teaches wherein the method further comprises manually performing a preceding distribution of keys to components for forming the IPSec connection (Kunzinger, [0067], IKE is used to for the IPSec connection).

As to claim 5, Kunzinger and Gunter teaches wherein the method further comprises performing a preceding distribution of keys for forming the IPSec connection by an automated key exchange protocol (Kunzinger, [0067], IKE is used to for the IPSec connection).

As to claim 6, Kunzinger and Gunter teaches wherein the method further comprises performing the automated key exchange protocol used for the preceding distribution of keys for forming the IP Sec connection by means of a modified IKE key exchange protocol between the first computer and the intermediate computer (Kunzinger, [0067]).

Art Unit: 2469

using phase2 IKE exchange between the client and gateway, this is a modified protocol because the table at the gateway modifies the IKE packets and inserts a new address automatically) and by means of a standard IKE key exchange protocol between the intermediate computer and the second computer (Kunzinger, [0069] using IKE between gateway and server).

As to claim 7, Kunzinger and Gunter teaches wherein the method further comprises sending the message that is sent from the first computer as a packet that contains message data, an inner IP header containing the actual sender and receiver addresses, an outer IP header containing the addresses of the first computer and the intermediate computer, the unique identity (Kunzinger, [0013], inner and outer headers and negotiated security association).

As to claim 8, Kunzinger and Gunter teaches wherein the method further comprises the IPsec connection being one or more security associations (SA) and the unique identity being one or more SPI values (Kunzinger, [0067], setting up the IPsec SA and the values are SPI values).

As to claim 9, Kunzinger and Gunter teaches wherein the method further comprises performing the matching by using a translation table stored at the intermediate computer (Kunzinger, [0066], the databases are the translation tables).

As to claim 10, Kunzinger and Gunter teaches wherein the method further comprises changing both the address and the SPI-value by the intermediate computer (Kunzinger,

Art Unit: 2469

[0074], the address is changed to point to the tunnel and the ID(SPI) is changed, the SPI is the ID that is exchanged for indexing).

As to claim 11, Kunzinger and Gunter teaches wherein the method further comprises the first computer being a mobile terminal (Kunzinger, [0038], the workstations communicate over a wireless cellular network) so that the mobility is enabled by modifying the translation table at the intermediate computer (Kunzinger, [0067] L13-17, the SAD on the gateway is modified with IKE value).

As to claim 12, Kunzinger and Gunter teaches wherein the method further comprises performing the modification of the translation tables by sending a request for registration of the new address from the first computer to the intermediate computer (Kunzinger, [0062], the client is the IKE initiator with negotiations with the gateway).

As to claim 13, Kunzinger and Gunter teaches wherein the method further comprises sending a reply to the request for registration from the intermediate computer to the first computer (Kunzinger, [0063], the gateway is the IKE responder to the client in the IKE negotiations).

As to claim 14, Kunzinger and Gunter teaches wherein the method further comprises authenticating or encrypting by IPSec the request for registration and/or reply (Kunzinger, [0067], authenticating IPSec).

As to claim 15, Kunzinger and Gunter teaches wherein the method further comprises establishing the key distribution for the secure connections by establishing an IKE protocol translation table, and using the translation table to modify IP addresses and

Art Unit: 2469

cookie values of IKE packets in the intermediate computer (Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel and [0066]-[0067], the IKE protocol addresses, etc are stored in the SAD tables).

As to claim 16, Kunzinger and Gunter teaches wherein the method further comprises establishing the key exchange distribution by: generating an initiator cookie and sending a zero responder cookie to the second computer, generating a responder cookie in the second computer (Kunzinger, [0064] [0065] and [0067], the gateway is the initiator and the server is the responder in the IKE negotiations. [0069] shows an example of IKE negotiations the IDCi and IDCr values are set), establishing a mapping between IP addresses and IKE cookie values in the intermediate computer, and using the translation table to modify IKE packets in flight by modifying the external IP addresses and possibly IKE cookies of the IKE packets (Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel and [0066]-[0067], the IKE protocol addresses, etc are stored in the SAD tables).

As to claim 17, Kunzinger and Gunter teaches wherein the method further comprises modifying a modified IKE protocol between the first computer and the intermediate computer by transmitting the IKE keys from the first computer to the intermediate computer in order to decrypt and modify IKE packets (Kunzinger, [0067], using phase2 IKE exchange between the client and gateway, this is a modified protocol because the table at the gateway modifies the IKE packets and inserts a new address automatically).

Art Unit: 2469

As to claim 18, Kunzinger and Gunter teaches wherein the method further comprises carrying out in a modified IKE protocol between the first computer and the intermediate computer the modification of the IKE packets by the first computer with the intermediate computer requesting such modifications (Kunzinger, [0067], using phase2 IKE exchange between the client and gateway, this is a modified protocol because the table at the gateway modifies the IKE packets and inserts a new address automatically).

As to claim 19, Kunzinger and Gunter teaches wherein the method further comprises defining the address so that the first computer is identified for the second computer by the intermediate computer by means of an IP address taken from a pool of user IP addresses when forming the translation table (Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel and the data is then forwarded/send the over the second tunnel and [0013] the new packet has the address of the second computer).

As to claim 20, Kunzinger and Gunter teaches wherein the method further comprises sending the secure message by using an IPSec transport mode (Kunzinger, [0075] L12-15, IPSec operates in transport mode).

As to claim 21, Kunzinger and Gunter teaches wherein the method further comprises sending the secure message by using an IPSec tunnel mode (Kunzinger, [0075] L12-15, IPSec operates in tunnel mode).

Art Unit: 2469

As to claim 22, Kunzinger teaches a telecommunication network for secure forwarding of messages (Kunzinger, [0047] L1-13, end to end data sending via an intermediate gateway using secure tunnels), comprising:

a first computer, a second computer and an intermediate computer (Kunzinger, [0047] L1-13 and Fig 4, the endpoints and intermediate computer),

the first and the second computers having means for performing an IPSec processing, the intermediate computer having translation means for using translation tables to perform IPSec and IKE translation and for changing a destination address of the intermediate computer of a secure message containing a unique identity to a destination address of the second computer (Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel (IKE/IPSec) and the data is then forwarded/send the over the second tunnel and [0013] the new packet has the address of the second computer), and

the intermediate computer having means for using the unique identity when forwarding the secure message received from the first computer to the second computer in the security association (Kunzinger, [0074] forwarding the IPSec datagram and [0013] and [0068] the hash value and id and address are in the packet of data).

Kunzinger does not expressly teach means for directly negotiating and exchanging keys, according to a key exchange protocol, between the first computer and the second computer to establish a security association having a source address of the first computer as a first end point and a destination address of the second computer as

Art Unit: 2469

a second end point and the intermediate computer forwarding without decrypting the secure message.

However Gunter teaches means for directly negotiating and exchanging keys, according to a key exchange protocol, between the first computer and the second computer to establish a security association (Gunter, Fig 4 and Col 6 L36-40, external client 42 and internal client 44 establish a secure connection via the intermediate firewall using a key exchange protocol) having a source address of the first computer as a first end point and a destination address of the second computer as a second end point (Gunter, Fig 4, the external client 42 is the source of the secure connection and the internal client 44 is the destination) and the intermediate computer forwarding without decrypting the secure message (Gunter, Fig 4 #220-#224, the intermediate firewall transmits the packet without first decrypting it)

It would have been obvious to one of ordinary skill in the art at the time of invention to combine the teachings of Kunzinger and Gunter to have the endpoints directly negotiate a key to establish a secure connection, because Gunter teaches that direct key negotiation is a well know method for two endpoints to communicate securely with an intermediary involved (Gunter Col 3 L50-57).

As to claim 23, Kunzinger and Gunter teaches wherein the translation table for IPSec translation has IP addresses of the intermediate computer to be matched with IP addresses of the second computer (Kunzinger [0074] the gateway uses tables and id to

Art Unit: 2469

translate the packet into a corresponding tunnel and the data is then forwarded/send the over the second tunnel and [0013] the new packet has the address of the second computer).

As to claim 24, Kunzinger and Gunter teaches wherein the translation tables for IKE translation consists of two partitions, one for the communication between the first computer and the intermediate computer and another for the communication between the intermediate computer and the second computer (Kunzinger, [0066] L1-10, each set of interfaces has its own databases).

As to claim 25, Kunzinger and Gunter teaches wherein both partitions of the mapping table for IKE translation contains translation fields for a source IP address, a destination IP address (Kunzinger, [0067] IKE tables have the addresses for endpoint association), initiator and responder cookies between respective computers (Kunzinger, [0067], IDci and IDcr values).

As to claim 26, Kunzinger and Gunter teaches wherein there is another translation table for IKE translation containing fields for matching a given user to a given computer (Kunzinger, [0066], association for a user to an endpoint).

As to claim 27, Kunzinger teaches a telecommunication network for secure forwarding of messages (Kunzinger, [0047] L1-13, end to end data sending via an intermediate gateway using secure tunnels), comprising:

Art Unit: 2469

a first computer, a second computer, an intermediate computer electronically connected to the first computer and the second computer (Kunzinger, [0047] L1-13 and Fig 4, the endpoints and intermediate computer),

means for directly negotiating and exchanging keys between the first computer and the second computer to establish a secure connection having a source address of the first computer as a first end point and a destination address of the second computer as a second end point (Kunzinger, [0072] the cascade enabled flag can not be set and prior art negotiatiion of keys directly takes place [0007] L1-9 and [0014] L1-2 and [0017] L1-3), and

the intermediate computer having means for performing translation between destination addresses and secure identities (Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel and the data is then forwarded/send the over the second tunnel and [0013] the new packet has the address of the second computer) for forwarding a secure message containing a unique identity received from the first computer and using the second computer in the secure connection to the second computer in the secure connection (Kunzinger, [0074] forwarding the IPSec datagram and [0013] and [0068] the id and address are in the packet of data).

Kunzinger does not expressly teach means for directly negotiating and exchanging keys between the first computer and the second computer to establish a secure connection having a source address of the first computer as a first end point

Art Unit: 2469

and a destination address of the second computer as a second end point the intermediate computer forwards without decrypting the secure message and being aware of the keys to encrypt and/or authenticate the secure message and without establishing a new secure connection.

Gunter teaches means for directly negotiating and exchanging keys between the first computer and the second computer to establish a secure connection (*Gunter, Fig 4 and Col 6 L36-40, external client 42 and internal client 44 establish a secure connection via the intermediate firewall using a key exchange protocol*) having a source address of the first computer as a first end point and a destination address of the second computer as a second end point (*Gunter, Fig 4, the external client 42 is the source of the secure connection and the internal client 44 is the destination*) the intermediate computer forwards without decrypting the secure message and being aware of the keys to encrypt and/or authenticate the secure message and without establishing a new secure connection (*Gunter, Fig 4 #220-#224, the intermediate firewall transmits the packet without first decrypting it*)

As to claim 28, Kunzinger and Gunter teaches the method further comprises the intermediate computer substituting the first unique identity with the second unique identity of the secure connection without establishing a new secure connection and without involving the second computer (*Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel (IKE/IPSec) and the data is then*

Art Unit: 2469

forwarded/send the over the second tunnel and [0013] the new packet has the address of the second computer. The second computer is uninvolved in this step and no new connections are created).

As to claim 29, Kunzinger and Gunter teaches the packets between the first computer and the intermediate computers are sent using a UDP protocol (Kunzinger [0043], the packets are UDP packets sent over the protocol).

6. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kunzinger and Gunter as applied to claim 1 above, and further in view of Patel (Pub No: 2002/0004900).

As to claim 3, Kunzinger and Gunter teaches the limitations of claim 1. Kunzinger and Gunter does not teach wherein the method further comprises performing a secure forwarding of the message by making use of SSL or TLS protocols. Patel teaches wherein the method further comprises performing a secure forwarding of the message by making use of SSL or TLS protocols (Patel, [0037] L18-21, SSL for secure connection). It would have been obvious to one of ordinary skill in the art at the time of invention to combine the teachings of Kunzinger and Gunter with Patel to use SSL for the secure connection because Patel teaches that SSL is a well know protocol for a secure connection that can be used like IPsec.

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.

/A. T./
Examiner, Art Unit 2469

Application/Control Number: 10/500,930

Page 18

Art Unit: 2469

/Ian N. Moore/

Supervisory Patent Examiner, Art Unit 2469

Notice of References Cited	Application/Control No. 10/500,930	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	Classification
*	A US-7,055,027	05-2006	Gunter et al.	713/151
	B US-			
	C US-			
	D US-			
	E US-			
	F US-			
	G US-			
	H US-			
	I US-			
	J US-			
	K US-			
	L US-			
	M US-			


FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)				
	U				
	V				
	W				
	X				

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

Index of Claims 	Application/Control No. 10500930	Applicant(s)/Patent Under Reexamination VAARALA ET AL.
	Examiner Jeffrey Seto	Art Unit 2458

✓	Rejected
=	Allowed


-	Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

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

CLAIM		DATE								
Final	Original	10/28/2008	05/28/2009	09/08/2009	03/15/2010	08/21/2010	01/17/2011	04/28/2011		
	1	✓	✓	✓	✓	✓	✓	✓		
	2	✓	✓	✓	✓	✓	✓	✓		
	3	✓	✓	✓	✓	✓	✓	✓		
	4	✓	✓	✓	✓	✓	✓	✓		
	5	✓	✓	✓	✓	✓	✓	✓		
	6	✓	✓	✓	✓	✓	✓	✓		
	7	✓	✓	✓	✓	✓	✓	✓		
	8	✓	✓	✓	✓	✓	✓	✓		
	9	✓	✓	✓	✓	✓	✓	✓		
	10	✓	✓	✓	✓	✓	✓	✓		
	11	✓	✓	✓	✓	✓	✓	✓		
	12	✓	✓	✓	✓	✓	✓	✓		
	13	✓	✓	✓	✓	✓	✓	✓		
	14	✓	✓	✓	✓	✓	✓	✓		
	15	✓	✓	✓	✓	✓	✓	✓		
	16	✓	✓	✓	✓	✓	✓	✓		
	17	✓	✓	✓	✓	✓	✓	✓		
	18	✓	✓	✓	✓	✓	✓	✓		
	19	✓	✓	✓	✓	✓	✓	✓		
	20	✓	✓	✓	✓	✓	✓	✓		
	21	✓	✓	✓	✓	✓	✓	✓		
	22	✓	✓	✓	✓	✓	✓	✓		
	23	✓	✓	✓	✓	✓	✓	✓		
	24	✓	✓	✓	✓	✓	✓	✓		
	25	✓	✓	✓	✓	✓	✓	✓		
	26	✓	✓	✓	✓	✓	✓	✓		
	27	✓	✓	✓	✓	✓	✓	✓		
	28							✓		
	29							✓		

Search Notes 	Application/Control No. 10500930	Applicant(s)/Patent Under Reexamination VAARALA ET AL.
	Examiner Jeffrey Seto	Art Unit 2458

SEARCHED			
Class	Subclass	Date	Examiner
709	236, 229, 245	11-5-2008	JS
ABOVE	UPDATED		

SEARCH NOTES		
Search Notes	Date	Examiner
Limited classification of 709/229, 245	11-5-2008	JS
Inventor search	11-5-2008	JS
Text search of EAST (US Pat, US PG Pub, JPO, EPO, Derwent)	11-5-2008	JS
Updated Text search of EAST (see attached history)	5-28-2009	JS
Updated text search of EAST (see attached history)	9-8-09	JS
EAST search with previous examiner's classes and focus on new limitations	3/15/2010	AT
Conf with B.Bruckart and J.Avellino - Reopen and search IPsec/tunneling/gateway/proxy	8/21/2010	AT
Updated EAST search - see attached	8/21/2010	AT
EAST (USPAT, USGPUB) - see search history printout (Updated 4/28/11)	1/17/2011 (Updated 4/28/11)	AT

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

--	--

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 same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2011/01/17 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

EAST Search History (Interference)

< This search history is empty >

4/ 29/ 2011 6:20:03 PM

H:\ EAST Workspaces\ jeff930.wsp

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

Request for Continued Examination (RCE) Transmittal

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

Application Number	10500930
Filing Date	19 October 2005
First Named Inventor	Sami Vaarala
Art Unit	2458
Examiner Name	Afshawn M. Towfighi
Attorney Docket Number	290.1078USN

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.

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

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

- a. Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.
- i. Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
- ii. Other _____
- b. Enclosed
- i. Amendment/Reply
- ii. Affidavit(s)/ Declaration(s)
- iii. Information Disclosure Statement (IDS)
- iv. Other _____

2. Miscellaneous

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

3. Fees

- The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.
- a. The Director is hereby authorized to charge the following fees, or credit any overpayments, to Deposit Account No. 06-0243. I have enclosed a duplicate copy of this sheet.
- i. RCE fee required under 37 CFR 1.17(e)
- ii. Extension of time fee (37 CFR 1.136 and 1.17)
- iii. Other _____
- b. Check in the amount of \$ _____ enclosed
- c. Payment by credit card (Form PTO-2038 enclosed)

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

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Signature	/rfasth/	Date	8 April 2011
Name (Print/Type)	ROLF FASTH	Registration No.	36,999

CERTIFICATE OF MAILING OR TRANSMISSION

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

Signature	Electronic Submission	Date	8 April 2011
Name (Print/Type)	Rolf Fasth /rfasth/		

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop RCE, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
Attorney Ref. No. 290.1078USN

In re application of

Sami Vaarala, Antti Nuopponen

Art Unit 2458
 Confirmation No. 1571

Serial No. 10/500,930

CERTIFICATE OF MAILING

Filed: 19 October 2005

I HEREBY CERTIFY THAT THIS PAPER AND THE DOCUMENTS
 REFERRED TO AS BEING ATTACHED OR ENCLOSED HERewith
 ARE BEING SUBMITTED ELECTRONICALLY TO THE UNITED
 STATES PATENT AND TRADEMARK OFFICE ON 8 April 2011.

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

/rfasth/

Examiner: Afshawn M. Towfighi

Rolf Fasth
 Attorney for Applicant

Date: 8 April 2011

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) Response to Office Action dated 9 February 2011.
- (X) RCE
- (X) The Commissioner is hereby authorized to charge any 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
 26 Pinecrest Plaza, Suite 2
 Southern Pines, North Carolina 28387-4301

Telephone: 910-687-0001
 Facsimile: 910-295-2152

Attorney Ref. No. 290.1078USN

Electronic Patent Application Fee Transmittal

Application Number:	10500930
Filing Date:	19-Oct-2005
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:	290.1078USN

Filed as Small Entity

U.S. National Stage under 35 USC 371 Filing Fees

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

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Request for continued examination	2801	1	405	405
Total in USD (\$)				405

Electronic Acknowledgement Receipt

EFS ID:	9837112
Application Number:	10500930
International Application Number:	
Confirmation Number:	1571
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:	290.1078USN
Receipt Date:	08-APR-2011
Filing Date:	19-OCT-2005
Time Stamp:	07:02:18
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$405
RAM confirmation Number	9017
Deposit Account	060243
Authorized User	

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

Charge any Additional Fees required under 37 C.F.R. 1.492 (National application filing, search, and examination fees)

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

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

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

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment After Final	AMD.PDF	923306 207d7f4b66cb532ecf60bcb66082f225e8119db	no	27

Warnings:

Information:

2	Request for Continued Examination (RCE)	RCE.PDF	65610 572075a47d69af47ff0a2d6c1aeb40b927ca3a20	no	1
---	---	---------	---	----	---

Warnings:

This is not a USPTO supplied RCE SB30 form.

Information:

3	Miscellaneous Incoming Letter	TRX.PDF	33228 9c756e86bc6e6f868c367929e2f9848e17cebada0	no	1
---	-------------------------------	---------	--	----	---

Warnings:

Information:

4	Fee Worksheet (PTO-875)	fee-info.pdf	29761 d4d0836d0837ce8186b6d3a8aeb7e58525cfc91	no	2
---	-------------------------	--------------	--	----	---

Warnings:

Information:

Total Files Size (in bytes): 1051905

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Art Unit 2458

5 Sami Vaarala and Antti Nuopponen

Serial No. 10/500,930

Filed: 19 October 2005

10

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

Examiner: Afshawn M. Towfighi

15

Date: 7 April 2011

Attorney Docket No. 290.1078USN

20

AMENDMENT

Commissioner for Patents

25

P.O. Box 1450

Alexandria, VA 22313-1450

This is in response to the Office action of 9
February 2011. Please amend the above-identified patent
application as follows:

30

In the Claims:

Amend the claims as follows:

5

1. (Currently amended) A method for secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network, comprising:

10

the first computer and the second computer negotiating and exchanging keys with one another according to a key exchange protocol to establish a secure connection between the first computer and the second computer via the intermediate computer, the secure connection having a source address of the first computer as a first end point and a destination address of the second computer as a second end point of the secure connection,

15

in the first computer, forming a secure message by giving the secure message a first unique identity and a first destination address to the intermediate computer,

20

sending the secure message containing the first unique identity and the first destination address from the first computer to the intermediate computer,

25

the intermediate computer receiving the secure message and performing a translation by using the first unique identity to find a second destination address to the second computer, the intermediate computer substituting the first destination address with the second destination address to the second computer,

30

the intermediate computer substituting the first unique identity with a second unique identity of the secure connection, and

35

the intermediate computer forwarding the secure message with the second destination address and the second unique identity to the second computer in the secure connection.

2. (Previously presented) The method of claim 1 wherein the method further comprises forming the secure message by using an IPSec connection between the first computer and the second computer.

3. (Previously presented) The method of claim 1 wherein the method further comprises performing a secure forwarding of the message by making use of SSL or TLS protocols.

4. (Previously presented) The method of claim 2 wherein the method further comprises manually performing a preceding distribution of keys to components for forming the IPSec connection.

5. (Previously presented) The method of claim 2 wherein the method further comprises performing a preceding distribution of keys for forming the IPSec connection by an automated key exchange protocol.

6. (Previously presented) The method of claim 5 wherein the method further comprises performing the automated key exchange protocol used for the preceding distribution of keys for forming the IP Sec connection by means of a modified IKE key exchange protocol between the first computer and the intermediate computer and by means of a standard IKE key exchange protocol between the intermediate computer and the second computer.

7. (Previously presented) The method of claim 2 wherein the method further comprises sending the message that is sent from the first computer as a packet that contains message data, an inner IP header containing the actual sender and receiver addresses, an outer IP header containing the addresses of the first computer and the intermediate computer, the unique

identity.

8. (Previously presented) The method of claim 1 wherein the
method further comprises the IPsec connection being one or
5 more security associations (SA) and the unique identity being
one or more SPI values.

9. (Previously presented) The method of claim 1 wherein the
method further comprises performing the matching by using a
10 translation table stored at the intermediate computer.

10. (Previously presented) The method of claim 1 wherein the
method further comprises changing both the address and the
SPI-value by the intermediate computer.

15 11. (Previously presented) The method of claim 1 wherein the
method further comprises the first computer being a mobile
terminal so that the mobility is enabled by modifying the
translation table at the intermediate computer.

20 12. (Previously presented) The method of claim 11 wherein the
method further comprises performing the modification of the
translation tables by sending a request for registration of
the new address from the first computer to the intermediate
25 computer.

13. (Previously presented) The method of claim 12 wherein the
method further comprises sending a reply to the request for
registration from the intermediate computer to the first
30 computer.

14. (Previously presented) The method of claim 12 wherein the
method further comprises authenticating or encrypting by IPsec
the request for registration and/or reply.

35

15. (Previously presented) The method of claim 4 wherein the method further comprises establishing the key distribution for the secure connections by establishing an IKE protocol translation table, and using the translation table to modify
5 IP addresses and cookie values of IKE packets in the intermediate computer.

16. (Previously presented) The method of claim 15 wherein the method further comprises establishing the key exchange
10 distribution by:
generating an initiator cookie and sending a zero responder cookie to the second computer,
generating a responder cookie in the second computer,
establishing a mapping between IP addresses and IKE cookie
15 values in the intermediate computer, and
using the translation table to modify IKE packets in flight by modifying the external IP addresses and possibly IKE cookies of the IKE packets.

17. (Previously presented) The method of claim 15 wherein the method further comprises modifying a modified IKE protocol between the first computer and the intermediate computer by transmitting the IKE keys from the first computer to the intermediate computer in order to decrypt and modify IKE
25 packets.

18. (Previously presented) The method of claim 15 wherein the method further comprises carrying out in a modified IKE protocol between the first computer and the intermediate
30 computer the modification of the IKE packets by the first computer with the intermediate computer requesting such modifications.

19. (Previously presented) The method of claim 17 wherein the
35 method further comprises defining the address so that the

first computer is identified for the second computer by the intermediate computer by means of an IP address taken from a pool of user IP addresses when forming the translation table.

5 20. (Previously presented) The method of claim 1 wherein the method further comprises sending the secure message by using an IPSec transport mode.

10 21. (Previously presented) The method of claim 1 wherein the method further comprises sending the secure message by using an IPSec tunnel mode.

22. (Currently amended) A telecommunication network for secure forwarding of messages, comprising:
15 a first computer, a second computer and an intermediate computer,
means for directly negotiating and exchanging keys, according to a key exchange protocol, between the first computer and the second computer to establish a security association having a
20 source address of the first computer as a first end point and an IP destination address of the second computer as a second end point,
the first and the second computers having means for performing an IPSec processing,
25 the intermediate computer having translation means for using translation tables to perform IPsec ~~IPSee~~ and IKE translation and for changing a destination address of the intermediate computer of a secure message, containing a unique identity, to
30 a destination address of the second computer without decrypting the secure message, and
the intermediate computer having means for using the unique identity when forwarding the secure message received from the first computer to the second computer in the security association.

35

23. (Previously presented) The telecommunication network of claim 22 wherein the translation table for IPSec translation has IP addresses of the intermediate computer to be matched with IP addresses of the second computer.

5

24. (Previously presented) The telecommunication network of claim 22 wherein the translation tables for IKE translation consists of two partitions, one for the communication between the first computer and the intermediate computer and another
10 for the communication between the intermediate computer and the second computer.

25. (Previously presented) The telecommunication network of claim 24 wherein both partitions of the mapping table for IKE
15 translation contains translation fields for a source IP address, a destination IP address, initiator and responder cookies between respective computers.

26. (Previously presented) The telecommunication network of claim 22 wherein there is another translation table for IKE
20 translation containing fields for matching a given user to a given computer.

27. (Currently amended) A telecommunication network for secure
25 forwarding of messages, comprising:
a first computer,
a second computer,
an intermediate computer electronically connected to the first computer and the second computer,
30 a negotiating and key exchanging module between the first computer and the second computer to establish a secure connection having a source address of the first computer as a first end point and a destination address of the second computer as a second end point, and
35 the intermediate computer performing translation between

destination addresses and secure identities for forwarding ~~secure messages~~ a secure message, containing a unique identity, received from the first computer and using the unique identity when forwarding the secure message to the
5 second computer in the secure connection without decrypting the secure message and being aware of the keys to encrypt and/or authenticate the secure message and without establishing a new secure connection.

10 28. (New) The method of claim 1 wherein the method further comprises the intermediate computer substituting the first unique identity with the second unique identity of the secure connection without establishing a new secure connection and without involving the second computer.

15 29. (New) The method of claim 1 wherein the packets between the first computer and intermediate computers are sent using a UDP protocol.

REMARKS/ARGUMENTS

5 Reconsideration of the application is respectfully
requested. Claims 1-2, 4-27 were rejected under Section 102
as being anticipated by Kunzinger. This rejection is
respectfully traversed. Claims 28-29 have been added to the
application. No new matter has been added to the application.

10 Applicants submit that Kunzinger merely teaches end-
to-end protection between the client and the server when the
flag cannot be set and the use of cascaded tunnels (see
abstract) when the flag can be set in which, as shown in Fig.
4, a first tunnel extends between the first computer (client)
15 and the intermediate computer (boundary device or gateway) and
a second tunnel extends between the intermediate computer and
a second computer (server). The first tunnel provides
security through the Internet and the second tunnel provides
security through an intranet (see paragraph [0051] of
20 Kunzinger). Kunzinger explains in paragraph [0047] that the
"use of cascaded tunnels (as opposed to one tunnel or SA
extending from the client to the server) allows security
protection to be tailored to the requirements of a particular
network segment." He also explains that the security gateway
25 serves as a point of entry into the intranet (paragraph 0050)
and that the security gateway 420 retains the ability to
provide of the type of services available in the environment

of Fig. 3. These services include access control and network address translation that require content inspection. In other words, the gateway protects the intranet from undesirable communication from the open Internet by inspecting the content of incoming packets before the packets enter into the intranet. This requires the gateway (intermediate computer) to decrypt the incoming packet in order to be able to inspect the content of the incoming packet. In the current invention, the intermediate computer does not need to know the cryptographic keys or read the content but is able to use the outer IP addresses and the incoming SPI value (= unique identity) to determine how to modify the outer address and the SPI to suite the second computer, which is the next destination.

In paragraph [0013], Kunzinger explains that the security associations are negotiated between the tunnel endpoints i.e. a first negotiation is between the endpoints of tunnel 1 and a second negotiation is between the endpoints of tunnel 2. This means the client 405 negotiates with the gateway 420 to establish tunnel 1 (but not with the server 440). Similarly, the gateway 420 negotiates with the server 440 to establish tunnel 2.

As indicated above, Kunzinger clearly teaches the advantage of using cascade tunnels which provide the tailoring features (see paragraph [0047]) "as opposed to a tunnel or SA extending from the client to the server." Also, in paragraphs

[0012-0014] Kunzinger explains that each tunnel is a separate connection. Also, in paragraphs 0067-0068 Kunzinger explains if there is no existing cascaded tunnel available between the gateway 420 and the server 440 then a pair of IKE and IPSec security associations are established to provide the next tunnel (which again indicates that there are two separate tunnels and not one tunnel).

On page 4 of the Office action, the Examiner states that Kunzinger's key is equivalent to the "first unique identity" required in the claim 1. Applicants are still puzzled over this statement. A key is something used for encryption and decryption (lock and unlock). It is submitted it would not make sense to send a secure message that includes the key in the same message. If the key is sent together with the encrypted message then the encryption would be meaningless since anyone would have access to the key and would be able to decrypt and read the encrypted secure message. A key therefore does not need to be sent in the same encrypted message. It could be like leaving the key in a locked door when leaving your house. Also, if the key were sent as data in the encrypted message, then the recipient could not gain access to the key included in the encrypted message because the recipient could not gain access to the key either to be able to decrypt/open the encrypted message. It is therefore submitted that the key in Kunzinger does not correspond to the unique identity of the present invention and that the key in

Kunzinger would not be contained in the secured message since the amended claim 1 now requires that the secure message contains the first unique identity and the first destination address. Support may, for example, be found in paragraph
5 [0043] and the original claim 7 of the published US 2006/0173968.

Claim 1 has also been amended to specify that there is a secure connection between the first computer and the second computer via the intermediate computer. Support may be
10 found in paragraph [0075] which states that an IPSec connection is formed between the first computer and the second computer. As clearly shown in Fig. 4 of Kunzinger, his system has two connections when the flag can be set, one tunnel between the client 405 and the gateway 420 and a second tunnel
15 between the device 420 and the gateway 440. More particularly, the amended claim 1 requires the step of "the first computer and the second computer negotiating and exchanging keys with one another according to a key exchange protocol to establish a secure connection between the first
20 computer and the second computer via the intermediate computer." This means that there is a secure connection in the present invention that extends between the first computer and the second computer. Thanks to the unique features of the present invention, the secured information flow can work all
25 the way from the first computer to the second computer even if there is an intermediate computer therebetween.

In contrast, Kunzinger teaches two (or more) successive secure connections (IPSec tunnels one after another). As indicated above, this is clearly shown in Fig. 4 of Kunzinger wherein the first secure connection (Tunnel 1) extends between the client (the first computer) and the gateway (the intermediate computer) and the second secure connection (Tunnel 2) extends between the gateway and the endpoint (the second computer). In other words, each tunnel is a separate secure connection, as explained very well in paragraphs [0012] and [0014]. This means there is no direct secure connection extending between the client 405 and the server 440 in Kunzinger when the flag is set. This interpretation is verified in Kunzinger's claim 1 and abstract. Of course, as indicated earlier, Kunzinger expressly teaches away from using such a secure connection when the flag is set since the intermediate gateway 420 would be prevented from access, as explained in paragraph [0017].

In Kunzinger there is thus not any key negotiation between the client 405 and the server 440 when the flag is set. In contrast, the client 405 first changes keys with the gateway 420, and thereafter, the gateway 420 exchanges keys with the server 440. Please also see Fig. 11 and paragraphs [0071 - 0074] of Kunzinger.

On page 2 of the Office action, the Examiner states that Kunzinger teaches a direct key exchange between a first computer (client in Kunzinger) and a second computer (server

in Kunzinger). However, paragraph [0072] referred to by the Examiner teaches that if cascading-enabled flag is not set, the packet will be forwarded as in prior art. The prior art method is described in paragraphs [0050-0051] and in Fig. 3 of
5 Kunzinger. Fig. 3 clearly shows that the secure tunnel (Tunnel 1) is between the client and the gateway (equivalent to the intermediate computer of the present invention). So the key exchange to establish the secure connection takes place between the client and the gateway in Kunzinger (when
10 cascading-enabled flag is not set) and not between the client and the server via the gateway, as required by the amended claim 1. It should be noted that the prior art technology Kunzinger is referring to when the flag cannot be set is described in Figs. 1-3, 5 and 7 and not the prior art
15 technology described in paragraph [0017], lines 1-3. Paragraph [0017] merely mentions the possibility of extending the security association between the client and the server but Kunzinger never teaches that this end-to-end protection is to be used when the flag cannot be set. Even if Kunzinger did
20 teach this, Kunzinger still fails to teach or suggest sending a message that contains the unique identity and using this unique identity to identify the address to the second computer.

It is submitted that the secure tunnel (Tunnel 1) in
25 Fig. 3 could extend between the client and the server because in Kunzinger, the gateways has clear text access to datagrams

as explained in paragraph [0027], lines 13-15. If the tunnel would be between the client and the server, then the gateway would not have clear text access to the datagrams. In paragraph [0017], Kunzinger explains that there are several
5 disadvantages in providing an end-to-end security association between the two end-points (i.e. between the client and server, see paragraph 0017) because any "intermediate system in the network path are prevented from accessing the clear-text data content of the transmitted packets, because only the
10 two endpoints are able to encrypt and decrypt the packets on this SA." In other words, Kunzinger expressly teaches away from a security association that extends between the client (first computer) and the server (the second computer) when the flag is set which is the only time the gateway would be using
15 the id to identify the second computer. A secure connection that extends between the first computer and the second computer is exactly what is required by the amended claim 1 and that the intermediate computer uses the unique identity contained in the secure message to find the address to the
20 second computer.

Applicants fail to see why a person of ordinary skill in the art would look to Kunzinger to learn about establishing a secure connection between the first computer and the second computer in which the first computer is the
25 first end-point and the second computer the second end-point and the intermediate computer using the unique identity

contained in the secure message to find the address to the second computer when Kunzinger expressly teaches away from this feature when the flag is set since the intermediate computer would be prevented from accessing the clear-text data content described in paragraph [0017]. When the flag is not set the gateway would not use any unique identity contained in the secure message to find an address for the second computer.

It is noted that the Examiner has split up the step of "the first computer and the second computer negotiating and exchanging keys with one another according to a key exchange protocol to establish a secure connection between the first computer and the second computer via the intermediate computer." First, the Examiner states that the direct communication is taught in Kunzinger when the cascade-enabled flag is not set [see paragraph 0072] and then the use of intermediate computer is taught when cascade-enabled flag is set (see paragraph [0068]). The use of cascade-enabled flag is clearly mutually exclusive since it cannot be on and off at the same time so the teaching of paragraphs [0072] and [0068] cannot be combined in the manner suggested.

It is also noted that the Examiner has not commented on all the arguments presented in the previous response. The Examiner is respectfully requested to review and consider all the arguments presented.

On pages 3-8 of the Office action, the Examiner refers to paragraphs [0067] and [0068] of Kunzinger. However

the cited paragraphs, among other things, explain that the gateway decrypts that incoming data packet by using the decryption key that corresponds to the particular secure association i.e. Tunnel 1 extending between the client and the gateway. Kunzinger then explains that whether the message is intended to be forwarded further in the secured form (to the endpoint) then a Tunnel 2 has to be used and if there is no Tunnel 2 then it has to be established by means of a key exchange (IKE) procedure. Kunzinger explains that the policy "will direct the gateway to either use an existing cascaded tunnel, or if one is not available, to establish a pair of IKE and IPsec security associations that will provide this next cascaded tunnel. Kunzinger is here referring to Tunnel 2. This again confirms that Kunzinger teaches two separate tunnels (secure connections) and it is submitted that it would not have been possible for Kunzinger's gateway to have decrypted the packet had the tunnel extended all the way between Kunzinger's client and server.

In several places of the Office action, the Examiner refers to paragraph [0013] of Kunzinger. This paragraph explains what an IPsec packet generally consists of. More importantly, the paragraph explains that the negotiation takes place between the tunnel endpoints. This means there is no secure connection negotiation between the client and the server since the first tunnel (Tunnel 1) ends at the gateway and the second tunnel (Tunnel 2) only extends between the

gateway and the server. In other words, the negotiations take place between the client and the gateway regarding Tunnel 1 and between the gateway and the server regarding Tunnel 2 since those represent the endpoints of the two tunnels when
5 the flag is set and the gateway is actively involved. The amended claim 1 requires negotiation between the first computer (Kunzinger's client) and the second computer (Kunzinger's server) since the current invention needs only one secure connection even if there is an intermediate
10 computer between the endpoints of the secure connection. It is submitted that Kunzinger fails to teach or suggest all these steps.

It is submitted that Kunzinger would require extensive modifications that are not taught or suggested to
15 arrive at the features of the present invention. Applicants fail to see why a person of ordinary skill in the art would look to Kunzinger to learn about the secure connection and the key exchange between the first and second computer when Kunzinger completely fails to teach or suggest these and other
20 steps of the amended claim 1.

In view thereof, claim 1 is submitted to be allowable.

Claims 2, 4-21 are submitted to be allowable because they depend upon the allowable base claim 1 and because each
25 claim includes limitations that are not taught or suggested in the cited references.

Independent claim 22 is submitted to be allowable for reasons similar to the reasons put forth above. Claim 22 has been amended to now require that the secure message contains the unique identity and that the intermediate
5 computer has a module performing the IPsec and IKE translation etc. without decrypting the secure message. Support for this limitation may be found in paragraph [0085].

In contrast, the intermediate computer in Kunzinger decrypts the incoming secured message, as explained above. An
10 important function of Kunzinger's gateways is to function as a port of entry into an intranet and to inspect the content of incoming secure packets which requires decryption of the packets before forwarding them to the server (the second computer) in the intranet. In other words, the decryption is
15 an important function of Kunzinger's invention because the security gateway (intermediate computer) must be able to decrypt the packet so that it can provide the important services of access control, network address translation etc. that require content inspection, as explained in for example,
20 paragraph [0050] of Kunzinger. Throughout the Kunzinger patent, the feature of content inspection is emphasized and it is submitted it would be contrary to the spirit of Kunzinger to modify his system to prevent the security gateway from being able to inspect the content of the incoming packets. It
25 is submitted that Kunzinger would require extensive modifications that are not taught or suggested in the cited

references in order to meet the requirements of the amended claim 22.

5 Claims 23-26 are submitted to be allowable because they depend upon the allowable base claim 22 and because each claim includes limitations that are not taught or suggested in the cited references.

10 Independent claim 27 is submitted to be allowable for the same reasons as those put forth for the patentability of claim 22. In addition, the amended claim 27 requires a module for performing the IPsec and IKE translation etc. without undoing the IPsec processing and being aware of the keys to encrypt and/or authenticate the secure message and without establishing a new IPsec connection and that the secure message contains the unique identity. Support for
15 these amendments may, for example, be found in paragraphs [0045, 0047, and 0073].

Claim 3 was rejected under Section 103 as being obvious over Kunzinger in view of Patel. This rejection is respectfully traversed.

20 Claim 3 is submitted to be allowable because it depends upon the allowable base claim 1 and because the claim includes limitations that are not taught or suggested in the cited references.

25 New claims 28-29 are submitted to be allowable because they depend upon the allowable base claim 1 and because the claims include limitations that are not taught or

suggested in the cited references. Support may, for example, be found in paragraphs [0047 and 0053] of the current application.

Paragraph [0074] of Kunzinger explains that a second
5 successive secure connection is established (to create Tunnel
2), since there is a new key exchange performed between the
gateway and the server and the copied values (IDci and IDcr)
from the SAD database from Tunnel 1 are used to create Tunnel
2. To be able to fully understand paragraph [0074], the
10 Examiner is requested to also review paragraphs [0068] and
[0069] first. Paragraph [0068] explains that "when a data
packet arrives from the client at the gateway, the gateway can
decrypt that packet using the decryption key corresponding to
the IPsec SA established with the client on the Tunnel 1 side.
15 At this point in the process, the gateway is in possession of
a clear text copy" of the message with the start address
9.1.2.3. (=the client's address, i.e. the first computer) and
the destination address 8.1.2.3 (the server's address, i.e.
the second computer). Paragraph [0068] further states that
20 the gateway is directed to use an existing tunnel or to
establish a pair of IKE and IPsec security associations that
provide the next tunnel. Paragraph [0069] explains if the
message has to be sent further as an IPsec, then the gateway
plays the role of an IKE initiator for the purposes of
25 establishing an IPsec SA with server (which is the endpoint).
Kunzinger thus teaches the gateway establishing a new tunnel

(secure connection) and the gateway involves the server (the second computer) which is opposite to what is required by the new claim 28.

5 In view thereof, claims 28-29 are submitted to be allowable.

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

10 Respectfully submitted,
FASTH LAW OFFICES

15
20 /rfasth/
Rolf Fasth
Registration No. 36,999

ATTORNEY DOCKET NO. 290.1078USN

25 FASTH LAW OFFICES
26 Pinecrest Plaza, Suite 2
Southern Pines, NC 28387-4301

Telephone: (910) 687-0001
Facsimile: (910) 295-2152

It is submitted that Kunzinger and the other cited references fail to teach or suggest the step of the first and second computers exchanging keys with one another to establish the secure connection that has a source address of the first computer and a destination address of the second computer.

On page 4 of the Office action, the Examiner has interpreted paragraph [0013] of Kunzinger so that the IPsec inner header specifies the end points of the secure connection. However in paragraph [0013], it stated that the outer IP header specifies the end points of the tunnel (which is the secure connection in that context) and the inner header specifies the original source and the destination of the packet (so outside of the tunnel of those packets can be clear text).

Again, the examiner says that the key is the id, but in IPsec none of the messages contains any keys. Maybe we should ask the examiner to show where it is taught to put keys in packets? Or we could clarify the feature so that the unique identity must be in message?

REPETITION OUR FOREGOING INSTRUCTIONS
Please make use of them again and try to convince the examiner. He has not commented the most of our response:

When we, in our invention as claimed, "give the secure message an unique identity and a first destination address to the intermediate computer", we mean information that is outer information outside the encrypted message. The Examiner says that "the key is the id". This is, however, of no sense. A key is a tool that is used to decrypt (remove encryption) from an encrypted message.

As a summary we show in an illustrative way the differences between the invention and Kunzinger. Differences in our invention underlined.

40

	Our invention	Kunzinger
Message data	<u>IPSec encrypted=</u> <u>IPSec message</u>	<u>IPSec encrypted=</u> <u>IPSec message</u>
Outer IP header in IPSec message (outside encrypted	<u>the source</u> <u>address= first</u> <u>computer</u>	<u>the source</u> <u>address= first</u> <u>computer</u>

message data (the destination address= intermediate computer	the destination address= intermediate computer
Inner IP header in IPsec message (inside encrypted message data)	the source address= first computer the destination address= second computer	the source address= first computer the destination address= second computer
Inside outer IP header but outside inner IP header = in unencrypted part being outside information	Unique identity	No unique identity
Intermediate computer action	- No decryption of IPsec message - Finding address of second computer to be the new destination address by means of unique identity - Changing destination address in outer IP header to address of second computer	- Decryption of IPsec message - Finding address of second computer to be the new destination address by reading from Inner IPsec header - if found address not in use -> translating address by means of a table - creating new IPsec SA from intermediate to second computer by performing key exchange and IKE and - creating new outer and inner IP headers Or using an already established IPsec SA from intermediate to second computer
New outer IP header	the source	the source

	address= the intermediate computer the destination address= the second computer	address= the intermediate computer the destination address= the second computer, which might be a translated address, see above.
New inner IP header	the source address= first computer the destination address= second computer (Not changed!!!)	the source address= the intermediate computer the destination address= the second computer

~~Final comments~~

5 ~~As is explained in the table, in Kunzinger, the message is decrypted by the intermediate computer. And the intermediate computer uses another tunnel 2, which has to be separately established to sent the message further with IPSee.~~

10

~~Claim 1 has been amended to clarify that the first computer and second computer negotiate and exchanges key with one another to establish the secure connection. Support may be found in, for example, paragraphs 0075-0093 of the corresponding published US 2006/0173968. The secure connection extending between the first computer and the second computer is shown in Fig. 1.~~

15

~~In view thereof, Applicants even submit that Kunzinger teaches away from the first computer and the second computer negotiating and exchanging keys with one another to establish a secure connection between the first computer and~~

20

~~the second computer. More particularly, Kunzinger fails to teach or suggest the direct exchange of keys between the client 405 and the server 440. The key exchanges described in Kunzinger are only between the client (first computer) and the gateway (intermediate computer) to establish tunnel 1 and then between the gateway (intermediate computer) and the server (second computer) to establish tunnel 2. In other words, in Kunzinger the client 405 first exchanges keys with the gateway 420 (intermediate computer) and thereafter the gateway 420, in turn, exchanges keys with the server 440 (the second computer). There is thus no direct exchange between the client 405 and the server 440 to establish a tunnel between the client 405 to the server 440. There is therefore no key exchange between the client and the server either.~~

~~Independent claims 22 and 27 are submitted to be allowable for reasons similar to the reasons put forth for the allowability of the amended claim 1. More particularly, it is submitted that none of the cited references teaches means for directly exchanging and negotiating keys between the first and second computer. As explained above, an important function of Kunzinger's gateways is to function as a port of entry into an intranet and to inspect the content of incoming secure packets which requires decryption of the packets before forwarding them to the server (the second computer) in the intranet. There should therefore be no direct communication between the client and the server since the role of the gateway is to~~

~~inspect the incoming packets before they enter the intranet.~~

~~----- In view thereof, claims 22 and 27 are submitted to
be allowable.~~

~~Summary~~

5 ~~As is stated in [0013] of Kunzinger, A message that is sent
with IPsec contains~~

~~— Message data~~

~~— An outer IP header with~~

~~— the source address~~

10 ~~— the destination address~~

~~— An inner IP header with~~

~~— the source address~~

~~— the destination address~~

15 ~~Both our invention and Kunzinger have a first computer
(Kunzinger's client), an intermediate computer (Kunzinger's
gateway) and a second computer (Kunzinger's server)~~

20 ~~Also, please look at the table above, then it is understood
what is meant by network translating in Kunzinger. Sometimes
an endpoint address is just not right since e.g. a LAN uses
the same endpoint address for each computer in the Local Area
Network, officially end if a certain computer in the LAN is
wanted to reach, a network translation has to be done. But
25 this network translation has nothing with the IPsec message's
IP headers to do.~~

30 ~~The advantages are that, no new IPsec (no new tunnel has to be
established or used) and that the intermediate computer can
forward the message in IPsec form without reading the message
(which is a security question, too and improves the
security).~~

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 10/500,930	Filing Date 10/19/2005	<input type="checkbox"/> To be Mailed
---	---	----------------------------------	---------------------------------------

APPLICATION AS FILED – PART I			OTHER THAN SMALL ENTITY				
	(Column 1)	(Column 2)	SMALL ENTITY <input checked="" type="checkbox"/>	OR			
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	OR	RATE (\$)	FEE (\$)
<input type="checkbox"/> BASIC FEE <small>(37 CFR 1.16(a), (b), or (c))</small>	N/A	N/A	N/A			N/A	
<input type="checkbox"/> SEARCH FEE <small>(37 CFR 1.16(k), (j), or (m))</small>	N/A	N/A	N/A			N/A	
<input type="checkbox"/> EXAMINATION FEE <small>(37 CFR 1.16(o), (p), or (q))</small>	N/A	N/A	N/A			N/A	
TOTAL CLAIMS <small>(37 CFR 1.16(j))</small>	minus 20 =	*	X \$ =		OR	X \$ =	
INDEPENDENT CLAIMS <small>(37 CFR 1.16(h))</small>	minus 3 =	*	X \$ =			X \$ =	
<input type="checkbox"/> APPLICATION SIZE FEE <small>(37 CFR 1.16(s))</small>	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT <small>(37 CFR 1.16(j))</small>							
			TOTAL			TOTAL	

* If the difference in column 1 is less than zero, enter "0" in column 2.

APPLICATION AS AMENDED – PART II					OTHER THAN SMALL ENTITY				
	(Column 1)	(Column 2)	(Column 3)		SMALL ENTITY	OR			
AMENDMENT	04/08/2011	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	* 29	Minus ** 27	= 2	X \$26 =	52		X \$ =	
	Independent (37 CFR 1.16(h))	* 3	Minus ***3	= 0	X \$110 =	0		X \$ =	
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))								
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						OR		
					TOTAL ADD'L FEE	52	OR	TOTAL ADD'L FEE	

	(Column 1)	(Column 2)	(Column 3)						
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	*	Minus **	=	X \$ =			X \$ =	
	Independent (37 CFR 1.16(h))	*	Minus ***	=	X \$ =			X \$ =	
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))								
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

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

Legal Instrument Examiner:
/BRENDA WEBB/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
 If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Document code: WFEE

United States Patent and Trademark Office
Sales Receipt for Accounting Date: 04/12/2011

BDENNY SALE #00000001 Mailroom Dt: 04/08/2011 060243 10500930
 01 FC : 2202 52.00 DA



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.
10/500,930	10/19/2005	Sami Vaarala	290.1078USN	1571
33369	7590	02/09/2011	EXAMINER	
FASTH LAW OFFICES (ROLF FASTH) 26 PINECREST PLAZA, SUITE 2 SOUTHERN PINES, NC 28387-4301			TOWFIGHI, AFSHAWN M	
			ART UNIT	PAPER NUMBER
			2469	
			NOTIFICATION DATE	DELIVERY MODE
			02/09/2011	ELECTRONIC

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

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

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

sloan.smith@fasthlaw.com
nan_russell@fasthlaw.com

Office Action Summary

Application No. 10/500,930	Applicant(s) VAARALA ET AL.	
Examiner AFSHAWN TOWFIGHI	Art Unit 2469	

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

Period for Reply

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

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

Status

- 1) Responsive to communication(s) filed on 17 November 2010.
- 2a) This action is **FINAL**.
- 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-27 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-27 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

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

Attachment(s)

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

Examiner-Initiated Interview Summary	Application No. 10/500,930	Applicant(s) VAARALA ET AL.	
	Examiner AFSHAWN TOWFIGHI	Art Unit 2469	

All Participants:

(1) AFSHAWN TOWFIGHI.

(2) Rolf Fasth.

Status of Application: RESPONSE TO NON-FINAL OFFICE ACTION ENTERED

(3) _____.

(4) _____.

Date of Interview: 19 January 2011

Time: 12:00pm

Type of Interview:

- Telephonic
 Video Conference
 Personal (Copy given to: Applicant Applicant's representative)

Exhibit Shown or Demonstrated: Yes No

If Yes, provide a brief description:

Part I.

Rejection(s) discussed:

N/A

Claims discussed:

N/A

Prior art documents discussed:

N/A

Part II.

SUBSTANCE OF INTERVIEW DESCRIBING THE GENERAL NATURE OF WHAT WAS DISCUSSED:

See Continuation Sheet

Part III.

- It is not necessary for applicant to provide a separate record of the substance of the interview, since the interview directly resulted in the allowance of the application. The examiner will provide a written summary of the substance of the interview in the Notice of Allowability.
 It is not necessary for applicant to provide a separate record of the substance of the interview, since the interview did not result in resolution of all issues. A brief summary by the examiner appears in Part II above.

/A. T./

Examiner, Art Unit 2469

(Applicant/Applicant's Representative Signature – if appropriate)

Continuation of Substance of Interview including description of the general nature of what was discussed: Examiner contacted applicant's representative and informed him of possible allowable subject matter that was found and to contact the examiner as soon as possible. Examiner and applicant agreed to send the final office action, and speak after the applicant's representative has spoken with the client and received the examiner's action.

DETAILED ACTION

1. Claims 1-27 are pending.
2. Claims 1, 22, and 27 are amended.

Response to Arguments

4. Applicant's arguments filed with respect to claims 1-27 have been fully considered but they are not persuasive.

On page 11 of the applicant's response, the applicant argues that Kunzinger fails to teach or suggest the direct exchange of keys between the client and the server, and that Kunzinger teaches away from the first computer and second computer negotiating and exchanging keys with one another.

The examiner respectfully disagrees. Kunzinger teaches a security method between two end points, and does not teach away from direct communication but in fact teaches an embodiment where direct negotiation occurs. Kunzinger, [0072], teaches that the cascade enabled flag may not be set. When the flag is not set then the system uses prior art methods of secure connection. Prior art methods have the two endpoints negotiate keys with one another [0007] L1-9 and [0014] L1-2 and [0017] L1-3. The negotiation is direct with one another, and each endpoint is equivalent to the first computer and the second computer. Therefore Kunzinger does teach the argued limitations and does not teach away from the claimed invention.

Art Unit: 2469

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1, 2, 4-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Kunzinger (Pub No: 2002/0091921).

As to claim 1, Kunzinger teaches a method for secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network (*Kunzinger, [0047] L1-13, end to end data sending via an intermediate gateway using secure tunnels*), comprising: the first computer and the second computer negotiating and exchanging keys with one another (*Kunzinger, [0072] the cascade enabled flag can not be set and prior art negotiatiion of keys directly takes place [0007] L1-9 and [0014] L1-2 and [0017] L1-3*) according to a key exchange protocol to establish a secure connection between the first computer and the second computer via the intermediate computer (*Kunzinger, [0067] and [0068], the client establishes a secure connection to the endpoint using the IPSec and internet key exchange policy since the endpoint is within and intranet a gateway is an intermediary*), the secure connection having a source address of the first computer as a first end point

Art Unit: 2469

and a destination address of the second computer as a second end point of the secure connection (Kunzinger, [0013], the IPSec packet has an inner header with the source and destination addresses), in the first computer, forming a secure message by giving the secure message a first unique identity and a first destination address to the intermediate computer, (Kunzinger, [0068] L1-3, the key is the id and [0013] the outer header has the address of the endpoint of the tunnel, i.e. gateway), sending the secure message from the first computer to the intermediate computer, the intermediate computer receiving the secure message (Kunzinger, [0068] L1-3, the message is sent from the client and received by the gateway) and performing a translation by using the first unique identity to find a second destination address to the second computer, the intermediate computer substituting the first destination address with the second destination address to the second computer, the intermediate computer substituting the first unique identity with a second unique identity of the secure connection (Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel and the data is then forwarded/send the over the second tunnel and [0013] the new packet has the address of the second computer), and the intermediate computer forwarding the secure message with the second destination address and the second unique identity to the second computer in the secure connection (Kunzinger, [0074] forwarding the IPSec datagram and [0013] and [0068] the id and address are in the packet of data).

Art Unit: 2469

As to claim 2, Kunzinger teaches wherein the method further comprises forming the secure message by using an IPSec connection between the first computer and the second computer (Kunzinger, [0067], IPSec protection).

As to claim 4, Kunzinger teaches wherein the method further comprises manually performing a preceding distribution of keys to components for forming the IPSec connection (Kunzinger, [0067], IKE is used to for the IPSec connection).

As to claim 5, Kunzinger teaches wherein the method further comprises performing a preceding distribution of keys for forming the IPSec connection by an automated key exchange protocol (Kunzinger, [0067], IKE is used to for the IPSec connection).

As to claim 6, Kunzinger teaches wherein the method further comprises performing the automated key exchange protocol used for the preceding distribution of keys for forming the IP Sec connection by means of a modified IKE key exchange protocol between the first computer and the intermediate computer (Kunzinger, [0067], using phase2 IKE exchange between the client and gateway, this is a modified protocol because the table at the gateway modifies the IKE packets and inserts a new address automatically) and by means of a standard IKE key exchange protocol between the intermediate computer and the second computer (Kunzinger, [0069] using IKE between gateway and server).

As to claim 7, Kunzinger teaches wherein the method further comprises sending the message that is sent from the first computer as a packet that contains message data, an inner IP header containing the actual sender and receiver addresses, an outer IP header containing the addresses of the first computer and the intermediate computer,

Art Unit: 2469

the unique identity (Kunzinger, [0013], inner and outer headers and negotiated security association).

As to claim 8, Kunzinger teaches wherein the method further comprises the IPsec connection being one or more security associations (SA) and the unique identity being one or more SPI values (Kunzinger, [0067], setting up the IPsec SA and the values are SPI values).

As to claim 9, Kunzinger teaches wherein the method further comprises performing the matching by using a translation table stored at the intermediate computer (Kunzinger, [0066], the databases are the translation tables).

As to claim 10, Kunzinger teaches wherein the method further comprises changing both the address and the SPI-value by the intermediate computer (Kunzinger, [0074], the address is changed to point to the tunnel and the ID(SPI) is changed, the SPI is the ID that is exchanged for indexing).

As to claim 11, Kunzinger teaches wherein the method further comprises the first computer being a mobile terminal (Kunzinger, [0038], the workstations communicate over a wireless cellular network) so that the mobility is enabled by modifying the translation table at the intermediate computer (Kunzinger, [0067] L13-17, the SAD on the gateway is modified with IKE value).

As to claim 12, Kunzinger teaches wherein the method further comprises performing the modification of the translation tables by sending a request for registration of the new

Art Unit: 2469

address from the first computer to the intermediate computer (Kunzinger, [0062], the client is the IKE initiator with negotiations with the gateway).

As to claim 13, Kunzinger teaches wherein the method further comprises sending a reply to the request for registration from the intermediate computer to the first computer (Kunzinger, [0063], the gateway is the IKE responder to the client in the IKE negotiations).

As to claim 14, Kunzinger teaches wherein the method further comprises authenticating or encrypting by IPSec the request for registration and/or reply (Kunzinger, [0067], authenticating IPSec).

As to claim 15, Kunzinger teaches wherein the method further comprises establishing the key distribution for the secure connections by establishing an IKE protocol translation table, and using the translation table to modify IP addresses and cookie values of IKE packets in the intermediate computer (Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel and [0066]-[0067], the IKE protocol addresses, etc are stored in the SAD tables).

As to claim 16, Kunzinger teaches wherein the method further comprises establishing the key exchange distribution by: generating an initiator cookie and sending a zero responder cookie to the second computer, generating a responder cookie in the second computer (Kunzinger, [0064] [0065] and [0067], the gateway is the initiator and the server is the responder in the IKE negotiations. [0069] shows an example of IKE negotiations the IDCi and IDCr values are set), establishing a mapping between IP

Art Unit: 2469

addresses and IKE cookie values in the intermediate computer, and using the translation table to modify IKE packets in flight by modifying the external IP addresses and possibly IKE cookies of the IKE packets (Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel and [0066]-[0067], the IKE protocol addresses, etc are stored in the SAD tables).

As to claim 17, Kunzinger teaches wherein the method further comprises modifying a modified IKE protocol between the first computer and the intermediate computer by transmitting the IKE keys from the first computer to the intermediate computer in order to decrypt and modify IKE packets (Kunzinger, [0067], using phase2 IKE exchange between the client and gateway, this is a modified protocol because the table at the gateway modifies the IKE packets and inserts a new address automatically).

As to claim 18, Kunzinger teaches wherein the method further comprises carrying out in a modified IKE protocol between the first computer and the intermediate computer the modification of the IKE packets by the first computer with the intermediate computer requesting such modifications (Kunzinger, [0067], using phase2 IKE exchange between the client and gateway, this is a modified protocol because the table at the gateway modifies the IKE packets and inserts a new address automatically).

As to claim 19, Kunzinger teaches wherein the method further comprises defining the address so that the first computer is identified for the second computer by the intermediate computer by means of an IP address taken from a pool of user IP addresses when forming the translation table (Kunzinger [0074] the gateway uses

Art Unit: 2469

tables and id to translate the packet into a corresponding tunnel and the data is then forwarded/send the over the second tunnel and [0013] the new packet has the address of the second computer).

As to claim 20, Kunzinger teaches wherein the method further comprises sending the secure message by using an IPSec transport mode (Kunzinger, [0075] L12-15, IPSec operates in transport mode).

As to claim 21, Kunzinger teaches wherein the method further comprises sending the secure message by using an IPSec tunnel mode (Kunzinger, [0075] L12-15, IPSec operates in tunnel mode).

As to claim 22, Kunzinger teaches a telecommunication network for secure forwarding of messages (Kunzinger, [0047] L1-13, end to end data sending via an intermediate gateway using secure tunnels), comprising: a first computer, a second computer and an intermediate computer, means for directly negotiating and exchanging keys, according to a key exchange protocol, between the first computer and the second computer to establish a security association having a source address of the first computer as a first end point and a destination address of the second computer as a second end point (Kunzinger, [0072] the cascade enabled flag can not be set and prior art negotiatiion of keys directly takes place [0007] L1-9 and [0014] L1-2 and [0017] L1-3), the first and the second computers having means for performing an IPSec processing, the intermediate computer having translation means for using translation tables to perform IPSec and IKE translation and for changing a destination address of the intermediate computer of a

Art Unit: 2469

secure message to a destination address of the second computer (Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel (IKE/IPSec) and the data is then forwarded/send the over the second tunnel and [0013] the new packet has the address of the second computer), and the intermediate computer having means for forwarding the secure message received from the first computer to the second computer in the security association (Kunzinger, [0074] forwarding the IPSec datagram and [0013] and [0068] the id and address are in the packet of data).

As to claim 23, Kunzinger teaches wherein the translation table for IPSec translation has IP addresses of the intermediate computer to be matched with IP addresses of the second computer (Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel and the data is then forwarded/send the over the second tunnel and [0013] the new packet has the address of the second computer).

As to claim 24, Kunzinger teaches wherein the translation tables for IKE translation consists of two partitions, one for the communication between the first computer and the intermediate computer and another for the communication between the intermediate computer and the second computer (Kunzinger, [0066] L1-10, each set of interfaces has its own databases).

As to claim 25, Kunzinger teaches wherein both partitions of the mapping table for IKE translation contains translation fields for a source IP address, a destination IP address (Kunzinger, [0067] IKE tables have the addresses for endpoint association), initiator and

Art Unit: 2469

responder cookies between respective computers (Kunzinger, [0067], IDci and IDcr values).

As to claim 26, Kunzinger teaches wherein there is another translation table for IKE translation containing fields for matching a given user to a given computer (Kunzinger, [0066], association for a user to an endpoint).

As to claim 27, Kunzinger teaches a telecommunication network for secure forwarding of messages (Kunzinger, [0047] L1-13, end to end data sending via an intermediate gateway using secure tunnels), comprising: a first computer, a second computer, an intermediate computer electronically connected to the first computer and the second computer, means for directly negotiating and exchanging keys between the first computer and the second computer to establish a secure connection having a source address of the first computer as a first end point and a destination address of the second computer as a second end point (Kunzinger, [0072] the cascade enabled flag can not be set and prior art negotiatiion of keys directly takes place [0007] L1-9 and [0014] L1-2 and [0017] L1-3)), and the intermediate computer having means for performing translation between destination addresses and secure identities (Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel and the data is then forwarded/send the over the second tunnel and [0013] the new packet has the address of the second computer) for forwarding secure messages received from the first computer to the second computer in the secure connection (Kunzinger, [0074] forwarding the IPSec datagram and [0013] and [0068] the id and address are in the packet of data).

Claim Rejections - 35 USC § 103

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

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

7. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kunzinger as applied to claim 1 above, and further in view of Patel (Pub No: 2002/0004900).

As to claim 3, Kunzinger teaches the limitations of claim 1. Kunzinger does not teach wherein the method further comprises performing a secure forwarding of the message by making use of SSL or TLS protocols. Patel teaches wherein the method further comprises performing a secure forwarding of the message by making use of SSL or TLS protocols (*Patel, [0037] L18-21, SSL for secure connection*). It would have been obvious to one of ordinary skill in the art at the time of invention to combine the teachings of Kunzinger with Patel to use SSL for the secure connection because Patel teaches that SSL is a well know protocol for a secure connection that can be used like IPsec.

Conclusion

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

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

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.

Art Unit: 2469

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.

/A. T./
Examiner, Art Unit 2469

/Ian N. Moore/
Supervisory Patent Examiner, Art Unit 2469

Notice of References Cited	Application/Control No. 10/500,930	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	Classification
	A US-			
	B US-			
	C US-			
	D US-			
	E US-			
	F US-			
	G US-			
	H US-			
	I US-			
	J US-			
	K US-			
	L US-			
	M US-			


FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)			
	U				
	V				
	W				
	X				

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

Index of Claims 	Application/Control No. 10500930	Applicant(s)/Patent Under Reexamination VAARALA ET AL.
	Examiner Jeffrey Seto	Art Unit 2458

✓	Rejected
=	Allowed


-	Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

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

CLAIM		DATE							
Final	Original	10/28/2008	05/28/2009	09/08/2009	03/15/2010	08/21/2010	01/17/2011		
	1	✓	✓	✓	✓	✓	✓		
	2	✓	✓	✓	✓	✓	✓		
	3	✓	✓	✓	✓	✓	✓		
	4	✓	✓	✓	✓	✓	✓		
	5	✓	✓	✓	✓	✓	✓		
	6	✓	✓	✓	✓	✓	✓		
	7	✓	✓	✓	✓	✓	✓		
	8	✓	✓	✓	✓	✓	✓		
	9	✓	✓	✓	✓	✓	✓		
	10	✓	✓	✓	✓	✓	✓		
	11	✓	✓	✓	✓	✓	✓		
	12	✓	✓	✓	✓	✓	✓		
	13	✓	✓	✓	✓	✓	✓		
	14	✓	✓	✓	✓	✓	✓		
	15	✓	✓	✓	✓	✓	✓		
	16	✓	✓	✓	✓	✓	✓		
	17	✓	✓	✓	✓	✓	✓		
	18	✓	✓	✓	✓	✓	✓		
	19	✓	✓	✓	✓	✓	✓		
	20	✓	✓	✓	✓	✓	✓		
	21	✓	✓	✓	✓	✓	✓		
	22	✓	✓	✓	✓	✓	✓		
	23	✓	✓	✓	✓	✓	✓		
	24	✓	✓	✓	✓	✓	✓		
	25	✓	✓	✓	✓	✓	✓		
	26	✓	✓	✓	✓	✓	✓		
	27	✓	✓	✓	✓	✓	✓		

Search Notes 	Application/Control No. 10500930	Applicant(s)/Patent Under Reexamination VAARALA ET AL.
	Examiner Jeffrey Seto	Art Unit 2458

SEARCHED			
Class	Subclass	Date	Examiner
709	236, 229, 245	11-5-2008	JS

SEARCH NOTES		
Search Notes	Date	Examiner
Limited classification of 709/229, 245	11-5-2008	JS
Inventor search	11-5-2008	JS
Text search of EAST (US Pat, US PG Pub, JPO, EPO, Derwent)	11-5-2008	JS
Updated Text search of EAST (see attached history)	5-28-2009	JS
Updated text search of EAST (see attached history)	9-8-09	JS
EAST search with previous examiner's classes and focus on new limitations	3/15/2010	AT
Conf with B.Bruckart and J.Avellino - Reopen and search IPsec/tunneling/gateway/proxy	8/21/2010	AT
Updated EAST search - see attached	8/21/2010	AT
EAST (USPAT, USPGPUB) - see search history printout	1/17/2011	AT

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

--	--

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 exchange\$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 same (gateway or proxy or intermediate) and cookie	US-PGPUB; USPAT	OR	OFF	2011/01/17 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

EAST Search History (Interference)

< This search history is empty >

1/ 17/ 2011 11:05:33 PM

H:\ EAST Workspaces\ jeff930.wsp

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Art Unit 2458

5 Sami Vaarala and Antti Nuopponen

Serial No. 10/500,930

10 Filed: 19 October 2005

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

15 Examiner: Afshawn M. Towfighi

Date: 16 November 2010

Attorney Docket No. 290.1078USN

20

AMENDMENT

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

This is in response to the Office action of 26
August 2010. Please amend the above-identified patent
application as follows:

30

In the Claims:

Amend the claims as follows:

5

1. (Currently amended) A method for secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network, comprising:

10

the first computer and the second computer negotiating and exchanging keys with one another according to a key exchange protocol to establish a secure connection between the first computer and the second computer via the intermediate computer, the secure connection having a source address of the first computer as a first end point and a destination address of the second computer as a second end point of the secure connection,

15

in the first computer, forming a secure message by giving the secure message a first unique identity and a first destination address to the intermediate computer,

20

sending the secure message from the first computer to the intermediate computer,

the intermediate computer receiving the secure message and performing a translation by using the first unique identity to

25

find a second destination address to the second computer, the intermediate computer substituting the first destination address with the second destination address to the second computer,

the intermediate computer substituting the first unique

30

identity with a second unique identity of the secure connection ~~without establishing a new secure connection and without involving the second computer,~~ and

the intermediate computer forwarding the secure message with the second destination address and the second unique identity to the second computer in the secure connection.

35

2. (Previously presented) The method of claim 1 wherein the method further comprises forming the secure message by using an IPsec connection between the first computer and the second
5 computer.

3. (Previously presented) The method of claim 1 wherein the method further comprises performing a secure forwarding of the message by making use of SSL or TLS protocols.
10

4. (Previously presented) The method of claim 2 wherein the method further comprises manually performing a preceding distribution of keys to components for forming the IPsec connection.
15

5. (Previously presented) The method of claim 2 wherein the method further comprises performing a preceding distribution of keys for forming the IPsec connection by an automated key exchange protocol.
20

6. (Previously presented) The method of claim 5 wherein the method further comprises performing the automated key exchange protocol used for the preceding distribution of keys for forming the IP Sec connection by means of a modified IKE key exchange protocol between the first computer and the
25 intermediate computer and by means of a standard IKE key exchange protocol between the intermediate computer and the second computer.

7. (Previously presented) The method of claim 2 wherein the method further comprises sending the message that is sent from the first computer as a packet that contains message data, an inner IP header containing the actual sender and receiver addresses, an outer IP header containing the addresses of the
30 first computer and the intermediate computer, the unique
35

identity.

8. (Previously presented) The method of claim 1 wherein the
method further comprises the IPSec connection being one or
5 more security associations (SA) and the unique identity being
one or more SPI values.

9. (Previously presented) The method of claim 1 wherein the
method further comprises performing the matching by using a
10 translation table stored at the intermediate computer.

10. (Previously presented) The method of claim 1 wherein the
method further comprises changing both the address and the
SPI-value by the intermediate computer.

11. (Previously presented) The method of claim 1 wherein the
method further comprises the first computer being a mobile
terminal so that the mobility is enabled by modifying the
translation table at the intermediate computer.

12. (Previously presented) The method of claim 11 wherein the
method further comprises performing the modification of the
translation tables by sending a request for registration of
the new address from the first computer to the intermediate
25 computer.

13. (Previously presented) The method of claim 12 wherein the
method further comprises sending a reply to the request for
registration from the intermediate computer to the first
30 computer.

14. (Previously presented) The method of claim 12 wherein the
method further comprises authenticating or encrypting by IPSec
the request for registration and/or reply.

35

15. (Previously presented) The method of claim 4 wherein the method further comprises establishing the key distribution for the secure connections by establishing an IKE protocol translation table, and using the translation table to modify
5 IP addresses and cookie values of IKE packets in the intermediate computer.

16. (Previously presented) The method of claim 15 wherein the method further comprises establishing the key exchange
10 distribution by:
generating an initiator cookie and sending a zero responder cookie to the second computer,
generating a responder cookie in the second computer,
establishing a mapping between IP addresses and IKE cookie
15 values in the intermediate computer, and
using the translation table to modify IKE packets in flight by modifying the external IP addresses and possibly IKE cookies of the IKE packets.

20 17. (Previously presented) The method of claim 15 wherein the method further comprises modifying a modified IKE protocol between the first computer and the intermediate computer by transmitting the IKE keys from the first computer to the intermediate computer in order to decrypt and modify IKE
25 packets.

18. (Previously presented) The method of claim 15 wherein the method further comprises carrying out in a modified IKE protocol between the first computer and the intermediate
30 computer the modification of the IKE packets by the first computer with the intermediate computer requesting such modifications.

19. (Previously presented) The method of claim 17 wherein the
35 method further comprises defining the address so that the

first computer is identified for the second computer by the intermediate computer by means of an IP address taken from a pool of user IP addresses when forming the translation table.

5 20. (Previously presented) The method of claim 1 wherein the method further comprises sending the secure message by using an IPSec transport mode.

10 21. (Previously presented) The method of claim 1 wherein the method further comprises sending the secure message by using an IPSec tunnel mode.

22. (Currently amending) A telecommunication network for secure forwarding of messages, comprising:
15 a first computer, a second computer and an intermediate computer,
means for directly negotiating and exchanging keys, according to a key exchange protocol, between the first computer and the second computer to establish a security association having a
20 source address of the first computer as a first end point and a destination address of the second computer as a second end point,
the first and the second computers having means for performing an IPSec processing,
25 the intermediate computer having translation means for using translation tables to perform IPSec and IKE translation and for changing a destination address of the intermediate computer of a secure message to a destination address of the second computer, and
30 the intermediate computer having means for forwarding the secure message received from the first computer to the second computer in the security association.

35 23. (Previously presented) The telecommunication network of claim 22 wherein the translation table for IPSec translation

has IP addresses of the intermediate computer to be matched with IP addresses of the second computer.

5 24. (Previously presented) The telecommunication network of claim 22 wherein the translation tables for IKE translation consists of two partitions, one for the communication between the first computer and the intermediate computer and another for the communication between the intermediate computer and the second computer.

10

25. (Previously presented) The telecommunication network of claim 24 wherein both partitions of the mapping table for IKE translation contains translation fields for a source IP address, a destination IP address, initiator and responder cookies between respective computers.

15

26. (Previously presented) The telecommunication network of claim 22 wherein there is another translation table for IKE translation containing fields for matching a given user to a given computer.

20

27. (Currently amended) A telecommunication network for secure forwarding of messages, comprising:
a first computer,
25 a second computer,
an intermediate computer electronically connected to the first computer and the second computer,
means for directly negotiating and exchanging keys between the first computer and the second computer to establish a secure
30 connection having a source address of the first computer as a first end point and a destination address of the second computer as a second end point, and
the intermediate computer having means for performing translation between destination addresses and secure
35 identities for forwarding secure messages received from the

first computer to the second computer in the secure connection.

REMARKS/ARGUMENTS

5 Reconsideration of the application is respectfully requested. Claims 1-2, 4-27 were rejected under Section 102 as being anticipated by Kunzinger. This rejection is respectfully traversed. No new matter has been added to the application.

10 Claim 1 has been amended to clarify that the first computer and second computer negotiate and exchanges key with one another to establish the secure connection. Support may be found in, for example, paragraphs 0075-0093 of the corresponding published US 2006/0173968. The secure
15 connection extending between the first computer and the second computer is shown in Fig. 1.

 Kunzinger merely teaches the use of cascaded tunnels (see abstract) in which, as shown in Fig. 4, a first tunnel extends between the first computer (client) and the
20 intermediate computer (boundary device) and a second tunnel extends between the intermediate computer and a second computer (server). The first tunnel provides security through the Internet and the second tunnel provides security through an intranet (see paragraph 0051). Kunzinger explains in
25 paragraph 0047 that the "use of cascaded tunnels (as opposed to a single tunnel or SA extending from the client to the server) allows security protection to be tailored to the

requirements of a particular network segment.” He also explains that the security gateway serves as a point of entry into the intranet (paragraph 0050) and that the security gateway 420 retains the ability to provide of the type of services available in the environment of Fig. 3. These services include access control and network address translation that require content inspection. In other words, the gateway protects the intranet from undesirable communication from the open Internet by inspecting the content of incoming packets before the packets enter into the intranet. In paragraph 0013, Kunzinger explains that the security associations are negotiated between the tunnel endpoints i.e. between the endpoints of tunnel 1 and the endpoints of tunnel 2. This means the client 405 negotiates with the gateway 420 to establish tunnel 1 (but not with the server 440). Similarly, the gateway 420 negotiates with the server 440 to establish tunnel 2.

It is submitted that Kunzinger and the other cited references fail to teach or suggest the step of the first and second computers exchanging keys with one another to establish the secure connection that has a source address of the first computer and a destination address of the second computer.

As indicated above, Kunzinger clearly teaches the advantage of using cascade tunnels which provide the tailoring features (see paragraph 0047) “as opposed to a single tunnel or SA extending from the client to the server.” Also, in

paragraphs 0012-0014 Kunzinger explains that each tunnel is a separate connection. In other words, there is no single secure connection that extends between the client 405 and the server 440 in Kunzinger's system. Also, in paragraphs 0067-
5 0068 Kunzinger explains if there is no existing cascaded tunnel available between the gateway 420 and the server 440 then a pair of IKE and IPSsec security associations will be established to provide the next tunnel (which again indicates that there are two separate tunnels and not a single tunnel).

10 In view thereof, Applicants even submit that Kunzinger teaches away from the first computer and the second computer negotiating and exchanging keys with one another to establish a secure connection between the first computer and the second computer. More particularly, Kunzinger fails to
15 teach or suggest the direct exchange of keys between the client 405 and the server 440. The key exchanges described in Kunzinger are only between the client (first computer) and the gateway (intermediate computer) to establish tunnel 1 and then between the gateway (intermediate computer) and the server
20 (second computer) to establish tunnel 2. In other words, in Kunzinger the client 405 first exchanges keys with the gateway 420 (intermediate computer) and thereafter the gateway 420, in turn, exchanges keys with the server 440 (the second computer). There is thus no direct exchange between the
25 client 405 and the server 440 to establish a tunnel between the client 405 to the server 440. There is therefore no key

exchange between the client and the server either.

On page 4, line 3 of the Office action, the Examiner states that "the key is the id." Applicants are puzzled over this statement. The exchange of keys is a basic concept in
5 all kinds of cryptography to encrypt and decrypt information. In the present invention, the unique identity is in the secure message and it would not make sense to send the key together with the secure message itself. This would make the encryption meaningless since any recipient would be able to
10 decrypt the secure message with the key. It is like locking a door but leaving the key in the door. It is therefore submitted that the key in Kunzinger does not correspond to the unique identity of the present invention.

It is submitted that Kunzinger would require
15 extensive modifications that are not taught or suggested to arrive at the features of the present invention. Applicants fail to see why a person of ordinary skill in the art would look to Kunzinger to learn about the single secure connection and the key exchange between the first and second computer
20 when Kunzinger completely fails to teach or suggest these steps.

In view thereof, claim 1 is submitted to be allowable.

Claims 2, 4-21 are submitted to be allowable because
25 they depend upon the allowable base claim 1 and because each claim includes limitations that are not taught or suggested in

the cited references.

Independent claims 22 and 27 are submitted to be allowable for reasons similar to the reasons put forth for the allowability of the amended claim 1. More particularly, it is submitted that none of the cited references teaches means for directly exchanging and negotiating keys between the first and second computer. As explained above, an important function of Kunzinger's gateways is to function as a port of entry into an intranet and to inspect the content of incoming secure packets which requires decryption of the packets before forwarding them to the server (the second computer) in the intranet. There should therefore be no direct communication between the client and the server since the role of the gateway is to inspect the incoming packets before they enter the intranet.

In view thereof, claims 22 and 27 are submitted to be allowable.

Claims 23-26 are submitted to be allowable because they depend upon the allowable base claim 22 and because each claim includes limitations that are not taught or suggested in the cited references.

Claim 3 was rejected under Section 103 as being obvious over Kunzinger in view of Patel. This rejection is respectfully traversed.

Claim 3 is submitted to be allowable because it depends upon the allowable base claim 1 and because the claim includes limitations that are not taught or suggested in the

RF Attorney Docket No. 290.1078USN 11/16/10 - 14 -
cited references.

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

5

Respectfully submitted,

FASTH LAW OFFICES

10

/rfasth/

Rolf Fasth

Registration No. 36,999

15

ATTORNEY DOCKET NO. 290.1078USN

20

FASTH LAW OFFICES
26 Pinecrest Plaza, Suite 2
Southern Pines, NC 28387-4301

Telephone: (910) 687-0001

Facsimile: (910) 295-2152

25

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
Attorney Ref. No. 290.1078APP

In re application of
 Sami Vaarala, Antti Nuopponen
 Serial No. 10/500,930

Art Unit 2458
 Confirmation No. 1571

Filed: 19 October 2005

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

Examiner: Afshawn M. Towfighi

Date: 17 November 2010

CERTIFICATE OF MAILING

I HEREBY CERTIFY THAT THIS PAPER AND THE DOCUMENTS
 REFERRED TO AS BEING ATTACHED OR ENCLOSED HERewith
 ARE BEING SUBMITTED ELECTRONICALLY TO THE UNITED
 STATES PATENT AND TRADEMARK OFFICE ON **17 November**
2010.

/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) Response to Office Action dated 26 August 2010.
- (X) The Commissioner is hereby authorized to charge any 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
 26 Pinecrest Plaza, Suite 2
 Southern Pines, North Carolina 28387-4301

Telephone: 910-687-0001
 Facsimile: 910-295-2152

Attorney Ref. No. 290.1078APP

Electronic Acknowledgement Receipt

EFS ID:	8852645
Application Number:	10500930
International Application Number:	
Confirmation Number:	1571
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:	290.1078USN
Receipt Date:	17-NOV-2010
Filing Date:	19-OCT-2005
Time Stamp:	06:52:28
Application Type:	U.S. National Stage under 35 USC 371

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	Amendment/Argument after Notice of Appeal	AMD.PDF	33790 <small>ea188f11c334e1e685ef2864ecd34aa8c4da def8</small>	no	15

Warnings:

Information:

2	Miscellaneous Incoming Letter	TRX.PDF	18199 5aaa43a041f808b35a4fcb0f9608968692ae3d6b	no	1
---	-------------------------------	---------	---	----	---

Warnings:

Information:

Total Files Size (in bytes):	51989
-------------------------------------	-------

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.

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 10/500,930	Filing Date 10/19/2005	<input type="checkbox"/> To be Mailed
---	---	----------------------------------	---------------------------------------

APPLICATION AS FILED – PART I			OTHER THAN SMALL ENTITY				
	(Column 1)	(Column 2)	SMALL ENTITY <input checked="" type="checkbox"/>	OR			
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	OR	RATE (\$)	FEE (\$)
<input type="checkbox"/> BASIC FEE <small>(37 CFR 1.16(a), (b), or (c))</small>	N/A	N/A	N/A			N/A	
<input type="checkbox"/> SEARCH FEE <small>(37 CFR 1.16(k), (l), or (m))</small>	N/A	N/A	N/A			N/A	
<input type="checkbox"/> EXAMINATION FEE <small>(37 CFR 1.16(o), (p), or (q))</small>	N/A	N/A	N/A			N/A	
TOTAL CLAIMS <small>(37 CFR 1.16(i))</small>	minus 20 =	*	X \$ =		OR	X \$ =	
INDEPENDENT CLAIMS <small>(37 CFR 1.16(h))</small>	minus 3 =	*	X \$ =			X \$ =	
<input type="checkbox"/> APPLICATION SIZE FEE <small>(37 CFR 1.16(s))</small>	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT <small>(37 CFR 1.16(j))</small>							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II					OTHER THAN SMALL ENTITY				
	(Column 1)	(Column 2)	(Column 3)		SMALL ENTITY	OR			
AMENDMENT	11/17/2010	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)
	Total <small>(37 CFR 1.16(i))</small>	* 27	Minus ** 27	= 0	X \$26 =	0	OR	X \$ =	
	Independent <small>(37 CFR 1.16(h))</small>	* 3	Minus *** 3	= 0	X \$110 =	0	OR	X \$ =	
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>								
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>						OR		
					TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

	(Column 1)	(Column 2)	(Column 3)		SMALL ENTITY	OR			
AMENDMENT	Total <small>(37 CFR 1.16(i))</small>	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)
	*	Minus	**	=	X \$ =		OR	X \$ =	
	Independent <small>(37 CFR 1.16(h))</small>	*	Minus	***	X \$ =		OR	X \$ =	
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>								
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>						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".

Legal Instrument Examiner:
 /TRACEY M. YOUNG/

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

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

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



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.
10/500,930	10/19/2005	Sami Vaarala	290.1078USN	1571
33369	7590	08/26/2010	EXAMINER	
FASTH LAW OFFICES (ROLF FASTH) 26 PINECREST PLAZA, SUITE 2 SOUTHERN PINES, NC 28387-4301			TOWFIGHI, AFSHAWN M	
			ART UNIT	PAPER NUMBER
			2458	
			NOTIFICATION DATE	DELIVERY MODE
			08/26/2010	ELECTRONIC

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

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

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

sloan.smith@fasthlaw.com
nan_russell@fasthlaw.com

Office Action Summary	Application No. 10/500,930	Applicant(s) VAARALA ET AL.	
	Examiner AFSHAWN TOWFIGHI	Art Unit 2458	

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

Period for Reply

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

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

Status

- 1) Responsive to communication(s) filed on 22 June 2010.
- 2a) This action is **FINAL**.
- 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-27 is/are pending in the application.
 - 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-27 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 - Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 - Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 - 1. Certified copies of the priority documents have been received.
 - 2. Certified copies of the priority documents have been received in Application No. _____.
 - 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

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

Attachment(s)

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

DETAILED ACTION

1. Claims 1-27 are pending.

Response to Arguments

2. In view of the Appeal Brief filed on 6/22/2010, PROSECUTION IS HEREBY REOPENED. New grounds of rejection are set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below.

Response to Arguments

3. Applicant's arguments with respect to claims 1-27 have been considered but are moot in view of the new ground(s) of rejection.

Art Unit: 2458

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1, 2, 4-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Kunzinger (Pub No: 2002/0091921).

As to claim 1, Kunzinger teaches a method for secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network (Kunzinger, [0047] L1-13, end to end data sending via an intermediate gateway using secure tunnels), comprising: the first computer and the second computer negotiating and exchanging keys according to a key exchange protocol to establish a secure connection between the first computer and the second computer via the intermediate computer (Kunzinger, [0067] and [0068], the client establishes a secure connection to the endpoint via cascaded tunnels and the gateway using the IPSec and internet key exchange policy), the secure connection having a source address of the first computer as a first end point and a destination address of the second computer as a second end point of the secure connection (Kunzinger, [0013] , the IPSec packet has an inner header with the source and destination addresses), in

Art Unit: 2458

the first computer, forming a secure message by giving the secure message a first unique identity and a first destination address to the intermediate computer, (Kunzinger, [0068] L1-3, the key is the id and [0013] the outer header has the address of the endpoint of the tunnel, i.e. gateway), sending the secure message from the first computer to the intermediate computer, the intermediate computer receiving the secure message (Kunzinger, [0068] L1-3, the message is sent from the client and received by the gateway) and performing a translation by using the first unique identity to find a second destination address to the second computer, the intermediate computer substituting the first destination address with the second destination address to the second computer, the intermediate computer substituting the first unique identity with a second unique identity of the secure connection without establishing a new secure connection and without involving the second computer (Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel and the data is then forwarded/send the over the second tunnel and [0013] the new packet has the address of the second computer), and the intermediate computer forwarding the secure message with the second destination address and the second unique identity to the second computer in the secure connection (Kunzinger, [0074] forwarding the IPSec datagram and [0013] and [0068] the id and address are in the packet of data).

As to claim 2, Kunzinger teaches wherein the method further comprises forming the secure message by using an IPSec connection between the first computer and the second computer (Kunzinger, [0067], IPSec protection).

Art Unit: 2458

As to claim 4, Kunzinger teaches wherein the method further comprises manually performing a preceding distribution of keys to components for forming the IPsec connection (Kunzinger, [0067], IKE is used to for the IPsec connection).

As to claim 5, Kunzinger teaches wherein the method further comprises performing a preceding distribution of keys for forming the IPsec connection by an automated key exchange protocol (Kunzinger, [0067], IKE is used to for the IPsec connection).

As to claim 6, Kunzinger teaches wherein the method further comprises performing the automated key exchange protocol used for the preceding distribution of keys for forming the IP Sec connection by means of a modified IKE key exchange protocol between the first computer and the intermediate computer (Kunzinger, [0067], using phase2 IKE exchange between the client and gateway, this is a modified protocol because the table at the gateway modifies the IKE packets and inserts a new address automatically) and by means of a standard IKE key exchange protocol between the intermediate computer and the second computer (Kunzinger, [0069] using IKE between gateway and server).

As to claim 7, Kunzinger teaches wherein the method further comprises sending the message that is sent from the first computer as a packet that contains message data, an inner IP header containing the actual sender and receiver addresses, an outer IP header containing the addresses of the first computer and the intermediate computer, the unique identity (Kunzinger, [0013], inner and outer headers and negotiated security association).

Art Unit: 2458

As to claim 8, Kunzinger teaches wherein the method further comprises the IPSec connection being one or more security associations (SA) and the unique identity being one or more SPI values(Kunzinger, [0067], setting up the IPSec SA and the values are SPI values).

As to claim 9, Kunzinger teaches wherein the method further comprises performing the matching by using a translation table stored at the intermediate computer (Kunzinger, [0066], the databases are the translation tables).

As to claim 10, Kunzinger teaches wherein the method further comprises changing both the address and the SPI-value by the intermediate computer (Kunzinger, [0074], the address is changed to point to the tunnel and the ID(SPI) is changed, the SPI is the ID that is exchanged for indexing).

As to claim 11, Kunzinger teaches wherein the method further comprises the first computer being a mobile terminal (Kunzinger, [0038], the workstations communicate over a wireless cellular network) so that the mobility is enabled by modifying the translation table at the intermediate computer (Kunzinger, [0067] L13-17, the SAD on the gateway is modified with IKE value).

As to claim 12, Kunzinger teaches wherein the method further comprises performing the modification of the translation tables by sending a request for registration of the new address from the first computer to the intermediate computer (Kunzinger, [0062], the client is the IKE initiator with negotiations with the gateway).

Art Unit: 2458

As to claim 13, Kunzinger teaches wherein the method further comprises sending a reply to the request for registration from the intermediate computer to the first computer (Kunzinger, [0063], the gateway is the IKE responder to the client in the IKE negotiations).

As to claim 14, Kunzinger teaches wherein the method further comprises authenticating or encrypting by IPsec the request for registration and/or reply (Kunzinger, [0067], authenticating IPsec).

As to claim 15, Kunzinger teaches wherein the method further comprises establishing the key distribution for the secure connections by establishing an IKE protocol translation table, and using the translation table to modify IP addresses and cookie values of IKE packets in the intermediate computer (Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel and [0066]-[0067], the IKE protocol addresses, etc are stored in the SAD tables).

As to claim 16, Kunzinger teaches wherein the method further comprises establishing the key exchange distribution by: generating an initiator cookie and sending a zero responder cookie to the second computer, generating a responder cookie in the second computer (Kunzinger, [0064] [0065] and [0067], the gateway is the initiator and the server is the responder in the IKE negotiations. [0069] shows an example of IKE negotiations the IDCi and IDCr values are set), establishing a mapping between IP addresses and IKE cookie values in the intermediate computer, and using the translation table to modify IKE packets in flight by modifying the external IP addresses

Art Unit: 2458

and possibly IKE cookies of the IKE packets (Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel and [0066]-[0067], the IKE protocol addresses, etc are stored in the SAD tables).

As to claim 17, Kunzinger teaches wherein the method further comprises modifying a modified IKE protocol between the first computer and the intermediate computer by transmitting the IKE keys from the first computer to the intermediate computer in order to decrypt and modify IKE packets (Kunzinger, [0067], using phase2 IKE exchange between the client and gateway, this is a modified protocol because the table at the gateway modifies the IKE packets and inserts a new address automatically).

As to claim 18, Kunzinger teaches wherein the method further comprises carrying out in a modified IKE protocol between the first computer and the intermediate computer the modification of the IKE packets by the first computer with the intermediate computer requesting such modifications (Kunzinger, [0067], using phase2 IKE exchange between the client and gateway, this is a modified protocol because the table at the gateway modifies the IKE packets and inserts a new address automatically).

As to claim 19, Kunzinger teaches wherein the method further comprises defining the address so that the first computer is identified for the second computer by the intermediate computer by means of an IP address taken from a pool of user IP addresses when forming the translation table (Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel and the data is then

Art Unit: 2458

forwarded/send the over the second tunnel and [0013] the new packet has the address of the second computer).

As to claim 20, Kunzinger teaches wherein the method further comprises sending the secure message by using an IPSec transport mode (Kunzinger, [0075] L12-15, IPSec operates in transport mode).

As to claim 21, Kunzinger teaches wherein the method further comprises sending the secure message by using an IPSec tunnel mode (Kunzinger, [0075] L12-15, IPSec operates in tunnel mode).

As to claim 22, Kunzinger teaches a telecommunication network for secure forwarding of messages (Kunzinger, [0047] L1-13, end to end data sending via an intermediate gateway using secure tunnels), comprising: a first computer, a second computer and an intermediate computer, means for negotiating and exchanging keys, according to a key exchange protocol, between the first computer and the second computer to establish a security association having a source address of the first computer as a first end point and a destination address of the second computer as a second end point (Kunzinger, [0067] and [0068], the client establishes a secure connection to the endpoint via cascaded tunnels and the gateway using the IPSec and internet key exchange policy), the first and the second computers having means for performing an IPSec processing, the intermediate computer having translation means for using translation tables to perform IPSec and IKE translation and for changing a destination address of the intermediate computer of a secure message to a destination address of the second

Art Unit: 2458

computer (Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel (IKE/IPSec) and the data is then forwarded/send the over the second tunnel and [0013] the new packet has the address of the second computer), and the intermediate computer having means for forwarding the secure message received from the first computer to the second computer in the security association (Kunzinger, [0074] forwarding the IPSec datagram and [0013] and [0068] the id and address are in the packet of data) .

As to claim 23, Kunzinger teaches wherein the translation table for IPSec translation has IP addresses of the intermediate computer to be matched with IP addresses of the second computer (Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel and the data is then forwarded/send the over the second tunnel and [0013] the new packet has the address of the second computer).

As to claim 24, Kunzinger teaches wherein the translation tables for IKE translation consists of two partitions, one for the communication between the first computer and the intermediate computer and another for the communication between the intermediate computer and the second computer (Kunzinger, [0066] L1-10, each set of interfaces has its own databases).

As to claim 25, Kunzinger teaches wherein both partitions of the mapping table for IKE translation contains translation fields for a source IP address, a destination IP address (Kunzinger, [0067] IKE tables have the addresses for endpoint association), initiator and responder cookies between respective computers (Kunzinger, [0067], IDci and IDcr values).

Art Unit: 2458

As to claim 26, Kunzinger teaches wherein there is another translation table for IKE translation containing fields for matching a given user to a given computer (Kunzinger, [0066], association for a user to an endpoint).

As to claim 27, Kunzinger teaches a telecommunication network for secure forwarding of messages (Kunzinger, [0047] L1-13, end to end data sending via an intermediate gateway using secure tunnels), comprising: a first computer, a second computer, an intermediate computer electronically connected to the first computer and the second computer, means for negotiating and exchanging keys between the first computer and the second computer to establish a secure connection having a source address of the first computer as a first end point and a destination address of the second computer as a second end point (Kunzinger, [0067] and [0068], the client establishes a secure connection to the endpoint via cascaded tunnels and the gateway using the IPSec and internet key exchange policy), and the intermediate computer having means for performing translation between destination addresses and secure identities (Kunzinger [0074] the gateway uses tables and id to translate the packet into a corresponding tunnel and the data is then forwarded/send the over the second tunnel and [0013] the new packet has the address of the second computer) for forwarding secure messages received from the first computer to the second computer in the secure connection (Kunzinger, [0074] forwarding the IPSec datagram and [0013] and [0068] the id and address are in the packet of data).

Art Unit: 2458

Claim Rejections - 35 USC § 103

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

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

7. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kunzinger as applied to claim 1 above, and further in view of Patel (Pub No: 2002/0004900).

As to claim 3, Kunzinger teaches the limitations of claim 1. Kunzinger does not teach wherein the method further comprises performing a secure forwarding of the message by making use of SSL or TLS protocols. Patel teaches wherein the method further comprises performing a secure forwarding of the message by making use of SSL or TLS protocols (Patel, [0037] L18-21, SSL for secure connection). It would have been obvious to one of ordinary skill in the art at the time of invention to combine the teachings of Kunzinger with Patel to use SSL for the secure connection because Patel teaches that SSL is a well know protocol for a secure connection that can be used like IPsec.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to AFSHAWN TOWFIGHI whose telephone number is

Art Unit: 2458

(571)270-7296. The examiner can normally be reached on Monday - Friday 8:00 A.M. to 5:00 P.M..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph E. Avellino can be reached on (571)272-3905. 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.

/Joseph E. Avellino/
Supervisory Patent Examiner, Art Unit 2458

Notice of References Cited	Application/Control No. 10/500,930	Applicant(s)/Patent Under Reexamination VAARALA ET AL.	
	Examiner AFSHAWN TOWFIGHI	Art Unit 2458	Page 1 of 1

U.S. PATENT DOCUMENTS

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A US-2002/0091921	07-2002	Kunzinger, Charles A.	713/153
*	B US-2002/0004900	01-2002	PATEL, BAIJU V.	713/155
	C US-			
	D US-			
	E US-			
	F US-			
	G US-			
	H US-			
	I US-			
	J US-			
	K US-			
	L US-			
	M US-			


FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)				
	U				
	V				
	W				
	X				

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

Index of Claims 	Application/Control No. 10500930	Applicant(s)/Patent Under Reexamination VAARALA ET AL.
	Examiner Jeffrey Seto	Art Unit 2458

✓	Rejected
=	Allowed


-	Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

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

CLAIM		DATE									
Final	Original	10/28/2008	05/28/2009	09/08/2009	03/15/2010	08/21/2010					
	1	✓	✓	✓	✓	✓					
	2	✓	✓	✓	✓	✓					
	3	✓	✓	✓	✓	✓					
	4	✓	✓	✓	✓	✓					
	5	✓	✓	✓	✓	✓					
	6	✓	✓	✓	✓	✓					
	7	✓	✓	✓	✓	✓					
	8	✓	✓	✓	✓	✓					
	9	✓	✓	✓	✓	✓					
	10	✓	✓	✓	✓	✓					
	11	✓	✓	✓	✓	✓					
	12	✓	✓	✓	✓	✓					
	13	✓	✓	✓	✓	✓					
	14	✓	✓	✓	✓	✓					
	15	✓	✓	✓	✓	✓					
	16	✓	✓	✓	✓	✓					
	17	✓	✓	✓	✓	✓					
	18	✓	✓	✓	✓	✓					
	19	✓	✓	✓	✓	✓					
	20	✓	✓	✓	✓	✓					
	21	✓	✓	✓	✓	✓					
	22	✓	✓	✓	✓	✓					
	23	✓	✓	✓	✓	✓					
	24	✓	✓	✓	✓	✓					
	25	✓	✓	✓	✓	✓					
	26	✓	✓	✓	✓	✓					
	27	✓	✓	✓	✓	✓					

Search Notes 	Application/Control No. 10500930	Applicant(s)/Patent Under Reexamination VAARALA ET AL.
	Examiner Jeffrey Seto	Art Unit 2458

SEARCHED			
Class	Subclass	Date	Examiner
709	236, 229, 245	11-5-2008	JS

SEARCH NOTES		
Search Notes	Date	Examiner
Limited classification of 709/229, 245	11-5-2008	JS
Inventor search	11-5-2008	JS
Text search of EAST (US Pat, US PG Pub, JPO, EPO, Derwent)	11-5-2008	JS
Updated Text search of EAST (see attached history)	5-28-2009	JS
Updated text search of EAST (see attached history)	9-8-09	JS
EAST search with previous examiner's classes and focus on new limitations	3/15/2010	AT
Conf with B.Bruckart and J.Avellino - Reopen and search IPSec/tunneling/gateway/proxy	8/21/2010	AT
Updated EAST search - see attached	8/21/2010	AT

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

--	--

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

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	2210	ipsec same (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2010/08/23 11:02
L2	1902	ipsec with(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2010/08/23 11:02
L3	1902	ipsec with (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2010/08/23 11:02
L4	1468	ipsec near5(ssl or tls)	US-PGPUB; USPAT	OR	OFF	2010/08/23 11:03
L5	1468	ipsec near5 (ssl or tls)	US-PGPUB; USPAT	OR	OFF	2010/08/23 11:03
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

EAST Search History (Interference)

< This search history is empty >

8/ 23/ 2010 11:28:07 AM

C:\ Documents and Settings\ atowfighi\ My Documents\ EAST\ Workspaces\ jeff930.wsp

Attorney Matter No. 290.1078APP

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF APPEALS AND INTERFERENCES

In re application of: Sami Vaarala et al

Serial No. 10/500,930)
)
) APPEAL BRIEF
)
Filed: 19 October 2005)
)
For: METHOD AND SYSTEM FOR)
SENDING A MESSAGE THROUGH)
A SECURE CONNECTION)
) Art Unit 2458
)
) Examiner Afshawn M. Towfighi
)
)
)
)
Date: 22 June, 2010).

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

APPELLANT'S BRIEF ON APPEAL

Real Party in Interest

The real party in interest is MPH Technologies Oy,
Tekniikantie 14, FIN-02150 Espoo, Finland, the recorded assignee
of the above-captioned patent application.

Related Appeals and Interferences

No related appeals or interferences of this application
are known to the Appellant, the Appellant's legal representative
or assignee which will directly affect or be directly affected by
or have a bearing on the Board's decision in the pending appeal.

Status of the Claims

Rejection 1

Claims 1-5, 7-10, 22-24 and 26-27 stand rejected in the Office action dated 23 March 2010 as being anticipated by US Patent Application No. 2001/0047487 to Linnakangas et al.

Rejection 2

Claims 6, 11-14, 20-21 stand rejected in the Office action dated 23 March 2010 as being obvious over Linnakangas in view of Applicant's Admitted Prior Art (AAPA).

Rejection 3

Claims 15-19 and 25 stand rejected in the Office action dated 23 March 2010 as being obvious over Linnakangas in view of Sandhu.

The application has been rejected at least twice. A copy of the claims is reproduced as Claims Appendix hereto. The rejections of claims 1-27 are appealed.

Status of Amendments

All Amendments have been entered.

Summary of Claimed Subject Matter

The application has three independent claims (i.e. claims 1, 22 and 27). Independent claim 1 refers to a method for secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network (see abstract and paragraph 0039 of US 2006/0173968). The first computer and the second computer negotiate and exchange keys according to a key exchange protocol to establish a secure connection (such as a security association (SA)) between the first computer and the second computer via the intermediate computer (see paragraphs 0039, 0070, 0104-0113). The secure connection has a source address of the first computer as a first end point and a destination address of the second computer as a second end point of the secure connection (see Figs. 1-2, paragraphs 0010, 0013-0014 and 0021). A secure message is formed in the first computer by giving the secure message a first unique identity and a first destination address to the intermediate computer (see abstract, paragraphs 0039, 0041, 0043-0044). The secure message is sent from the first computer to the

intermediate computer (see abstract). The intermediate computer receives the secure message and performs a translation by using the first unique identity to find a second destination address of the second computer (see paragraphs 0023, 0041, 0045-0048, 0053-0060, 0072-0095). The intermediate computer substitutes the first destination address with the second destination address to the second computer (see abstract, original claim 1, paragraphs 0039 and 0086). The intermediate computer substitutes the first unique identity with a second unique identity of the same secure connection without establishing a new secure connection between the intermediate computer and the second computer and without involving the second computer (see abstract, paragraphs 0039, 0047 and 0086). The intermediate computer then forwards the secure message with the second destination address and the second unique identity to the second computer in the same secure connection (see abstract, Figs. 1-2, paragraphs 0039, 0041, 0045-0048, 0052-0061, 0070-0076, 0083-0090, 0096-0118).

Claim 2 refers to the step of forming the secure message by using an IPSec connection between the first computer and the second computer (see original claim 2, paragraphs 0009, 0024-0033, 0043 and 0045).

Claim 3 refers to the step of performing a secure forwarding of the message by making use of SSL or TLS protocols (see original claim 3).

Claim 4 refers to the step of manually performing a preceding distribution of keys to components for forming the IPsec connection (see original claim 4).

Claim 5 refers to the step of performing a preceding distribution of keys for forming the IPsec connection by an automated key exchange protocol (see original claim 5).

Claim 6 refers to the step of performing the automated key exchange protocol used for the preceding distribution of keys for forming the IPsec connection by means of a modified IKE key exchange protocol between the first computer and the intermediate computer and by means of a standard IKE key exchange protocol between the intermediate computer and the second computer (see original claim 6 and paragraphs 0018, 0024 and 0043-0062).

Claim 7 refers to the step of sending the message that is sent from the first computer as a packet that contains message data, an inner IP header containing the actual sender and receiver addresses, an outer IP header containing the addresses of the first computer and the intermediate computer, the unique identity (see original claim 7, paragraphs 0041-0062, 0082-0091).

Claim 8 refers to the IPsec connection being one or more security associations (SA) and the unique identity being one or more SPI values (see original claim 8).

Claim 9 refers to the step of performing the matching by using a translation table stored at the intermediate computer

(see original claim 9 and paragraphs 0041-0048, 0086, 0090, 0149-0150 and 0214-0216).

Claim 10 refers to the step of changing both the address and the SPI-value by the intermediate computer (see original claim 10 and paragraphs 0043-0046).

Claim 11 refers to the first computer being a mobile terminal so that the mobility is enabled by modifying the translation table at the intermediate computer (see original claim 11 and paragraphs 0020-0033, 0079-0085).

Claim 12 refers to the step of performing the modification of the translation tables by sending a request for registration of the new address from the first computer to the intermediate computer (see original claim 12).

Claim 13 refers to the step of sending a reply to the request for registration from the intermediate computer to the first computer (see original claim 13).

Claim 14 refers to the step of authenticating or encrypting by IPSec the request for registration and/or reply (see original claim 14 and paragraphs 0051, 0073 and 0081).

Claim 15 refers to the step of establishing the key distribution for the secure connections by establishing an IKE protocol translation table, and using the translation table to modify IP addresses and cookie values of IKE packets in the intermediate computer (see original claim 15 and paragraphs 0039-

0062 and 0111-0142).

Claim 16 refers to the step of establishing the key exchange distribution by generating an initiator cookie and sending a zero responder cookie to the second computer, generating a responder cookie in the second computer, establishing a mapping between IP addresses and IKE cookie values in the intermediate computer, and using the translation table to modify IKE packets in flight by modifying the external IP addresses and possibly IKE cookies of the IKE packets (see original claim 16 and paragraphs 0039-0062).

Claim 17 refers to the step of modifying a modified IKE protocol between the first computer and the intermediate computer by transmitting the IKE keys from the first computer to the intermediate computer in order to decrypt and modify IKE packets (see original claim 17 and paragraphs 0039-0062).

Claim 18 refers to the step of carrying out in a modified IKE protocol between the first computer and the intermediate computer the modification of the IKE packets by the first computer with the intermediate computer requesting such modifications (see original claim 18 and paragraphs 0039-0062).

Claim 19 refers to the step of defining the address so that the first computer is identified for the second computer by the intermediate computer by means of an IP address taken from a pool of user IP addresses when forming the translation table (see

original claim 19).

Claim 20 refers to the step of sending the secure message by using an IPSec transport mode (see original claim 20).

Claim 21 refers to the step of sending the secure message by using an IPSec tunnel mode (see original claim 21).

Independent claim 22 refers to a telecommunication network for secure forwarding of messages that has a first computer, a second computer and an intermediate computer (see abstract and paragraph 0039). The network has means for negotiating and exchanging keys, according to a key exchange protocol, between the first computer and the second computer to establish a security association (SA) that has a source address of the first computer as a first end point and a destination address of the second computer as a second end point (see Figs. 1-2, paragraphs 0010, 0013-0014, 0021, 0039-0062, 0070 and 0104-0113). The first and the second computers have means for performing IPSec processing (see paragraphs 0009, 0024-0033, 0043-0045 and 0054). The intermediate computer has translation means for using translation tables to perform IPSec and IKE translation and for changing a destination address of the intermediate computer of a secure message to a destination address of the second computer (see paragraphs 0020-0033, 0043-0062 and 0079-0085). Furthermore, the intermediate computer has means for forwarding the secure message received from the first

computer to the second computer in the same security association (see paragraph 0039).

Claim 23 refers to the translation table for IPsec translation has IP addresses of the intermediate computer to be matched with IP addresses of the second computer (see original claim 23 and paragraphs 0046-0062).

Claim 24 refers to the translation tables for IKE translation consists of two partitions, one for the communication between the first computer and the intermediate computer and another for the communication between the intermediate computer and the second computer (see original claim 24 and paragraphs 0046-0062).

Claim 25 refers to both partitions of the mapping table for IKE translation contains translation fields for a source IP address, a destination IP address, initiator and responder cookies between respective computers (see original claim 25 and paragraphs 0049, 0054 and 0058).

Claim 26 refers to another translation table for IKE translation containing fields for matching a given user to a given computer (see original claim 26 and paragraphs 0041-0048, 0086, 0090, 0149-0150 and 0214-0216).

Independent claim 27 refers to a telecommunication network for secure forwarding of messages that has a first computer, a second computer and an intermediate computer

electronically connected to the first computer and the second computer (see abstract and paragraphs 0039. The network has means for negotiating and exchanging keys between the first computer and the second computer to establish a secure connection therebetween that has a source address of the first computer as a first end point and a destination address of the second computer as a second end point (see paragraphs 0039, 0041-0062, 0070 and 0104-0113). The intermediate computer has means for performing translation between destination addresses and secure identities for forwarding secure messages received from the first computer to the second computer in the same secure connection (see paragraphs 0023, 0041, 0045-0048, 0053-0060 and 0072-0095).

In summary, one problem with standard/conventional IPSec mobile telephone systems is that the end points of the IPsec tunnel mode SA (security association) are fixed. There is no feature in conventional systems for changing any of the parameters of an SA other than by establishing a new SA that replaces the previous SA. More particularly, since mobile terminals move and thus change their network points frequently and since IPsec connections are bound to fixed addresses, the mobile terminals must establish new IPsec connections from each new point of attachment. This requires the exchange of keys etc. which is a cumbersome process that uses computation time. The method of the present invention provides a solution to this

problem.

Unique features of the present invention are the secure connection is established all the way between the first computer and the second computer via the intermediate computer by exchanging keys and that the intermediate computer 1) uses the first unique identity to find a second destination address to the second computer and 2) substitutes the first destination address with the second destination address in the same secure connection. Thus, there is no need to set up a new secure connection between the intermediate computer and the second computer. In this way, a secure message, sent from the first computer to the intermediate computer, may be modified by the intermediate computer so that it can be forwarded from the intermediate computer to the second computer in the same secure connection without requiring the cumbersome exchange of additional keys to set up a new secure connection between the intermediate computer and the second computer and without involving the second computer.

Grounds Of Rejection To Be Reviewed On Appeal

Whether the Examiner properly rejected claims 1-5, 7-10, 22-24 and 26-27 as being anticipated by Linnakangas and whether the Examiner properly rejected claims 6, 11-14 and 20-21

Attorney Docket No. 290.1078APP 6/22/10

Serial No. 10/500,930
Filed: 19 October 2005
Art Unit: 2458

of the application as being obvious of Linnakangas in view of Applicants' Admitted Prior Art (AAPA). Finally, whether the Examiner properly rejected claims 15-19 and 25 of the application as being obvious of Linnakangas in view of Sandhu.

Argument (Rejection 1) - 35 U.S.C. 102 (Anticipation)

The 102 rejection is submitted to be improper because the cited Linnakangas reference (US 2001/0047487) does not, among other things, teach or suggest the steps establishing a secure connection between the first and second computer that requires the first and second computer to exchange keys between each other when establishing the secure connection so that the secure connection has a source address of the first computer as a first end point and a destination address of the second computer as a second end point of the secure connection. Additionally, Linnakangas fails to teach the step of the intermediate computer substituting the first destination address and first unique identity of the secure message with a second destination address and a second unique identity of a second computer in the same secure connection without establishing a new secure connection and without involving the second computer so that the intermediate computer forwards the secure message to the second computer in the same secure connection. Linnakangas merely teaches the step of setting up of a secure connection (security association) between the intermediate computer (router 2) and the second computer (remote hosts 4) and the prior segment between the intermediate computer and the first computer (local hosts 5) is merely within the same local area network (LAN) so that the intermediate computer decrypts packets going into the local hosts

5 of the LAN and encrypts packets going out from the local hosts 5 of the LAN to the second computer. If the segment between the intermediate computer (router 2) and the first computer (local hosts 5) had been part of the same security association there would be no need to decrypt and encrypt messages going to and from the first computer (local hosts 5). The decryption/encryption procedure of Linnakangas' intermediate computer (router 2) is quite different from sending a secure message in a secure connection that extends all the way from the first computer (local hosts 5) to the second computer (remote hosts 4). The above features are submitted to be novel and not obvious in view of the cited references.

More particularly, Linnakangas describes the establishment of a security association (which is one type of a secure connection). When a security association is formed between two computers, keys are first exchanged between the two computers. This is done according to an Internet Key Exchange (IKE) protocol and the security association is defined by unique identity and addresses of the two computers between which the security association is formed. Despite numerous efforts to try to explain in Linnakangas there is no security association established between the local hosts 5 (first computer) and the router 2 (intermediate computer), the Examiner still maintains that there is also a security association created between the

router 2 and the local hosts 5. Appellants maintain that there is only a security association created between the router 2 (intermediate computer) and the remote hosts 4 (second computer). It is submitted that the security association established does not extend to the local hosts 5 (first computer).

The Examiner refers to paragraphs 4 and 5 of Linnakangas as teaching the establishment of the secure connection between the first computer and the second computer.

Appellants respectfully disagree. Paragraphs 4 and 5 describe the establishment of security associations (SAs) in general and not that a SA is established between the remote hosts 4 and local hosts 5 or between the intermediate computer 2 and the local hosts 5. It is submitted that paragraph 24 of Linnakangas clearly teaches that each remote host 4 must negotiate at least one pair of SAs with the router 2. Linnakangas fails to teach the remote hosts 4 negotiating and establishing a security association with the local hosts 5. More importantly, there is absolutely nothing in Linnakangas about the local hosts 5 (first computer) negotiating a security association with the remote hosts 4 (second computer) so that a security association extends all the way from one of the local hosts 5 to one of the remote hosts 4. Appellants assert that Linnakangas and the other cited references completely fail to teach or suggest the step of the local hosts 5 (first computer)

establishing secure connections with the remote hosts 4 (second computer). On the contrary, Linnakangas' local hosts 5 and the router 2 communicate, as indicated above, via a Local Area Network (LAN) 1. The SA thus only extends between the remote hosts 4 and the router 2 but not between the router 2 and the local hosts 5. To further support that there is no security association established between the router 2 and the local hosts 5, the router 2 decrypts, reads and unwraps any secure message received from the remote hosts 4 to be able to determine that the message is to be forwarded (most likely as plain text) to the local hosts 5. This forwarding is done without implementing IPsec. There is nothing about forming a secure message in the local hosts 5 or the local hosts 5 negotiating secure associations with the remote hosts 4. In other words, it is important to note that the negotiated secure connection merely extends between the router 2 and the remote hosts 4. On page 4 of the Office action, the Examiner refers to paragraph 8, lines 1-5 of Linnakangas as teaching that "the destination of the packets is the second computer." Firstly, the claim does not require that the "destination of the packets is the second computer." The claim requires that the secure connection has a source address of the first computer as a first end point and a destination address of the second computer as a second end point of the secure connection. As explained above, Linnakangas' SA

only extends between the intermediate computer (router 2) and the remote hosts (4) but excludes the segment between the router (2) and the local hosts (5). Secondly, the cited text segment in paragraph 8, lines 1-5 of Linnakangas merely refers to the IP forwarder as being the receiver (or "destination" as the Examiner calls it). It is important to realize that the IP forwarder is an inner destination within the router 2 itself and not the local hosts (5). Paragraph 31, lines 1-3 of Linnakangas supports this. The IP forwarder (IPFW) is shown in Fig. 2 that describes the internal architecture of the router 2 (see paragraph 21 of Linnakangas). In paragraph 24, lines 4-8, Linnakangas explains that "[b]y using IPsec to control communication between the router 2 and the remote hosts 4 (and hence between remote hosts 4 and local hosts 5), a Virtual Private Network (VPN) may be established" (emphasis added). It is respectfully submitted that this is different from establishing a secure connection that extends all the way from the local hosts 5 to the remote hosts 4 which requires the exchange of keys according to a key exchange protocol. Additionally, "controlling" communication across the route from local hosts 5 via router 2 all the way to the remote hosts 4 does not mean that there is a secure connection established also between router 2 and host 5. As explained above, the nodes involved in the negotiation and exchange of keys according to the key exchange protocol IKE determines the

boundaries of the secure connection. In Linnakangas, the exchange of keys is only between the router 2 and the remote hosts 4. In other words, Linnakangas merely mentions controlling the communication, not securing. It should be noted that the virtual private network in Linnakangas is not secured since it is not part of the security association between the router 2 and the remote hosts 4. There is not really as much need for a secure connection between the router 2 and the host 5 since the connection is within the same LAN.

Even if the communication between the router 2 and the local hosts 5 may be considered quite safe, it is still not part of the SA because the SA merely extends between the router 2 and the remote hosts 4. The fact that there is no SA between the router 2 and the local hosts 5 is supported on line 2 of paragraph 4 in Linnakangas that discusses encapsulation and decapsulation of IPSec packets. This means the segment between the router 2 and the local hosts 5 is not part of the security association that extends between the router 2 and the remote hosts 4. If this segment would have been part of the same security association then there would not make sense to encrypt and decrypt incoming and outgoing messages between the router 2 and the local hosts 5. Instead, the packets are opened and decrypted by adding an IPSec layer. This is quite different from address substitution in a secure connection that extends between

the first computer and the second computer as required by claim 1. In other words, when the router 2 receives a packet from the outside (such as from the remote hosts 4), the router 2 opens the packet (decapsulation) and sends it to the local host 5 in a decrypted form and when the router 2 receives a packet from within the network (such as from the local hosts 5) the router encrypts the packets by adding an IPsec layer and sends it into the security association (SA) such as to the remote hosts 4.

On page 5 of the Office action, the Examiner states that the router is able to perform IPsec and IKE translation and inherently includes a translation table. Appellants cannot see that Linnakangas teaches that the router 2 can perform IPsec/IKE translation as asserted by the Examiner. The Examiner also states that "address substitution is a standard part of IPsec processing and IKE translation." It should be noted that address substitution is not a standard part of IPsec. The Examiner refers to paragraphs 4 and 24 of Linnakangas as teaching that address substitution is standard.

In view of the above, it is submitted that claim 1 is not anticipated by Linnakangas and that the Section 102 rejection should be withdrawn.

Claims 2-5 and 7-10 are submitted to be allowable because they depend upon the allowable base claim 1 and because each claim includes limitations that are not taught or suggested

in the cited references.

Claim 22 is submitted to be allowable for reasons similar to the arguments put forth for the allowability of claim 1. As mentioned above, Linnakangas merely shows the establishment of a secure connection between the remote hosts 4 and the router 2 by negotiating security associations (SAs) between those two components. Appellants fail to see where Linnakangas teaches means for negotiating and exchanging keys, according to a key exchange protocol, between the local hosts 4 (first computer) and the remote hosts 5 (second computer) to establish a security association that has a source address of the local host 5 as a first end point and a destination address of the remote host 4 as a second end point, as required by claim 22. In contrast, Linnakangas merely teaches the negotiation of the security associations between the router 2 (intermediate computer) and the remote hosts 4 (second computer), as expressly shown in paragraph 0024 of the Linnakangas reference and as explained above.

It is submitted that Linnakangas fails to teach or suggest all the limitations of claim 22. Therefore, the anticipation rejection of claim 22 under § 102 is improper, and should be removed.

Claims 23-24 and 26 are submitted to be allowable because the claims depend either directly or indirectly upon the

allowable base claim 22 and because each claim includes limitations that are not taught or suggested in the cited references.

Similar to claim 22, claim 27 requires means for negotiating and exchanging keys between the first computer and the second computer to establish a secure connection having a source address of the first computer as a first end point and a destination address of the second computer as a second end point. For reasons similar to the reasons put forth for the allowability of claims 1 and 22, claim 27 is submitted to be allowable.

Argument (Rejection 2, Claims 6, 11-14, 20-21) - 35
U.S.C. 103 (Obviousness)

Claims 6, 11-14 and 20-21 are submitted to be allowable because the claims depend upon the allowable base claim 1 and because the claims include limitations that are not taught or suggested in the cited references.

Additionally, the latest Section 103 obviousness rejection is submitted to be improper because the Examiner has applied the incorrect standard. On page 3 of the Office action of 23 March 2010 the Examiner writes "[t]he rationale for the combination of the references comes from a motivation that is obvious to one of ordinary skill in the art, and does not have to come from the cited references themselves. In this case, the

examiner feels that the increased security on a network is a motivation to combine one reference with another." (emphasis added). This is clearly not the obviousness standard as set out by the courts. The Examiner seems to use his own subjective standard for what he "feels" is a good rationale for the combination without finding support for the asserted rationale in the cited references. Appellants submit that this subjective or personal standard of the Examiner is not what the courts have ruled to be the proper standard.

Even assuming *arguendo* that the requisite method steps of claims 6, 11-14 and 20-21 are shown by the combination of Linnakangas and AAPA, *prima facie* support for combining the references, according to the requirements as set forth in M.P.E.P. § 2142 has not been provided in the Office Actions.

As provided in M.P.E.P. § 2142, the Supreme Court in *KSR International v. Teleflex Inc.*, 82 USPQ2d 1385, 1396 (2007) specified that the analysis supporting a rejection under 35 U.S.C. § 103 should be made explicit. "[R]ejections on obviousness cannot be sustained with mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006). Furthermore, the Examiner must make "explicit" this rationale of "the apparent reason to combine the

known elements in the fashion claimed," including a detailed explanation of "the effects of demands known to the design community or present in the marketplace" and "the background knowledge possessed by a person having ordinary skill in the art" (KSR, page 14).

The only rationale provided in support of the 103(a) rejection of claim 6 is at the bottom of page 7 of the Office action, which merely asserts it would have been obvious to modify the teaching method of Linnakangas with AAPA because it "would have added flexibility by allowing different networks to connect to the system" (emphasis added). The Examiner has merely provided one benefit, or advantage of the modification as the only rationale provided in the Office Action in support of the instant rejection.

However, merely stating that a benefit of the modification exists, as done above, does not provide the "articulated reasoning with some rationale underpinning to support the legal conclusion of obviousness, required under KSR. By definition, every patentable invention must be "beneficial" - and *arguendo* every invention contemplates at least some new benefit(s) in arriving at the invention - certainly this does not render the benefit obvious or expected. Because every modification or element has a corresponding use or benefit, the above reasoning could be applied to any improvement. It appears

therefore that "hindsight construction" may have perhaps played a role in arriving at the present ground for rejection in the Office action - which though difficult perhaps to avoid in many cases, is nonetheless impermissible in making a *prima facie* showing of obviousness.

According to M.P.E.P. 2142, "the examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness" (emphasis added). It is respectfully submitted that the Examiner has not factually supported the *prima facie* conclusion of obviousness. Appellants cannot see that any of the cited references discusses that "one of the most important factors that has shaped the computer and networking industry is compatibility" or that allowing for "different computers, or different networks, to communicate with each other is always at the forefront of designer's mind." Additionally, Appellants cannot find that the cited references mention that since "very sensitive information can be passed over an un-trusted network such as the Internet, engineers are always looking for ways to beef-up security, and make it harder for hackers to intercept their Internet traffic." It is respectfully submitted that the above text segments are merely speculations on behalf of the Examiner and that the rationale provided by the Examiner is not

supported in the cited references. Because a *prima facie* conclusion of obviousness has not been provided in the Office Action, Appellants respectfully request reconsideration and withdrawal of this ground for rejection.

Appellants further submit that it would not be obvious to modify Linnakangas to meet all the limitations of claim 1. It is submitted Linnakangas does not provide one of ordinary skill in the art the motivation to make the required modifications needed to arrive at the claimed invention. In In re Fine, 5 USPQ2d (Fed. Cir. 1988), the court ruled (on page 1944) that there must be a motivation for the required modification to be obvious. In Winner International Royalty Corp. v. Wing, 48 USPQ2d 1139, the court ruled (on page 1144) that there must have been some explicit teaching or suggestion in the art to motivate one of ordinary skill in the art to make the required modifications.

It is submitted that Linnakangas fails to provide such explicit teaching. Additionally, there is no desirability or motivation to make the required modifications because the current system is complete and functional since the router is a firewall to the Internet 3 for the local area network (LAN) 1. The IP forwarder in the router 2 is designed to open incoming packets (decapsulation) and sends them to the local hosts 5 in a decrypted form and when the router 2 receives outgoing packets

from within the network (i.e. from the local hosts 5) the router encrypts the packets by adding an IPSec layer and sends them to the outside receives such as to the remote hosts 4. This function of the IP forwarder would be useless if the security associations were to be extended all the way to the local hosts 5. The extension of the security association all the way to the local hosts 5 would even make Linnakangas' system inoperable because the decapsulation would interfere with the protocol of the security association. Even if one could find reasons to make the required modifications of Linnakangas' system, Linnakangas and the other cited references still completely fail to teach or suggest the required modifications.

It is thus submitted it would not be obvious to modify Linnakangas to substitute addresses in the same security association and to extend the security association to the local hosts 5 because Linnakangas does not teach or suggest these modifications and it would, among other things, interfere with the function of the IP forwarder.

In view of the above, it is submitted that the claims 6, 11-14 and 20-21 are allowable.

Argument (Rejection 3, Claims 15-19 and 25) - 35 U.S.C.

103 (Obviousness)

Claims 15-19 and 25 are submitted to be allowable because the claims depend upon the allowable base claim 1 and 25, respectively, and because the claims include limitations that are not taught or suggested in the cited references. In this rejection, the Examiner has provided additional "benefits" without providing any rationale for why the combination is obvious. The Examiner merely states (page 11, lines 11-12 of the Office action) that the combination of Linnakangas with Sandhu would have "added another layer of security within the secure connection." On page 12, lines 5-6, the Examiner states that the proposed combination would "have increased the number of security features available in the system." It is submitted that the rationale provided by the Examiner does not satisfy the requirement of providing some articulated reasoning with some rational underpinning, as explained above.

In view of the above, it is submitted that the claims 15-19 and 25 are allowable.

Attorney Docket No. 290.1078APP 6/22/10

Serial No. 10/500,930
Filed: 19 October 2005
Art Unit: 2458

In view of the above arguments, Appellants respectfully request that the Board reverse the Examiner's rejections.

Respectfully submitted,

FASTH LAW OFFICES

/rfasth/

Rolf Fasth

Registration No. 36,999

FASTH LAW OFFICES
26 Pinecrest Plaza, Suite 2
Southern Pines, NC 28387-4301
Telephone: (910) 687-0001
Facsimile: (910) 295-2152

Claims Appendix

1. (Previously presented) A method for secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network, comprising: the first computer and the second computer negotiating and exchanging keys according to a key exchange protocol to establish a secure connection between the first computer and the second computer via the intermediate computer, the secure connection having a source address of the first computer as a first end point and a destination address of the second computer as a second end point of the secure connection, in the first computer, forming a secure message by giving the secure message a first unique identity and a first destination address to the intermediate computer, sending the secure message from the first computer to the intermediate computer, the intermediate computer receiving the secure message and performing a translation by using the first unique identity to find a second destination address to the second computer, the intermediate computer substituting the first destination address with the second destination address to the second computer, the intermediate computer substituting the first unique identity with a second unique identity of the secure connection without

establishing a new secure connection and without involving the second computer, and the intermediate computer forwarding the secure message with the second destination address and the second unique identity to the second computer in the secure connection.

2. (Previously presented) The method of claim 1 wherein the method further comprises forming the secure message by using an IPSec connection between the first computer and the second computer.

3. (Previously presented) The method of claim 1 wherein the method further comprises performing a secure forwarding of the message by making use of SSL or TLS protocols.

4. (Previously presented) The method of claim 2 wherein the method further comprises manually performing a preceding distribution of keys to components for forming the IPSec connection.

5. (Previously presented) The method of claim 2 wherein the method further comprises performing a preceding distribution of keys for forming the IPSec connection by an automated key exchange protocol.

6. (Previously presented) The method of claim 5 wherein the method further comprises performing the automated key exchange protocol used for the preceding distribution of keys for forming the IP Sec connection by means of a modified IKE key exchange protocol between the first computer and the intermediate computer and by means of a standard IKE key exchange protocol between the intermediate computer and the second computer.

7. (Previously presented) The method of claim 2 wherein the method further comprises sending the message that is sent from the first computer as a packet that contains message data, an inner IP header containing the actual sender and receiver addresses, an outer IP header containing the addresses of the first computer and the intermediate computer, the unique identity.

8. (Previously presented) The method of claim 1 wherein the method further comprises the IPSec connection being one or more security associations (SA) and the unique identity being one or more SPI values.

9. (Previously presented) The method of claim 1 wherein the method further comprises performing the matching by using a

translation table stored at the intermediate computer.

10. (Previously presented) The method of claim 1 wherein the method further comprises changing both the address and the SPI-value by the intermediate computer.

11. (Previously presented) The method of claim 1 wherein the method further comprises the first computer being a mobile terminal so that the mobility is enabled by modifying the translation table at the intermediate computer.

12. (Previously presented) The method of claim 11 wherein the method further comprises performing the modification of the translation tables by sending a request for registration of the new address from the first computer to the intermediate computer.

13. (Previously presented) The method of claim 12 wherein the method further comprises sending a reply to the request for registration from the intermediate computer to the first computer.

14. (Previously presented) The method of claim 12 wherein the method further comprises authenticating or encrypting by IPsec the request for registration and/or reply.

15. (Previously presented) The method of claim 4 wherein the method further comprises establishing the key distribution for the secure connections by establishing an IKE protocol translation table, and using the translation table to modify IP addresses and cookie values of IKE packets in the intermediate computer.

16. (Previously presented) The method of claim 15 wherein the method further comprises establishing the key exchange distribution by:
generating an initiator cookie and sending a zero responder cookie to the second computer,
generating a responder cookie in the second computer,
establishing a mapping between IP addresses and IKE cookie values in the intermediate computer, and
using the translation table to modify IKE packets in flight by modifying the external IP addresses and possibly IKE cookies of the IKE packets.

17. (Previously presented) The method of claim 15 wherein the method further comprises modifying a modified IKE protocol between the first computer and the intermediate computer by transmitting the IKE keys from the first computer to the

intermediate computer in order to decrypt and modify IKE packets.

18. (Previously presented) The method of claim 15 wherein the method further comprises carrying out in a modified IKE protocol between the first computer and the intermediate computer the modification of the IKE packets by the first computer with the intermediate computer requesting such modifications.

19. (Previously presented) The method of claim 17 wherein the method further comprises defining the address so that the first computer is identified for the second computer by the intermediate computer by means of an IP address taken from a pool of user IP addresses when forming the translation table.

20. (Previously presented) The method of claim 1 wherein the method further comprises sending the secure message by using an IPSec transport mode.

21. (Previously presented) The method of claim 1 wherein the method further comprises sending the secure message by using an IPSec tunnel mode.

22. (Previously presented) A telecommunication network for secure forwarding of messages, comprising:

a first computer, a second computer and an intermediate computer, means for negotiating and exchanging keys, according to a key exchange protocol, between the first computer and the second computer to establish a security association having a source address of the first computer as a first end point and a destination address of the second computer as a second end point, the first and the second computers having means for performing an IPsec processing, the intermediate computer having translation means for using translation tables to perform IPsec and IKE translation and for changing a destination address of the intermediate computer of a secure message to a destination address of the second computer, and the intermediate computer having means for forwarding the secure message received from the first computer to the second computer in the security association.

23. (Previously presented) The telecommunication network of claim 22 wherein the translation table for IPsec translation has IP addresses of the intermediate computer to be matched with IP addresses of the second computer.

24. (Previously presented) The telecommunication network of claim

22 wherein the translation tables for IKE translation consists of two partitions, one for the communication between the first computer and the intermediate computer and another for the communication between the intermediate computer and the second computer.

25. (Previously presented) The telecommunication network of claim 24 wherein both partitions of the mapping table for IKE translation contains translation fields for a source IP address, a destination IP address, initiator and responder cookies between respective computers.

26. (Previously presented) The telecommunication network of claim 22 wherein there is another translation table for IKE translation containing fields for matching a given user to a given computer.

27. (Previously presented) A telecommunication network for secure forwarding of messages, comprising:

a first computer,

a second computer,

an intermediate computer electronically connected to the first computer and the second computer,

means for negotiating and exchanging keys between the first

computer and the second computer to establish a secure connection

having a source address of the first computer as a first end point and a destination address of the second computer as a second end point, and the intermediate computer having means for performing translation between destination addresses and secure identities for forwarding secure messages received from the first computer to the second computer in the secure connection.

Attorney Docket No. 290.1078APP 6/22/10

Serial No. 10/500,930
Filed: 19 October 2005
Art Unit: 2458

Evidence Appendix

There is no evidence to be presented in this appendix.

Attorney Docket No. 290.1078APP 6/22/10

Serial No. 10/500,930
Filed: 19 October 2005
Art Unit: 2458

Related Proceedings Appendix

There is no related proceeding to be presented in this appendix.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of
Sami Vaarala, Antti Nuopponen

Art Unit 2458
Confirmation No. 1571

Serial No. 10/500,930

CERTIFICATE OF MAILING

Filed: 19 October 2005

I HEREBY CERTIFY THAT THIS PAPER AND THE DOCUMENTS
REFERRED TO AS BEING ATTACHED OR ENCLOSED HERewith
ARE BEING SUBMITTED ELECTRONICALLY TO THE UNITED
STATES PATENT AND TRADEMARK OFFICE ON **22 June 2010**.

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

/rfasth/

Examiner: Towfighi, Afshawn

Rolf Fasth
Attorney for Applicant

Date: 22 June 2010

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) Revised Appeal Brief
- (X) The Commissioner is hereby authorized to charge any 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
26 Pinecrest Plaza, Suite 2
Southern Pines, NC 28387-4301

Telephone: 910-687-0001
Facsimile: 910-295-2152
Attorney Docket No. 290.1078APP

Electronic Acknowledgement Receipt

EFS ID:	7861333
Application Number:	10500930
International Application Number:	
Confirmation Number:	1571
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:	290.1078USN
Receipt Date:	22-JUN-2010
Filing Date:	19-OCT-2005
Time Stamp:	06:25:34
Application Type:	U.S. National Stage under 35 USC 371

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	Supplemental Appeal Brief	REVISED_APEAL_BRIEF.PDF	62489 <small>d31629481828942db7845c85c8ee5d75385a71d9</small>	no	39

Warnings:

Information:

2	Miscellaneous Incoming Letter	TRX.PDF	18340	no	1
			2b29e34751692f5535c7d763bb3b0dbf19bbbeab		

Warnings:

Information:

Total Files Size (in bytes):	80829
-------------------------------------	-------

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

Attorney Matter No. 290.1078APP

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF APPEALS AND INTERFERENCES

In re application of: Sami Vaarala et al

)	
)	
Serial No. 10/500,930)	
)	APPEAL BRIEF
)	
Filed: 19 October 2005)	
)	
For: METHOD AND DEVICE FOR)	
CLEANING OF FILTER)	Art Unit 2458
)	
)	Examiner Afshawn M. Towfighi
)	
)	
)	
Date: 24 May, 2010)	

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

APPELLANT'S BRIEF ON APPEAL

Real Party in Interest

The real party in interest is MPH Technologies Oy,
Tekniikantie 14, FIN-02150 Espoo, Finland, the recorded assignee
of the above-captioned patent application.

Related Appeals and Interferences

No related appeals or interferences of this application
are known to the Appellant, the Appellant's legal representative
or assignee which will directly affect or be directly affected by
or have a bearing on the Board's decision in the pending appeal.

Status of the Claims

Rejection 1

Claims 1-5, 7-10, 22-24 and 26-27 stand rejected in the Office action dated 23 March 2010 as being anticipated by US Patent Application No. 2001/0047487 to Linnakangas et al.

Rejection 2

Claims 6, 11-14, 20-21 stand rejected in the Office action dated 23 March 2010 as being obvious over Linnakangas in view of Applicant's Admitted Prior Art (AAPA).

Rejection 3

Claims 15-19 and 25 stand rejected in the Office action dated 23 March 2010 as being obvious over Linnakangas in view of Sandhu.

The application has been rejected at least twice. A copy of the claims is reproduced as Claims Appendix hereto. The rejections of claims 1-27 are appealed.

Status of Amendments

All Amendments have been entered.

Summary of Claimed Subject Matter

The application has three independent claims (i.e. claims 1, 22 and 27). Independent claim 1 refers to a method for secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network. The first computer and the second computer negotiate and exchange keys according to a key exchange protocol to establish a secure connection (such as a security association (SA)) between the first computer and the second computer via the intermediate computer. The secure connection has a source address of the first computer as a first end point and a destination address of the second computer as a second end point of the secure connection. A secure message is formed in the first computer by giving the secure message a first unique identity and a first destination address to the intermediate computer. The secure message is sent from the first computer to the intermediate computer. The intermediate computer receives the secure message and performs a translation by using the first unique identity to find a second destination address of the second computer. The intermediate computer substitutes the first destination address with the second destination address to the second computer. The intermediate computer substitutes the first unique identity with a second unique identity of the same secure

connection without establishing a new secure connection between the intermediate computer and the second computer and without involving the second computer. The intermediate computer then forwards the secure message with the second destination address and the second unique identity to the second computer in the same secure connection.

Independent claim 22 refers to a telecommunication network for secure forwarding of messages that has a first computer, a second computer and an intermediate computer. The network has means for negotiating and exchanging keys, according to a key exchange protocol, between the first computer and the second computer to establish a security association (SA) that has a source address of the first computer as a first end point and a destination address of the second computer as a second end point. The first and the second computers have means for performing IPSec processing. The intermediate computer has translation means for using translation tables to perform IPSec and IKE translation and for changing a destination address of the intermediate computer of a secure message to a destination address of the second computer. Furthermore, the intermediate computer has means for forwarding the secure message received from the first computer to the second computer in the same security association.

Independent claim 27 refers to a telecommunication

network for secure forwarding of messages that has a first computer, a second computer and an intermediate computer electronically connected to the first computer and the second computer. The network has means for negotiating and exchanging keys between the first computer and the second computer to establish a secure connection therebetween that has a source address of the first computer as a first end point and a destination address of the second computer as a second end point. The intermediate computer has means for performing translation between destination addresses and secure identities for forwarding secure messages received from the first computer to the second computer in the same secure connection.

In summary, one problem with standard/conventional IPSec mobile telephone systems is that the end points of the IPSec tunnel mode SA (security association) are fixed. There is no feature in conventional systems for changing any of the parameters of an SA other than by establishing a new SA that replaces the previous SA. More particularly, since mobile terminals move and thus change their network points frequently and since IPSec connections are bound to fixed addresses, the mobile terminals must establish new IPSec connections from each new point of attachment. This requires the exchange of keys etc. which is a cumbersome process that uses computation time. The method of the present invention provides a solution to this

problem.

Unique features of the present invention are the secure connection is established all the way between the first computer and the second computer via the intermediate computer by exchanging keys and that the intermediate computer 1) uses the first unique identity to find a second destination address to the second computer and 2) substitutes the first destination address with the second destination address in the same secure connection. Thus, there is no need to set up a new secure connection between the intermediate computer and the second computer. In this way, a secure message, sent from the first computer to the intermediate computer, may be modified by the intermediate computer so that it can be forwarded from the intermediate computer to the second computer in the same secure connection without requiring the cumbersome exchange of additional keys to set up a new secure connection between the intermediate computer and the second computer and without involving the second computer.

Grounds Of Rejection To Be Reviewed On Appeal

Whether the Examiner properly rejected claims 1-5, 7-10, 22-24 and 26-27 as being anticipated by Linnakangas and whether the Examiner properly rejected claims 6, 11-14 and 20-21

Attorney Docket No. 290.1078APP 5/24/10

Serial No. 10/500,930
Filed: 19 October 2005
Art Unit: 2458

of the application as being obvious of Linnakangas in view of Applicants' Admitted Prior Art (AAPA). Finally, whether the Examiner properly rejected claims 15-19 and 25 of the application as being obvious of Linnakangas in view of Sandhu.

Argument (Rejection 1) - 35 U.S.C. 102 (Anticipation)

The 102 rejection is submitted to be improper because the cited Linnakangas reference (US 2001/0047487) does not, among other things, teach or suggest the steps establishing a secure connection between the first and second computer that requires the first and second computer to exchange keys between each other when establishing the secure connection so that the secure connection has a source address of the first computer as a first end point and a destination address of the second computer as a second end point of the secure connection. Additionally, Linnakangas fails to teach the step of the intermediate computer substituting the first destination address and first unique identity of the secure message with a second destination address and a second unique identity of a second computer in the same secure connection without establishing a new secure connection and without involving the second computer so that the intermediate computer forwards the secure message to the second computer in the same secure connection. Linnakangas merely teaches the step of setting up of a secure connection (security association) between the intermediate computer (router 2) and the second computer (remote hosts 4) and the prior segment between the intermediate computer and the first computer (local hosts 5) is merely within the same local area network (LAN) so that the intermediate computer decrypts packets going into the local hosts

5 of the LAN and encrypts packets going out from the local hosts 5 of the LAN to the second computer. If the segment between the intermediate computer (router 2) and the first computer (local hosts 5) had been part of the same security association there would be no need to decrypt and encrypt messages going to and from the first computer (local hosts 5). The decryption/encryption procedure of Linnakangas' intermediate computer (router 2) is quite different from sending a secure message in a secure connection that extends all the way from the first computer (local hosts 5) to the second computer (remote hosts 4). The above features are submitted to be novel and not obvious in view of the cited references.

More particularly, Linnakangas describes the establishment of a security association (which is one type of a secure connection). When a security association is formed between two computers, keys are first exchanged between the two computers. This is done according to an Internet Key Exchange (IKE) protocol and the security association is defined by unique identity and addresses of the two computers between which the security association is formed. Despite numerous efforts to try to explain in Linnakangas there is no security association established between the local hosts 5 (first computer) and the router 2 (intermediate computer), the Examiner still maintains that there is also a security association created between the

router 2 and the local hosts 5. Appellants maintain that there is only a security association created between the router 2 (intermediate computer) and the remote hosts 4 (second computer). It is submitted that the security association established does not extend to the local hosts 5 (first computer).

The Examiner refers to paragraphs 4 and 5 of Linnakangas as teaching the establishment of the secure connection between the first computer and the second computer.

Appellants respectfully disagree. Paragraphs 4 and 5 describe the establishment of security associations (SAs) in general and not that a SA is established between the remote hosts 4 and local hosts 5 or between the intermediate computer 2 and the local hosts 5. It is submitted that paragraph 24 of Linnakangas clearly teaches that each remote host 4 must negotiate at least one pair of SAs with the router 2. Linnakangas fails to teach the remote hosts 4 negotiating and establishing a security association with the local hosts 5. More importantly, there is absolutely nothing in Linnakangas about the local hosts 5 (first computer) negotiating a security association with the remote hosts 4 (second computer) so that a security association extends all the way from one of the local hosts 5 to one of the remote hosts 4. Appellants assert that Linnakangas and the other cited references completely fail to teach or suggest the step of the local hosts 5 (first computer)

establishing secure connections with the remote hosts 4 (second computer). On the contrary, Linnakangas' local hosts 5 and the router 2 communicate, as indicated above, via a Local Area Network (LAN) 1. The SA thus only extends between the remote hosts 4 and the router 2 but not between the router 2 and the local hosts 5. To further support that there is no security association established between the router 2 and the local hosts 5, the router 2 decrypts, reads and unwraps any secure message received from the remote hosts 4 to be able to determine that the message is to be forwarded (most likely as plain text) to the local hosts 5. This forwarding is done without implementing IPsec. There is nothing about forming a secure message in the local hosts 5 or the local hosts 5 negotiating secure associations with the remote hosts 4. In other words, it is important to note that the negotiated secure connection merely extends between the router 2 and the remote hosts 4. On page 4 of the Office action, the Examiner refers to paragraph 8, lines 1-5 of Linnakangas as teaching that "the destination of the packets is the second computer." Firstly, the claim does not require that the "destination of the packets is the second computer." The claim requires that the secure connection has a source address of the first computer as a first end point and a destination address of the second computer as a second end point of the secure connection. As explained above, Linnakangas' SA

only extends between the intermediate computer (router 2) and the remote hosts (4) but excludes the segment between the router (2) and the local hosts (5). Secondly, the cited text segment in paragraph 8, lines 1-5 of Linnakangas merely refers to the IP forwarder as being the receiver (or "destination" as the Examiner calls it). It is important to realize that the IP forwarder is an inner destination within the router 2 itself and not the local hosts (5). Paragraph 31, lines 1-3 of Linnakangas supports this. The IP forwarder (IPFW) is shown in Fig. 2 that describes the internal architecture of the router 2 (see paragraph 21 of Linnakangas). In paragraph 24, lines 4-8, Linnakangas explains that "[b]y using IPsec to control communication between the router 2 and the remote hosts 4 (and hence between remote hosts 4 and local hosts 5), a Virtual Private Network (VPN) may be established" (emphasis added). It is respectfully submitted that this is different from establishing a secure connection that extends all the way from the local hosts 5 to the remote hosts 4 which requires the exchange of keys according to a key exchange protocol. Additionally, "controlling" communication across the route from local hosts 5 via router 2 all the way to the remote hosts 4 does not mean that there is a secure connection established also between router 2 and host 5. As explained above, the nodes involved in the negotiation and exchange of keys according to the key exchange protocol IKE determines the

boundaries of the secure connection. In Linnakangas, the exchange of keys is only between the router 2 and the remote hosts 4. In other words, Linnakangas merely mentions controlling the communication, not securing. It should be noted that the virtual private network in Linnakangas is not secured since it is not part of the security association between the router 2 and the remote hosts 4. There is not really as much need for a secure connection between the router 2 and the host 5 since the connection is within the same LAN.

Even if the communication between the router 2 and the local hosts 5 may be considered quite safe, it is still not part of the SA because the SA merely extends between the router 2 and the remote hosts 4. The fact that there is no SA between the router 2 and the local hosts 5 is supported on line 2 of paragraph 4 in Linnakangas that discusses encapsulation and decapsulation of IPSec packets. This means the segment between the router 2 and the local hosts 5 is not part of the security association that extends between the router 2 and the remote hosts 4. If this segment would have been part of the same security association then there would not make sense to encrypt and decrypt incoming and outgoing messages between the router 2 and the local hosts 5. Instead, the packets are opened and decrypted by adding an IPSec layer. This is quite different from address substitution in a secure connection that extends between

the first computer and the second computer as required by claim 1. In other words, when the router 2 receives a packet from the outside (such as from the remote hosts 4), the router 2 opens the packet (decapsulation) and sends it to the local host 5 in a decrypted form and when the router 2 receives a packet from within the network (such as from the local hosts 5) the router encrypts the packets by adding an IPsec layer and sends it into the security association (SA) such as to the remote hosts 4.

On page 5 of the Office action, the Examiner states that the router is able to perform IPsec and IKE translation and inherently includes a translation table. Appellants cannot see that Linnakangas teaches that the router 2 can perform IPsec/IKE translation as asserted by the Examiner. The Examiner also states that "address substitution is a standard part of IPsec processing and IKE translation." It should be noted that address substitution is not a standard part of IPsec. The Examiner refers to paragraphs 4 and 24 of Linnakangas as teaching that address substitution is standard.

In view of the above, it is submitted that claim 1 is not anticipated by Linnakangas and that the Section 102 rejection should be withdrawn.

Claims 2-5 and 7-10 are submitted to be allowable because they depend upon the allowable base claim 1 and because each claim includes limitations that are not taught or suggested

in the cited references.

Claim 22 is submitted to be allowable for reasons similar to the arguments put forth for the allowability of claim 1. As mentioned above, Linnakangas merely shows the establishment of a secure connection between the remote hosts 4 and the router 2 by negotiating security associations (SAs) between those two components. Appellants fail to see where Linnakangas teaches means for negotiating and exchanging keys, according to a key exchange protocol, between the local hosts 4 (first computer) and the remote hosts 5 (second computer) to establish a security association that has a source address of the local host 5 as a first end point and a destination address of the remote host 4 as a second end point, as required by claim 22. In contrast, Linnakangas merely teaches the negotiation of the security associations between the router 2 (intermediate computer) and the remote hosts 4 (second computer), as expressly shown in paragraph 0024 of the Linnakangas reference and as explained above.

It is submitted that Linnakangas fails to teach or suggest all the limitations of claim 22. Therefore, the anticipation rejection of claim 22 under § 102 is improper, and should be removed.

Claims 23-24 and 26 are submitted to be allowable because the claims depend either directly or indirectly upon the

allowable base claim 22 and because each claim includes limitations that are not taught or suggested in the cited references.

Similar to claim 22, claim 27 requires means for negotiating and exchanging keys between the first computer and the second computer to establish a secure connection having a source address of the first computer as a first end point and a destination address of the second computer as a second end point. For reasons similar to the reasons put forth for the allowability of claims 1 and 22, claim 27 is submitted to be allowable.

Argument (Rejection 2, Claims 6, 11-14, 20-21) - 35
U.S.C. 103 (Obviousness)

Claims 6, 11-14 and 20-21 are submitted to be allowable because the claims depend upon the allowable base claim 1 and because the claims include limitations that are not taught or suggested in the cited references.

Additionally, the latest Section 103 obviousness rejection is submitted to be improper because the Examiner has applied the incorrect standard. On page 3 of the Office action of 23 March 2010 the Examiner writes "[t]he rationale for the combination of the references comes from a motivation that is obvious to one of ordinary skill in the art, and does not have to come from the cited references themselves. In this case, the

examiner feels that the increased security on a network is a motivation to combine one reference with another." (emphasis added). This is clearly not the obviousness standard as set out by the courts. The Examiner seems to use his own subjective standard for what he "feels" is a good rationale for the combination without finding support for the asserted rationale in the cited references. Appellants submit that this subjective or personal standard of the Examiner is not what the courts have ruled to be the proper standard.

Even assuming *arguendo* that the requisite method steps of claims 6, 11-14 and 20-21 are shown by the combination of Linnakangas and AAPA, *prima facie* support for combining the references, according to the requirements as set forth in M.P.E.P. § 2142 has not been provided in the Office Actions.

As provided in M.P.E.P. § 2142, the Supreme Court in *KSR International v. Teleflex Inc.*, 82 USPQ2d 1385, 1396 (2007) specified that the analysis supporting a rejection under 35 U.S.C. § 103 should be made explicit. "[R]ejections on obviousness cannot be sustained with mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006). Furthermore, the Examiner must make "explicit" this rationale of "the apparent reason to combine the

known elements in the fashion claimed," including a detailed explanation of "the effects of demands known to the design community or present in the marketplace" and "the background knowledge possessed by a person having ordinary skill in the art" (KSR, page 14).

The only rationale provided in support of the 103(a) rejection of claim 6 is at the bottom of page 7 of the Office action, which merely asserts it would have been obvious to modify the teaching method of Linnakangas with AAPA because it "would have added flexibility by allowing different networks to connect to the system" (emphasis added). The Examiner has merely provided one benefit, or advantage of the modification as the only rationale provided in the Office Action in support of the instant rejection.

However, merely stating that a benefit of the modification exists, as done above, does not provide the "articulated reasoning with some rationale underpinning to support the legal conclusion of obviousness, required under KSR. By definition, every patentable invention must be "beneficial" - and *arguendo* every invention contemplates at least some new benefit(s) in arriving at the invention - certainly this does not render the benefit obvious or expected. Because every modification or element has a corresponding use or benefit, the above reasoning could be applied to any improvement. It appears

therefore that "hindsight construction" may have perhaps played a role in arriving at the present ground for rejection in the Office action - which though difficult perhaps to avoid in many cases, is nonetheless impermissible in making a *prima facie* showing of obviousness.

According to M.P.E.P. 2142, "the examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness" (emphasis added). It is respectfully submitted that the Examiner has not factually supported the *prima facie* conclusion of obviousness. Appellants cannot see that any of the cited references discusses that "one of the most important factors that has shaped the computer and networking industry is compatibility" or that allowing for "different computers, or different networks, to communicate with each other is always at the forefront of designer's mind." Additionally, Appellants cannot find that the cited references mention that since "very sensitive information can be passed over an un-trusted network such as the Internet, engineers are always looking for ways to beef-up security, and make it harder for hackers to intercept their Internet traffic." It is respectfully submitted that the above text segments are merely speculations on behalf of the Examiner and that the rationale provided by the Examiner is not

supported in the cited references. Because a *prima facie* conclusion of obviousness has not been provided in the Office Action, Appellants respectfully request reconsideration and withdrawal of this ground for rejection.

Appellants further submit that it would not be obvious to modify Linnakangas to meet all the limitations of claim 1. It is submitted Linnakangas does not provide one of ordinary skill in the art the motivation to make the required modifications needed to arrive at the claimed invention. In In re Fine, 5 USPQ2d (Fed. Cir. 1988), the court ruled (on page 1944) that there must be a motivation for the required modification to be obvious. In Winner International Royalty Corp. v. Wing, 48 USPQ2d 1139, the court ruled (on page 1144) that there must have been some explicit teaching or suggestion in the art to motivate one of ordinary skill in the art to make the required modifications.

It is submitted that Linnakangas fails to provide such explicit teaching. Additionally, there is no desirability or motivation to make the required modifications because the current system is complete and functional since the router is a firewall to the Internet 3 for the local area network (LAN) 1. The IP forwarder in the router 2 is designed to open incoming packets (decapsulation) and sends them to the local hosts 5 in a decrypted form and when the router 2 receives outgoing packets

from within the network (i.e. from the local hosts 5) the router encrypts the packets by adding an IPSec layer and sends them to the outside receives such as to the remote hosts 4. This function of the IP forwarder would be useless if the security associations were to be extended all the way to the local hosts 5. The extension of the security association all the way to the local hosts 5 would even make Linnakangas' system inoperable because the decapsulation would interfere with the protocol of the security association. Even if one could find reasons to make the required modifications of Linnakangas' system, Linnakangas and the other cited references still completely fail to teach or suggest the required modifications.

It is thus submitted it would not be obvious to modify Linnakangas to substitute addresses in the same security association and to extend the security association to the local hosts 5 because Linnakangas does not teach or suggest these modifications and it would, among other things, interfere with the function of the IP forwarder.

In view of the above, it is submitted that the claims 6, 11-14 and 20-21 are allowable.

Argument (Rejection 3, Claims 15-19 and 25) - 35 U.S.C.

103 (Obviousness)

Claims 15-19 and 25 are submitted to be allowable because the claims depend upon the allowable base claim 1 and 25, respectively, and because the claims include limitations that are not taught or suggested in the cited references. In this rejection, the Examiner has provided additional "benefits" without providing any rationale for why the combination is obvious. The Examiner merely states (page 11, lines 11-12 of the Office action) that the combination of Linnakangas with Sandhu would have "added another layer of security within the secure connection." On page 12, lines 5-6, the Examiner states that the proposed combination would "have increased the number of security features available in the system." It is submitted that the rationale provided by the Examiner does not satisfy the requirement of providing some articulated reasoning with some rational underpinning, as explained above.

In view of the above, it is submitted that the claims 15-19 and 25 are allowable.

In view of the above arguments, Appellants respectfully request that the Board reverse the Examiner's rejections.

Respectfully submitted,

FASTH LAW OFFICES

/rfasth/

Rolf Fasth

Registration No. 36,999

FASTH LAW OFFICES
26 Pinecrest Plaza, Suite 2
Southern Pines, NC 28387-4301
Telephone: (910) 687-0001
Facsimile: (910) 295-2152

Claims Appendix

1. (Previously presented) A method for secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network, comprising: the first computer and the second computer negotiating and exchanging keys according to a key exchange protocol to establish a secure connection between the first computer and the second computer via the intermediate computer, the secure connection having a source address of the first computer as a first end point and a destination address of the second computer as a second end point of the secure connection, in the first computer, forming a secure message by giving the secure message a first unique identity and a first destination address to the intermediate computer, sending the secure message from the first computer to the intermediate computer, the intermediate computer receiving the secure message and performing a translation by using the first unique identity to find a second destination address to the second computer, the intermediate computer substituting the first destination address with the second destination address to the second computer, the intermediate computer substituting the first unique identity with a second unique identity of the secure connection without

establishing a new secure connection and without involving the second computer, and the intermediate computer forwarding the secure message with the second destination address and the second unique identity to the second computer in the secure connection.

2. (Previously presented) The method of claim 1 wherein the method further comprises forming the secure message by using an IPSec connection between the first computer and the second computer.

3. (Previously presented) The method of claim 1 wherein the method further comprises performing a secure forwarding of the message by making use of SSL or TLS protocols.

4. (Previously presented) The method of claim 2 wherein the method further comprises manually performing a preceding distribution of keys to components for forming the IPSec connection.

5. (Previously presented) The method of claim 2 wherein the method further comprises performing a preceding distribution of keys for forming the IPSec connection by an automated key exchange protocol.

6. (Previously presented) The method of claim 5 wherein the method further comprises performing the automated key exchange protocol used for the preceding distribution of keys for forming the IP Sec connection by means of a modified IKE key exchange protocol between the first computer and the intermediate computer and by means of a standard IKE key exchange protocol between the intermediate computer and the second computer.

7. (Previously presented) The method of claim 2 wherein the method further comprises sending the message that is sent from the first computer as a packet that contains message data, an inner IP header containing the actual sender and receiver addresses, an outer IP header containing the addresses of the first computer and the intermediate computer, the unique identity.

8. (Previously presented) The method of claim 1 wherein the method further comprises the IPSec connection being one or more security associations (SA) and the unique identity being one or more SPI values.

9. (Previously presented) The method of claim 1 wherein the method further comprises performing the matching by using a

translation table stored at the intermediate computer.

10. (Previously presented) The method of claim 1 wherein the method further comprises changing both the address and the SPI-value by the intermediate computer.

11. (Previously presented) The method of claim 1 wherein the method further comprises the first computer being a mobile terminal so that the mobility is enabled by modifying the translation table at the intermediate computer.

12. (Previously presented) The method of claim 11 wherein the method further comprises performing the modification of the translation tables by sending a request for registration of the new address from the first computer to the intermediate computer.

13. (Previously presented) The method of claim 12 wherein the method further comprises sending a reply to the request for registration from the intermediate computer to the first computer.

14. (Previously presented) The method of claim 12 wherein the method further comprises authenticating or encrypting by IPsec the request for registration and/or reply.

15. (Previously presented) The method of claim 4 wherein the method further comprises establishing the key distribution for the secure connections by establishing an IKE protocol translation table, and using the translation table to modify IP addresses and cookie values of IKE packets in the intermediate computer.

16. (Previously presented) The method of claim 15 wherein the method further comprises establishing the key exchange distribution by:
generating an initiator cookie and sending a zero responder cookie to the second computer,
generating a responder cookie in the second computer,
establishing a mapping between IP addresses and IKE cookie values in the intermediate computer, and
using the translation table to modify IKE packets in flight by modifying the external IP addresses and possibly IKE cookies of the IKE packets.

17. (Previously presented) The method of claim 15 wherein the method further comprises modifying a modified IKE protocol between the first computer and the intermediate computer by transmitting the IKE keys from the first computer to the

intermediate computer in order to decrypt and modify IKE packets.

18. (Previously presented) The method of claim 15 wherein the method further comprises carrying out in a modified IKE protocol between the first computer and the intermediate computer the modification of the IKE packets by the first computer with the intermediate computer requesting such modifications.

19. (Previously presented) The method of claim 17 wherein the method further comprises defining the address so that the first computer is identified for the second computer by the intermediate computer by means of an IP address taken from a pool of user IP addresses when forming the translation table.

20. (Previously presented) The method of claim 1 wherein the method further comprises sending the secure message by using an IPSec transport mode.

21. (Previously presented) The method of claim 1 wherein the method further comprises sending the secure message by using an IPSec tunnel mode.

22. (Previously presented) A telecommunication network for secure forwarding of messages, comprising:

a first computer, a second computer and an intermediate computer, means for negotiating and exchanging keys, according to a key exchange protocol, between the first computer and the second computer to establish a security association having a source address of the first computer as a first end point and a destination address of the second computer as a second end point, the first and the second computers having means for performing an IPsec processing, the intermediate computer having translation means for using translation tables to perform IPsec and IKE translation and for changing a destination address of the intermediate computer of a secure message to a destination address of the second computer, and the intermediate computer having means for forwarding the secure message received from the first computer to the second computer in the security association.

23. (Previously presented) The telecommunication network of claim 22 wherein the translation table for IPsec translation has IP addresses of the intermediate computer to be matched with IP addresses of the second computer.

24. (Previously presented) The telecommunication network of claim

22 wherein the translation tables for IKE translation consists of two partitions, one for the communication between the first computer and the intermediate computer and another for the communication between the intermediate computer and the second computer.

25. (Previously presented) The telecommunication network of claim 24 wherein both partitions of the mapping table for IKE translation contains translation fields for a source IP address, a destination IP address, initiator and responder cookies between respective computers.

26. (Previously presented) The telecommunication network of claim 22 wherein there is another translation table for IKE translation containing fields for matching a given user to a given computer.

27. (Previously presented) A telecommunication network for secure forwarding of messages, comprising:

a first computer,

a second computer,

an intermediate computer electronically connected to the first computer and the second computer,

means for negotiating and exchanging keys between the first

computer and the second computer to establish a secure connection

having a source address of the first computer as a first end point and a destination address of the second computer as a second end point, and the intermediate computer having means for performing translation between destination addresses and secure identities for forwarding secure messages received from the first computer to the second computer in the secure connection.

Attorney Docket No. 290.1078APP 5/24/10

Serial No. 10/500,930
Filed: 19 October 2005
Art Unit: 2458

Evidence Appendix

There is no evidence to be presented in this appendix.

Attorney Docket No. 290.1078APP 5/24/10

Serial No. 10/500,930
Filed: 19 October 2005
Art Unit: 2458

Related Proceedings Appendix

There is no related proceeding to be presented in this appendix.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of
Sami Vaarala, Antti Nuopponen

Art Unit 2458
Confirmation No. 1571

Serial No. 10/500,930

CERTIFICATE OF MAILING

Filed: 19 October 2005

I HEREBY CERTIFY THAT THIS PAPER AND THE DOCUMENTS
REFERRED TO AS BEING ATTACHED OR ENCLOSED HERewith
ARE BEING SUBMITTED ELECTRONICALLY TO THE UNITED
STATES PATENT AND TRADEMARK OFFICE ON **24 May 2010**.

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

/rfasth/

Examiner: Towfighi, Afshawn

Rolf Fasth
Attorney for Applicant

Date: 24 May 2010

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) Appeal Brief
- (X) The Commissioner is hereby authorized to charge any 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
26 Pinecrest Plaza, Suite 2
Southern Pines, NC 28387-4301

Telephone: 910-687-0001
Facsimile: 910-295-2152
Attorney Docket No. 290.1078APP

Electronic Patent Application Fee Transmittal

Application Number:	10500930
Filing Date:	19-Oct-2005
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:	290.1078USN

Filed as Small Entity

U.S. National Stage under 35 USC 371 Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Filing a brief in support of an appeal	2402	1	270	270

Post-Allowance-and-Post-Issuance:

Extension-of-Time:

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				270

Electronic Acknowledgement Receipt

EFS ID:	7670476
Application Number:	10500930
International Application Number:	
Confirmation Number:	1571
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:	290.1078USN
Receipt Date:	24-MAY-2010
Filing Date:	19-OCT-2005
Time Stamp:	13:35:45
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$270
RAM confirmation Number	11203
Deposit Account	060243
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:
Charge any Additional Fees required under 37 C.F.R. 1.492 (National application filing, search, and examination fees)
Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

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

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

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Appeal Brief Filed	APPEAL_BRIEF.PDF	56763 b692051b869db9bb6e74bbd742268fd0 a9cfb8	no	34

Warnings:

Information:

2	Miscellaneous Incoming Letter	TRX.PDF	18316 37c74dfc258fd6f1a082e4af1f82d814d7441 b8f	no	1
---	-------------------------------	---------	---	----	---

Warnings:

Information:

3	Fee Worksheet (PTO-875)	fee-info.pdf	29801 b88e8a7e9005115f5a47db1fa118f89e89af bc3e	no	2
---	-------------------------	--------------	---	----	---

Warnings:

Information:

Total Files Size (in bytes):

104880

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.

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.

NOTICE OF APPEAL FROM THE EXAMINER TO THE BOARD OF PATENT APPEALS AND INTERFERENCES		Docket Number (Optional) 290.1078APP	
I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] <u>20 May 2010 (electronically)</u> on _____ Signature <u>/rfasth/</u> _____ Typed or printed name <u>Rolf Fasth</u> _____		In re Application of Sami Vaarala, Antti Nuopponen	
		Application Number 10500930	Filed 2005-10-19
		For METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION	
		Art Unit 2458	Examiner Towfighi, Afshawn
Applicant hereby appeals to the Board of Patent Appeals and Interferences from the last decision of the examiner.			
The fee for this Notice of Appeal is (37 CFR 41.20(b)(1))		\$ <u>540.00</u>	
<input checked="" type="checkbox"/> Applicant claims small entity status. See 37 CFR 1.27. Therefore, the fee shown above is reduced by half, and the resulting fee is:		\$ <u>270.00</u>	
<input type="checkbox"/> A check in the amount of the fee is enclosed.			
<input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached.			
<input type="checkbox"/> The Director has already been authorized to charge fees in this application to a Deposit Account.			
<input checked="" type="checkbox"/> The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. <u>060243</u> .			
<input type="checkbox"/> A petition for an extension of time under 37 CFR 1.136(a) (PTO/SB/22) is enclosed.			
WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.			
I am the			
<input type="checkbox"/> applicant/inventor.		<u>/rfasth/</u> Signature	
<input type="checkbox"/> assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)		<u>Rolf Fasth</u> Typed or printed name	
<input checked="" type="checkbox"/> attorney or agent of record. <u>36999</u> Registration number _____		<u>910-687-0001</u> Telephone number	
<input type="checkbox"/> attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34. _____		<u>20 May 2010 (electronically)</u> Date	
NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.			

 *Total of 1 forms are submitted.

This collection of information is required by 37 CFR 41.31. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of
Sami Vaarala, Antti Nuopponen

Art Unit 2458
Confirmation No. 1571

Serial No. 10/500,930

CERTIFICATE OF MAILING

Filed: 19 October 2005

I HEREBY CERTIFY THAT THIS PAPER AND THE DOCUMENTS
REFERRED TO AS BEING ATTACHED OR ENCLOSED HERewith
ARE BEING SUBMITTED ELECTRONICALLY TO THE UNITED
STATES PATENT AND TRADEMARK OFFICE ON **20 May 2010**.

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

/rfasth/

Examiner: Towfighi, Afshawn

Rolf Fasth
Attorney for Applicant

Date: 20 May 2010

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) Notice of Appeal
- (X) The Commissioner is hereby authorized to charge any 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
26 Pinecrest Plaza, Suite 2
Southern Pines, NC 28387-4301

Telephone: 910-687-0001
Facsimile: 910-295-2152
Attorney Docket No. 290.1078APP

Electronic Patent Application Fee Transmittal

Application Number:	10500930
Filing Date:	19-Oct-2005
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:	290.1078USN

Filed as Small Entity

U.S. National Stage under 35 USC 371 Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Notice of appeal	2401	1	270	270

Post-Allowance-and-Post-Issuance:

Extension-of-Time:

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				270

Electronic Acknowledgement Receipt

EFS ID:	7649070
Application Number:	10500930
International Application Number:	
Confirmation Number:	1571
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:	290.1078USN
Receipt Date:	20-MAY-2010
Filing Date:	19-OCT-2005
Time Stamp:	07:05:50
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$270
RAM confirmation Number	8303
Deposit Account	060243
Authorized User	

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

Charge any Additional Fees required under 37 C.F.R. 1.492 (National application filing, search, and examination fees)

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

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

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

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Notice of Appeal Filed	sb0031.pdf	247902 5c802c126bffa3411e19022f32ac6edbb247aad8	no	2

Warnings:

Information:

2	Miscellaneous Incoming Letter	TRX.PDF	18264 0d322ca8ae2d8a3e5881f817bf48f78c79483296	no	1
---	-------------------------------	---------	---	----	---

Warnings:

Information:

3	Fee Worksheet (PTO-875)	fee-info.pdf	29689 9f717b7e1c5158750294d2bbe1a9308d76665f4a	no	2
---	-------------------------	--------------	---	----	---

Warnings:

Information:

Total Files Size (in bytes):

295855

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/500,930	10/19/2005	Sami Vaarala	290.1078USN	1571

33369 7590 05/28/2010

FASTH LAW OFFICES (ROLF FASTH)
26 PINECREST PLAZA, SUITE 2
SOUTHERN PINES, NC 28387-4301

EXAMINER

ART UNIT PAPER NUMBER

DATE MAILED: 05/28/2010

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

Notification of Non-Compliant Appeal Brief (37 CFR 41.37)	Application No. 10/500,930	Applicant(s) Vaarala, Sami	
	Examiner Towfighi, Afshawn	Art Unit 2458	

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

The Appeal Brief filed on 24 May 2010 is defective for failure to comply with one or more provisions of 37 CFR 41.37.

To avoid dismissal of the appeal, applicant must file an amended brief or other appropriate correction (see MPEP 1205.03) within **ONE MONTH or THIRTY DAYS** from the mailing date of this Notification, whichever is longer.
EXTENSIONS OF THIS TIME PERIOD MAY BE GRANTED UNDER 37 CFR 1.136.

1. The brief does not contain the items required under 37 CFR 41.37(c), or the items are not under the proper heading or in the proper order.
2. The brief does not contain a statement of the status of all claims, (e.g., rejected, allowed, withdrawn, objected to, canceled), or does not identify the appealed claims (37 CFR 41.37(c)(1)(iii)).
3. At least one amendment has been filed subsequent to the final rejection, and the brief does not contain a statement of the status of each such amendment (37 CFR 41.37(c)(1)(iv)).
4. (a) The brief does not contain a concise explanation of the subject matter defined in each of the independent claims involved in the appeal, referring to the specification by page and line number and to the drawings, if any, by reference characters; and/or (b) the brief fails to: (1) identify, for each independent claim involved in the appeal and for each dependent claim argued separately, every means plus function and step plus function under 35 U.S.C. 112, sixth paragraph, and/or (2) set forth the structure, material, or acts described in the specification as corresponding to each claimed function with reference to the specification by page and line number, and to the drawings, if any, by reference characters (37 CFR 41.37(c)(1)(v)).
5. The brief does not contain a concise statement of each ground of rejection presented for review (37 CFR 41.37(c)(1)(vi)).
6. The brief does not present an argument under a separate heading for each ground of rejection on appeal (37 CFR 41.37(c)(1)(vii)).
7. The brief does not contain a correct copy of the appealed claims as an appendix thereto (37 CFR 41.37(c)(1)(viii)).
8. The brief does not contain copies of the evidence submitted under 37 CFR 1.130, 1.131, or 1.132 or of any other evidence entered by the examiner **and relied upon by appellant in the appeal**, along with a statement setting forth where in the record that evidence was entered by the examiner, as an appendix thereto (37 CFR 41.37(c)(1)(ix)).
9. The brief does not contain copies of the decisions rendered by a court or the Board in the proceeding identified in the Related Appeals and Interferences section of the brief as an appendix thereto (37 CFR 41.37(c)(1)(x)).
10. Other (including any explanation in support of the above items):

The Summary of Claimed Subject Matter doesn't map independent claims 1, 22 & 27 to the specification by page, line number and to the drawings, the entire brief is not needed only the corrected section.

J. Dill, Paralegal
571-272-2983
Supervisory Paralegal: D. Perry
571-272-9797



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.
10/500,930	10/19/2005	Sami Vaarala	290.1078USN	1571
33369	7590	03/23/2010	EXAMINER	
FASTH LAW OFFICES (ROLF FASTH) 26 PINECREST PLAZA, SUITE 2 SOUTHERN PINES, NC 28387-4301			TOWFIGHI, AFSHAWN M	
			ART UNIT	PAPER NUMBER
			2458	
			NOTIFICATION DATE	DELIVERY MODE
			03/23/2010	ELECTRONIC

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

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

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

sloan.smith@fasthlaw.com
nan_russell@fasthlaw.com

Office Action Summary

Application No.	Applicant(s)	
10/500,930	VAARALA ET AL.	
Examiner	Art Unit	
AFSHAWN TOWFIGHI	2458	

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

Period for Reply

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

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

Status

- 1) Responsive to communication(s) filed on 29 October 2009.
- 2a) This action is **FINAL**. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-27 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-27 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

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

Attachment(s)

- | | |
|--|--|
| <p>1) <input type="checkbox"/> Notice of References Cited (PTO-892)</p> <p>2) <input type="checkbox"/> Notice of Draftperson's Patent Drawing Review (PTO-948)</p> <p>3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.</p> | <p>4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.</p> <p>5) <input type="checkbox"/> Notice of Informal Patent Application</p> <p>6) <input type="checkbox"/> Other: _____.</p> |
|--|--|

DETAILED ACTION

1. Claims 1-27 are pending.
2. Claims 1, 22, and 27 are amended.

Response to Arguments

3. Applicant's arguments filed 10/29/2009 have been fully considered but they are not persuasive.

On page 10 of the applicant's response, the applicant argues that Linnakangas teaches negotiating between a remote host and a router, and not negotiating the SA's between the remote host and local host or LAN.

The examiner respectfully disagrees with the applicant's response. Linnakangas teaches that IPsec is used to establish a secure connection between two endpoints (See par. 5, lines 1-6). Linnakangas teaches (See par 4) that IPsec has peer nodes negotiate and exchange keys to establish a secure connection between the two. Each computer does negotiate keys in order to establish a secure connection with other computers on the network. The computer does this via an intermediate computer (router). Once both computers have negotiated a keys using IPsec, then a secure connection between them exists. Inherently, data will be sent to/from each of the computers with each having a respective source/destination address of that secure

Art Unit: 2458

connection data path. As the claim language reads, the Linnakangas reference does teach the argued limitations.

On page 14 of the applicant's response, the applicant argues the examiner's interpretation of the IP forwarder as an intermediate computer, and that is simply a component of the router and not an intermediate computer. In addition, the examiner has not found a rationale for the combination within the cited references.

The examiner respectfully disagrees with the applicant's response. As stated above the router acts as an intermediate computer between the secure connection that exists between the two computers. The rationale for the combination of the references comes from a motivation that is obvious to one of ordinary skill in the art, and does not have to come from the cited references themselves. In this case, the examiner feels that increased security on a network is a motivation to combine one reference with another. Therefore, the cited references do teach the argued limitations.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States

Art Unit: 2458

only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

1. Claims 1-5, 7-10, 22-24, 26 & 27 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Application Publication No. 2001/0047487 to Linnakangas, et al. (Linnakangas).

Regarding claim 1, Linnakangas teaches a method for secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network(See paragraph 24, lines 4-8; wherein the local host 5 is the first computer, remote host 4 is the second computer, and router 2 is the intermediate computer), comprising: the first computer and the second computer negotiating and exchanging keys according to a key exchange protocol to establish a secure connection between the first computer and the second computer via the intermediate computer (See par 4 and "Response to Arguments) (See par. 24, lines 4-11; wherein message formation is inherent in "communication" and "exchanging user generated traffic"), the secure connection having a source address of the first computer as a first end point and a destination address of the second computer as a second end point of the secure connection (See par. 8, lines 1-5; wherein the destination of the packets is the second computer) in the first computer, forming a secure message by giving the secure message a first unique identity and a first destination address to the intermediate computer (See par.'s 4 & 24; wherein the SPI is the unique identity, and the header inherently includes the destination address), sending the secure message from the first computer to the intermediate computer (See par. 24, lines 4-6), the intermediate computer receiving the secure message and performing a translation by using the first

Art Unit: 2458

unique identity to find a second destination address to the second computer, (See par.'s 4 & 24; wherein a router that is able to perform IPsec and IKE translation, inherently includes a translation table), the intermediate computer substituting the first destination address with the second destination address to the second computer (See par.'s 4 & 24; wherein address substitution is a standard part of IPsec processing and IKE translation), the intermediate computer substituting the first unique identity with a second unique identity of the secure connection without establishing a new secure connection and without involving the second computer, (See par.'s 4 & 24; wherein generating and substituting SPI's is a standard part of IPsec processing and IKE translation; and, par. 8, lines 1-5; wherein a secure association, is the secure connection), and the intermediate computer forwarding the secure message with the second destination address and the second unique identity to the second computer in the secure connection (See par. 24, line 11).

2. Regarding claim 2, Linnakangas discloses forming the secure message in step b) by using an IPsec connection between the first computer and the second computer (See par. 24, lines 4-7).

3. Regarding claim 3, Linnakangas discloses performing a secure forwarding of the message by making use of SSL or TLS protocols (See par. 24, lines 4-7; wherein using a secure socket layer (SSL) is inherent in IPsec).

4. Regarding claim 4, Linnakangas discloses manually performing a preceding distribution of keys to components for forming the IPsec connection (See par. 40, lines

Art Unit: 2458

8-12; wherein manual distribution occurs when the IKE module is responding to a request).

5. Regarding claim 5, Linnakangas discloses performing a preceding distribution of keys for forming the IPSec connection by an automated key exchange protocol (See par. 40, lines 8-12; wherein automated key exchange occurs when the IKE module initiates negotiations).

6. Regarding claim 7, Linnakangas teaches sending the message that is sent from the first computer as a packet that contains message data, an inner IP header containing the actual sender and receiver addresses, an outer IP header containing the addresses of the first computer and the intermediate computer (See par. 3, lines 1-6).

7. Regarding claim 8, Linnakangas teaches the IPSec connection being one or more security associations (SA) and the unique identity being one or more SPI values (See par. 4, lines 5-14).

8. Regarding claim 9, Linnakangas teaches performing the matching in step d) by using a translation table stored at the intermediate computer (See par. 31, lines 1-6; wherein the IP forwarder module is part of the intermediate computer).

9. Regarding claim 10, Linnakangas teaches changing both the address and the SPI-value by the intermediate computer (See par. 24; wherein IPSec includes replacing addresses in accordance with the translation tables, and assigning a new SPI value to every received packet).

10. Regarding claim 22, Linnakangas teaches a telecommunication network for secure forwarding of messages, comprising: a first computer, a second computer and

Art Unit: 2458

an intermediate computer, means for negotiating and exchanging keys, according to a key exchange protocol, between the first computer and the second computer to establish a security association (See par 4 and "Response to Arguments) (See par. 24, lines 1-15; wherein local host 5 is the first computer, remote host 4 is the second computer, and router 2 is the intermediate computer), having a source address of the first computer as a first end point and a destination address of the second computer as a second end point (See par.'s 5, lines 1-6, and par. 8, lines 1-5), the first and the second computers having means for performing an IPSec processing, the intermediate computer having translation means for using translation tables to perform IPSec and IKE translation (See par. 14, lines 1-5) and for changing a destination address of the intermediate computer of a secure message to a destination address of the second computer, and the intermediate computer having means for forwarding the secure message received from the first computer to the second computer in the secure connection (See par. 8, lines 1-5).

11. Regarding claim 23, Linnakangas teaches the translation table for IPSec translation has IP addresses of the intermediate computer to be matched with IP addresses of the second computer (See par. 24, lines 4-6; wherein the router inherently has translation tables to perform IPSec).

12. Regarding claim 24, Linnakangas teaches the translation tables for IKE translation consists of two partitions, one for the communication between the first computer and the intermediate computer and another for the communication between the intermediate computer and the second computer (See par. 24, lines 4-8; wherein

Art Unit: 2458

the router (or intermediate computer) inherently includes at least two translation tables (or partitions), since one translation table is required for each IPSec connection, and there are at least two IPSec connections).

13. Regarding claim 26, Linnakangas teaches another translation table for IKE translation containing fields for matching a given user to a given second computer (See par. 24, lines 8-11; wherein each remote host must establish a new secure connection, which includes a new translation table).

14. Regarding claim 27, this claim recites a network for carrying out the method of claim 1, and is rejected for the same reasons.

Claim Rejections - 35 USC § 103

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

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

15. Claims 6, 11-14 & 20-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Linnakangas, as applied to claim 1 above, in view of Applicant's Admitted Prior Art (AAPA).

16. Regarding claim 6, Linnakangas teaches the invention as described in claim 5. Linnakangas does not teach performing the automated key exchange protocol used for the preceding distribution of keys for forming the IP Sec connection by means of a

Art Unit: 2458

modified IKE key exchange protocol between the first computer and the intermediate computer and by means of a standard IKE key exchange protocol between the intermediate computer and the second computer. However, AAPA teaches a modified IKE key exchange protocol between the first computer and the intermediate computer (See page 8, lines 27-29; wherein the key exchange is modified to support NAT traversal) and a standard IKE key exchange protocol between the intermediate computer and the second computer (See p. 8, lines 29-32).

Using the features of AAPA in the system of Linnakangas would have added flexibility by allowing different networks to connect to the system. Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention, to combine the teachings of AAPA and Linnakangas.

17. Regarding claim 11, Linnakangas teaches the invention as described in claim 1. Linnakangas does not teach the first computer being a mobile terminal, so that the mobility is enabled by modifying the translation table at the intermediate computer. However, AAPA teaches this limitation (See p. 7, lines 10-16).

Using the features of AAPA in the system of Linnakangas would have broadened the appeal and applicability of the system by allowing mobile units to connect to the network. Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention, to combine the teachings of AAPA and Linnakangas.

18. Regarding claim 12, Linnakangas, in view of AAPA, teach the invention as described in claim 11. Linnakangas further teaches performing the modification of the

Art Unit: 2458

translation tables by sending a request for registration of the new address from the first computer to the intermediate computer (See p. 3, par.'s 46-51).

19. Regarding claim 13, Linnakangas, in view of AAPA, teach the invention as described in claim 12. Linnakangas further teaches sending a reply to the request for registration from the intermediate computer to the first computer (See p. 3, par. 50).

20. Regarding claim 14, Linnakangas, in view of AAPA, teach the invention as described in claim 12. Linnakangas further teaches authenticating or encrypting by IPsec the request for registration and/or reply (See p. 3, par. 62).

21. Regarding claim 20, Linnakangas teaches the invention as described in claim 1. Linnakangas does not teach sending the secure message by using an IPsec transport mode. However, AAPA teaches this limitation (See p. 4, lines 14-19).

Using the features of AAPA in the system of Linnakangas would have added improved security to the system. Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention, to combine the teachings of AAPA and Linnakangas.

22. Regarding claim 21, Linnakangas teaches the invention as described in claim 1. Linnakangas does not teach sending the secure message by using an IPsec tunnel mode. However, AAPA teaches this limitation (See p. 4, lines 21-29).

Using the features of AAPA in the system of Linnakangas would have added improved security and flexibility to the system. Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention, to combine the teachings of AAPA and Linnakangas.

Art Unit: 2458

23. Claims 15-19 & 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Linnakangas, as applied to claims 4 & 24 above, in view of U.S. Patent Number 6,985,953 issued to Sandhu, et al. (Sandhu).

24. Regarding claim 15, Linnakangas teaches the invention as described in claim 4. Linnakangas further teaches establishing the key distribution for the secure connections by establishing an IKE protocol translation table, and using the translation table to modify IP addresses of IKE packets in the intermediate computer (See par. 24, lines 4-6). Linnakangas does not teach using the translation table to modify cookie values of IKE packets in the intermediate computer. However, Sandhu teaches this limitation (See col. 7, line 55 to col. 8, line 19; wherein the KDC is the intermediate computer).

Using the features of Sandhu in the system of Linnakangas would have added another layer of security within the secure connection. Therefore, it would have been obvious to one of ordinary skill, at the time of the invention, to combine the teachings of Sandhu and Linnakangas.

25. Regarding claim 16, Linnakangas in view of Sandhu teach the invention as described in claim 15. Linnakangas does not teach establishing the key exchange distribution by: generating an initiator cookie and sending a zero responder cookie to the second computer, generating a responder cookie in the second computer, and establishing a mapping between IKE cookie values in the intermediate computer. However, Sandhu teaches generating an initiator cookie and sending a zero responder cookie to the second computer (See col. 8, lines 41-47; wherein the Authenticator is the

Art Unit: 2458

initiator cookie), generating a responder cookie in the second computer (See col. 8, lines 41-47; wherein Bob's response is the responder cookie), and establishing a mapping between IKE cookie values in the intermediate computer (See col. 8, lines 49-51; wherein a mapping is required for authentication).

Using the features of Sandhu in the system of Linnakangas would have increased the number of security features available in the system. Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention, to combine the teachings of Sandhu and Linnakangas.

26. Regarding claim 17, Linnakangas in view of Sandhu teach the invention as is described in claim 15. Linnakangas further teaches modifying a IKE protocol between the first computer and the intermediate computer by transmitting the IKE keys from the first computer to the intermediate computer in order to decrypt and modify IKE packets (See par.'s 4 & 24; wherein the remote host 4 is an IPSec node that sends the IKE keys, and equates to applicant's first computer).

27. Regarding claim 18, Linnakangas in view of Sandhu teach the invention as is described in claim 15. Linnakangas further teaches carrying out the modification of the IKE packets by the first computer with the intermediate computer requesting such modifications (See par.'s 41-45; wherein the IKE module is in the intermediate computer).

28. Regarding claim 19, Linnakangas in view of Sandhu teach the invention as described in claim 17. Linnakangas further teaches defining the address so that the first computer is identified for the second computer by the intermediate computer by means

Art Unit: 2458

of an IP address taken from a pool of user IP addresses when forming the translation table (See par.'s 56 & 57).

29. Regarding claim 25, Linnakangas teaches the invention as described in claim 24. Linnakangas further teaches both partitions of the mapping table for IKE translation contains translation fields for a source IP address and a destination IP address between respective computers (See par. 24, lines 4-8; wherein source and destination addresses are inherent in IPSec). Linnakangas does not teach the mapping table for IKE translation contains translation fields for initiator and responder cookies between respective computers. However, Sandhu teaches a mapping table that contains translation fields for initiator and responder cookies between respective computers (See col. 8, lines 41-51; wherein the authenticator is the initiator cookie and Bob's response is the responder cookie).

Using the features of Sandhu in the system of Linnakangas would have provided increased security and insured that messages were transmitted to the correct destination. Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention, to combine the teachings of Sandhu and Linnakangas.

Conclusion

1. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

Art Unit: 2458

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

Any inquiry concerning this communication or earlier communications from the examiner should be directed to AFSHAWN TOWFIGHI whose telephone number is (571)270-7296. The examiner can normally be reached on Monday - Friday 8:00 A.M. to 5:00 P.M..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph E. Avellino can be reached on (571)272-3905. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2458

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.

/A. T./
Examiner, Art Unit 2458

/Joseph E. Avellino/
Supervisory Patent Examiner, Art Unit 2458

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 exchange\$3	US-PGPUB; USPAT	OR	OFF	2010/03/15 14:29

EAST Search History (Interference)

< This search history is empty >

3/ 15/ 2010 5:59:56 PM

C:\ Documents and Settings\ atowfighi\ My Documents\ EAST\ Workspaces\ jeff930.wsp

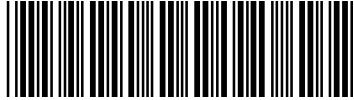
Search Notes 	Application/Control No. 10500930	Applicant(s)/Patent Under Reexamination VAARALA ET AL.
	Examiner Jeffrey Seto	Art Unit 2458

SEARCHED			
Class	Subclass	Date	Examiner
709	236, 229, 245	11-5-2008	JS

SEARCH NOTES		
Search Notes	Date	Examiner
Limited classification of 709/229, 245	11-5-2008	JS
Inventor search	11-5-2008	JS
Text search of EAST (US Pat, US PG Pub, JPO, EPO, Derwent)	11-5-2008	JS
Updated Text search of EAST (see attached history)	5-28-2009	JS
Updated text search of EAST (see attached history)	9-8-09	JS
EAST search with previous examiner's classes and focus on new limitations	3/15/2010	AT

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

--	--

Index of Claims 	Application/Control No. 10500930	Applicant(s)/Patent Under Reexamination VAARALA ET AL.
	Examiner Jeffrey Seto	Art Unit 2458

✓	Rejected
=	Allowed

-	Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

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

CLAIM		DATE							
Final	Original	10/28/2008	05/28/2009	09/08/2009	03/15/2010				
	1	✓	✓	✓	✓				
	2	✓	✓	✓	✓				
	3	✓	✓	✓	✓				
	4	✓	✓	✓	✓				
	5	✓	✓	✓	✓				
	6	✓	✓	✓	✓				
	7	✓	✓	✓	✓				
	8	✓	✓	✓	✓				
	9	✓	✓	✓	✓				
	10	✓	✓	✓	✓				
	11	✓	✓	✓	✓				
	12	✓	✓	✓	✓				
	13	✓	✓	✓	✓				
	14	✓	✓	✓	✓				
	15	✓	✓	✓	✓				
	16	✓	✓	✓	✓				
	17	✓	✓	✓	✓				
	18	✓	✓	✓	✓				
	19	✓	✓	✓	✓				
	20	✓	✓	✓	✓				
	21	✓	✓	✓	✓				
	22	✓	✓	✓	✓				
	23	✓	✓	✓	✓				
	24	✓	✓	✓	✓				
	25	✓	✓	✓	✓				
	26	✓	✓	✓	✓				
	27	✓	✓	✓	✓				

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Art Unit 2458

5 Sami Vaarala and Antti Nuopponen

Serial No. 10/500,930

10 Filed: 19 October 2005

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

15 Examiner: Jeffrey K. Seto

Date: 27 October 2009

Attorney Docket No. 290.1078USN

20

AMENDMENT

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

This is in response to the Office action of 16
September 2009. Please amend the above-identified patent
application as follows:

30

In the Claims:

Amend the claims as follows:

5

1. (Currently amended) A method for secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network, comprising:

10

the first computer and the second computer negotiating and exchanging keys according to a key exchange protocol to establishing a secure connection between the first computer and the second computer via the intermediate computer, ~~the secure connection extending between~~ the secure connection

15

having a source address of the first computer as a first end point and a destination address of the second computer as a second end point of the secure connection,

20

in the first computer, forming a secure message by giving the secure message a first unique identity and a first destination address to the intermediate computer, sending the secure message from the first computer to the intermediate computer,

25

the intermediate computer receiving the secure message and performing a translation by using the first unique identity to find a second destination address to the second computer, the intermediate computer substituting the first destination address with the second destination address to the second computer,

30

the intermediate computer substituting the first unique identity with a second unique identity of the secure connection without establishing a new secure connection and without involving the second computer, and

35

the intermediate computer forwarding the secure message with the second destination address and the second unique identity to the second computer in the secure connection.

2. (Previously presented) The method of claim 1 wherein the method further comprises forming the secure message by using an IPsec connection between the first computer and the second computer.

5

3. (Previously presented) The method of claim 1 wherein the method further comprises performing a secure forwarding of the message by making use of SSL or TLS protocols.

10

4. (Previously presented) The method of claim 2 wherein the method further comprises manually performing a preceding distribution of keys to components for forming the IPsec connection.

15

5. (Previously presented) The method of claim 2 wherein the method further comprises performing a preceding distribution of keys for forming the IPsec connection by an automated key exchange protocol.

20

6. (Previously presented) The method of claim 5 wherein the method further comprises performing the automated key exchange protocol used for the preceding distribution of keys for forming the IP Sec connection by means of a modified IKE key exchange protocol between the first computer and the intermediate computer and by means of a standard IKE key exchange protocol between the intermediate computer and the second computer.

25

7. (Previously presented) The method of claim 2 wherein the method further comprises sending the message that is sent from the first computer as a packet that contains message data, an inner IP header containing the actual sender and receiver addresses, an outer IP header containing the addresses of the first computer and the intermediate computer, the unique

35

identity.

8. (Previously presented) The method of claim 1 wherein the
method further comprises the IPsec connection being one or
5 more security associations (SA) and the unique identity being
one or more SPI values.

9. (Previously presented) The method of claim 1 wherein the
method further comprises performing the matching by using a
10 translation table stored at the intermediate computer.

10. (Previously presented) The method of claim 1 wherein the
method further comprises changing both the address and the
SPI-value by the intermediate computer.

15 11. (Previously presented) The method of claim 1 wherein the
method further comprises the first computer being a mobile
terminal so that the mobility is enabled by modifying the
translation table at the intermediate computer.

20 12. (Previously presented) The method of claim 11 wherein the
method further comprises performing the modification of the
translation tables by sending a request for registration of
the new address from the first computer to the intermediate
25 computer.

13. (Previously presented) The method of claim 12 wherein the
method further comprises sending a reply to the request for
registration from the intermediate computer to the first
30 computer.

14. (Previously presented) The method of claim 12 wherein the
method further comprises authenticating or encrypting by IPsec
the request for registration and/or reply.

35

15. (Previously presented) The method of claim 4 wherein the method further comprises establishing the key distribution for the secure connections by establishing an IKE protocol translation table, and using the translation table to modify
5 IP addresses and cookie values of IKE packets in the intermediate computer.

16. (Previously presented) The method of claim 15 wherein the method further comprises establishing the key exchange
10 distribution by:
generating an initiator cookie and sending a zero responder cookie to the second computer,
generating a responder cookie in the second computer,
establishing a mapping between IP addresses and IKE cookie
15 values in the intermediate computer, and
using the translation table to modify IKE packets in flight by modifying the external IP addresses and possibly IKE cookies of the IKE packets.

20 17. (Previously presented) The method of claim 15 wherein the method further comprises modifying a modified IKE protocol between the first computer and the intermediate computer by transmitting the IKE keys from the first computer to the intermediate computer in order to decrypt and modify IKE
25 packets.

18. (Previously presented) The method of claim 15 wherein the method further comprises carrying out in a modified IKE protocol between the first computer and the intermediate
30 computer the modification of the IKE packets by the first computer with the intermediate computer requesting such modifications.

19. (Previously presented) The method of claim 17 wherein the
35 method further comprises defining the address so that the

first computer is identified for the second computer by the intermediate computer by means of an IP address taken from a pool of user IP addresses when forming the translation table.

5 20. (Previously presented) The method of claim 1 wherein the method further comprises sending the secure message by using an IPSec transport mode.

10 21. (Previously presented) The method of claim 1 wherein the method further comprises sending the secure message by using an IPSec tunnel mode.

22. (Currently amended) A telecommunication network for secure forwarding of messages, comprising:
15 a first computer, a second computer and an intermediate computer,
means for negotiating and exchanging keys, according to a key exchange protocol, between the first computer and the second computer to establish a ~~having a secure connection~~ security association ~~therebetween via the intermediate computer, the~~ ~~secure connection~~ having a source address of the first computer as a first end point and a destination address of the second computer as a second end point,
the first and the second computers having means for performing
25 an IPSec processing,
the intermediate computer having translation means for using translation tables to perform IPSec and IKE translation and for changing a destination address of the intermediate computer of a secure message to a destination address of the
30 second computer, and
the intermediate computer having means for forwarding the secure message received from the first computer to the second computer in the security association ~~secure connection~~.

35 23. (Previously presented) The telecommunication network of

claim 22 wherein the translation table for IPsec translation has IP addresses of the intermediate computer to be matched with IP addresses of the second computer.

5 24. (Previously presented) The telecommunication network of claim 22 wherein the translation tables for IKE translation consists of two partitions, one for the communication between the first computer and the intermediate computer and another for the communication between the intermediate computer and
10 the second computer.

25. (Previously presented) The telecommunication network of claim 24 wherein both partitions of the mapping table for IKE translation contains translation fields for a source IP
15 address, a destination IP address, initiator and responder cookies between respective computers.

26. (Previously presented) The telecommunication network of claim 22 wherein there is another translation table for IKE translation containing fields for matching a given user to a
20 given computer.

27. (Currently amended) A telecommunication network for secure forwarding of messages, comprising:
25 a first computer,
a second computer,
an intermediate computer electronically connected to the first computer and the second computer,
means for negotiating and exchanging keys between the first
30 computer and the second computer to establish a ~~the first and the second computers having a secure connection between them via the intermediate computer,~~ the secure connection having a source address of the first computer as a first end point and a destination address of the second computer as a second end
35 point, and

the intermediate computer having means for performing translation between destination addresses and secure identities for forwarding secure messages received from the first computer to the second computer in the secure
5 connection.

REMARKS/ARGUMENTS

5 Reconsideration of the application is respectfully requested.
Claims 1-27 are pending in the present invention. No new
matter has been added to the application in this response.

10 1. Rejection of Claims 1-5, 7-10, 22-24 and 26-27 under 35
USC § 102(e).

Claims 1-5, 7-10, 22-24 and 26-27 were rejected under Section
102 as being anticipated by Linnakangas. This § 102 rejection
is respectfully traversed.

15

The independent claims 1, 22 and 27 have all been amended to
essentially require that the first computer and the second
computer negotiate and exchange keys, according to a key
exchange protocol, to establish a secure connection that has a
20 source address of the first computer as a first end point and
a destination address of the second computer as a second end
point of the secure connection.

25 It is respectfully submitted that Linnakangas completely fails
to teach or suggest this step of negotiation and exchange of
keys, according to a key exchange protocol, between the remote
hosts 4 and the local hosts 5. The local hosts 5 clearly do

not participate in the negotiation and exchange of keys whatsoever when the secure connection or security association is established between the remote hosts 4 and the router 2.

In contrast, Linnakangas expressly teaches in paragraph 0024
5 that each remote host 4 wishing to participate in the VPN must negotiate at least one pair of SAs (security associations) with the router 2 prior to exchanging user generated traffic with the LAN 5. In other words, the negotiation of to establish the SAs in Linnakangas is between the remote hosts 4
10 and the router 2 but NOT between the remote hosts 4 and the local hosts or LAN 5. This means the security association of Linnakangas has a source address of the host 4 as a first end point and a destination address of the router 2 as the second end point of the security association.

15

In view thereof, it is submitted that the anticipation rejection under Section 102 should be withdrawn and that the amended claim 1 is allowable over the cited reference.

20 1a. Dependent Claims 2-5 and 7-10

Claims 2-5, 7-10 are submitted to be allowable because the claims depend either directly or indirectly upon the allowable base claim 1 and because each claim includes limitations that
25 are not taught or suggested in the cited references.

2. The Requisite Limitations of Independent Claim 22 Are
Neither Taught Nor Suggested in the Cited Art.

As mentioned above, Linnakangas merely shows the establishment
5 of a secure connection between the remote host 4 and the
router 2 by negotiating security associations (SAs).

Applicants fails to see where Linnakangas teaches means for
negotiating and exchanging keys, according to a key exchange
protocol, between the remote host 4 (first computer) and the
10 local host 5 (second computer) to establish a security
association that has a source address of the remote host 4 as
a first end point and a destination address of the local host
5 as a second end point, as required by the amended claim 22.

In contrast, Linnakangas merely teaches the negotiation of
15 the security associations between the local host 4 and the
router 2, as expressly shown in paragraph 0024 of the
Linnakangas reference.

It is submitted that Linnakangas fails to teach or suggest all
20 the limitations of the amended claim 22. Therefore, the
anticipation rejection of claim 22 under § 102 is improper,
and should be removed.

2a. Dependent claims 23-24 and 26

25

Claims 23-24 and 26 are submitted to be allowable because the

claims depend either directly or indirectly upon the allowable base claim 22 and because each claim includes limitations that are not taught or suggested in the cited references.

5 3. The Requisite Limitations of Independent Claim 27 Are
Neither Taught Nor Suggested in the Cited Art.

Similar to claim 22, the amended claim 27 requires means for negotiating and exchanging keys between the first computer and
10 the second computer to establish a secure connection having a source address of the first computer as a first end point and a destination address of the second computer as a second end point. For reasons similar to the reasons put forth for the allowability of the amended claim 22 and claim 1 the amended
15 claim 27 is submitted to be allowable.

In summary, it is submitted that Linnakangas fails to teach or suggest all the limitations of the amended claim 27. Therefore, the anticipation rejection of claim 27 under § 102
20 is improper, and should be removed.

4. Rejection of Claims 6, 11-14 and 20-21 under 35 USC §
103(a).

25 Claims 6, 11-14 and 20-21 were rejected under Section 103 as being obvious over Linnakangas, as applied to claim 1 above,

in view of Applicant's Admitted Prior Art (AAPA). This § 103 rejection is respectfully traversed.

5 4a. The Requisite Steps of Claims 6, 11-14 and 20-21 Are Neither Taught Nor Suggested in the Cited Art.

10 Claims 6, 11-14 and 20-21 are submitted to be allowable because the claims depend either directly or indirectly upon the allowable base claim 1 and because each claim includes limitations that are not taught or suggested in the cited references. The section 103 rejection of the claims 6, 11-14 and 20-21 is also respectfully traversed because it is submitted the incorrect standard of obviousness has been used, as explained below.

15

5. Rejection of Claims 15-19 and 25 under 35 USC § 103(a).

20 Claims 15-19 and 25 were rejected under Section 103 as being obvious over Linnakangas in view of Sandhu. This rejection is respectfully traversed.

5a. The Requisite Steps of Claims 15-19 and 25 Are Neither Taught Nor Suggested in the Cited Art.

25 Claims 15-19 and 25 are submitted to be allowable because the claims depend either directly or indirectly upon the allowable

base claims 1 and 22, respectively, and because each claim includes limitations that are not taught or suggested in the cited references. The section 103 rejection of the claims 15-19 and 25 is also respectfully traversed because it is submitted that the incorrect standard of obviousness has been used, as explained below.

6. Comments Regarding Response To Arguments And the Applied Standard Of Obviousness

10

Applicants are very puzzled over the Examiner's interpretation that the IP forwarder is an intermediate computer. It should be pointed out that Fig. 2 illustrates the inside architecture of the router 2. Each box in Fig. 2 is thus a component of the router and not separate computers in a network. To assert that the IP forwarder is an intermediate computer that is somehow located inside the security association (between the end points of the security association) is respectfully submitted to be incorrect. The IP forwarder is merely a component of the router 2 which is, as explained above, the end point of the security association.

20

Applicants respectfully submit that the Examiner has applied the incorrect obviousness standard as illustrated in the last paragraph of page 3 and the first/second paragraphs of page 4. Applicants have not asserted that there is no rationale for

25