

the proposed combination in general. This is clearly not the obviousness standard set out by the courts. The Examiner seems to use his own subjective standard for what he thinks are good rationale for the combination without finding support
5 for the asserted rationale in the cited references.

Applicants submit that this subjective or personal standard of the Examiner is not what the courts have ruled to be the proper standard.

10 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
15 submitted that the Examiner has not factually supported the *prima facie* conclusion of obviousness. Applicants 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
20 "different computers, or different networks, to communicate with each other is always at the forefront of designer's mind." Additionally, applicants cannot find that the cited references mention that since "very sensitive information can be passed over an un-trusted network such as the Internet,
25 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 present Office Action, Applicants respectfully request reconsideration and withdrawal of this ground for rejection.

7. Conclusion

10

Based on the foregoing, Applicants respectfully request that the various grounds for rejection in the Office Action be reconsidered and withdrawn with respect to the previously amended form of the claims, and that a Notice of Allowance be issued for the present application to pass to issuance.

15

In the event any further matters remain at issue with respect to the present application, Applicants respectfully request that the Examiner please contact the undersigned below at the telephone number indicated in order to discuss such matter prior to the next action on the merits of this application.

20

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 **29 October**
2009.

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

Examiner: Jeffrey K. Seto

/rfasth/

Date: 29 October 2009

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 16 September 2009.
- (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 Docket No. 290.1078USN

Electronic Acknowledgement Receipt

EFS ID:	6351930
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:	29-OCT-2009
Filing Date:	19-OCT-2005
Time Stamp:	06:11:46
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		AMD.PDF	46431 <small>578dfbd84b58a1bc431d916ba45047b5d693cd1d</small>	yes	17

Multipart Description/PDF files in .zip description			
Document Description	Start	End	
Amendment/Req. Reconsideration-After Non-Final Reject	1	1	
Claims	2	8	
Applicant Arguments/Remarks Made in an Amendment	9	17	

Warnings:

Information:

2	Miscellaneous Incoming Letter	TRX.PDF	18290	no	1
			2b39e33e04a1935f680007763e6511bc8c8ec78		

Warnings:

Information:

Total Files Size (in bytes):			64721		
-------------------------------------	--	--	-------	--	--

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	10/29/2009	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:
 /ANNIE c. SINGLETON/

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	09/16/2009	EXAMINER	
FASTH LAW OFFICES (ROLF FASTH) 26 PINECREST PLAZA, SUITE 2 SOUTHERN PINES, NC 28387-4301			SETO, JEFFREY K	
			ART UNIT	PAPER NUMBER
			2458	
			NOTIFICATION DATE	DELIVERY MODE
			09/16/2009	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

DETAILED ACTION

1. Claims 1-27 are pending.

Continued Examination Under 37 CFR 1.114

2. 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 6-29-2009 has been entered.

Response to Arguments

3. Applicant's arguments filed 6-29-2009 have been fully considered but they are not persuasive. Regarding Applicant's argument that Linnakangas does not teach the intermediate computer uses the same secure connection without establishing a new secure connection and without involving the second computer. Linnakangas teaches an intermediate computer (IP forwarder) that receives packets and forwards the packets to their destination using a secure association (SA) (See paragraph 8, lines 1-5; wherein using the same secure association, is using the same secure connection).

Regarding Applicant's argument that there is no secure connection between local host 5 and router 2 in Linnakangas. Linnakangas teaches a method for providing Internet Protocol Security (IPSec) for communicating over un-trusted networks such as

Art Unit: 2458

the Internet 3 (See par.'s 1 & 2). Local host 5 and router 2 are both on a corporate Local Area Network (LAN) 1 (See par. 24, lines 1-3). Providing a secure connection between nodes on a private LAN is inherent and discussing such security would be repetitive. Linnakangas details the processing that goes on when traffic traverses the Internet, such as traffic between router 2 and remote host 4 (See par. 24, lines 3-8). While traffic between router 2 and remote host 4 is discussed in detail in Linnakangas, the destination of the traffic sent from remote host 4, is local host 5 (See par. 24, lines 6-7).

Regarding Applicant's argument that Linnakangas does not teach a secure connection extending between the 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. Linnakangas teaches that the establishment of a secure connection between a first end point and a second end point, wherein both end points are user terminals (See par. 5, lines 1-6). Linnakangas further teaches that the intermediate computer (or IP forwarder) receives packets from a source and forwards them to their destination, over a secure association (See par. 8, lines 1-5).

Regarding Applicant's argument that there is no rationale for combining Linnakangas and Applicant's Admitted Prior Art (AAPA). Both Linnakangas and AAPA deal with networking and providing secure connections between nodes. One of the most important factors that has shaped the computer and networking industry is compatibility. Allowing for different computers, or different networks, to communicate with each other is always at the forefront of designers' minds. Thus, adding flexibility by

Art Unit: 2458

allowing different networks to communicate is proper motivation for combining these related references.

Regarding Applicant's argument that there is no rationale for combining Linnakangas and Sandhu. Both Linnakangas and Sandhu deal with providing for secure communications over the Internet. 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. Sandhu provides an additional layer of security that can be used in the system of Linnakangas to make it harder for hackers to intercept and decode Internet traffic. Thus, sufficient motivation exists to combine Sandhu with Linnakangas.

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 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).

Art Unit: 2458

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: establishing a secure connection between the first computer and the second computer via the intermediate computer (See par. 24, lines 4-11; wherein message formation is inherent in “communication” and “exchanging user generated traffic”), the secure connection extending between 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 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

Art Unit: 2458

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 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).

Art Unit: 2458

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 an intermediate computer, the first and the second computers having a secure connection therebetween via the intermediate computer (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), 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 (See par.'s 5, lines 1-6, and par. 8, lines 1-5), the first

Art Unit: 2458

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 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).

Art Unit: 2458

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 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 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).

Art Unit: 2458

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.

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-

Art Unit: 2458

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 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.

Art Unit: 2458

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 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

Art Unit: 2458

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

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey Seto whose telephone number is (571)270-7198. The examiner can normally be reached on Monday thru Thursday and alt. Fridays, 9:30 AM-7 PM.

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.

JKS
9/8/2009

/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
L1	6	"864593".ap.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/08 14:57
L2	8386	709/236,229,245.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/08 15:49
L3	26813	"address translation" "translation table"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/08 15:50
L4	26865	l1and L3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/08 15:50
L5	773	l2 and L3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/08 15:50
L6	48	(chang\$3 modif\$4 replac\$5) near2 (cookie near value)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/08 15:51
L7	0	l5 and l6	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/08 15:51
L8	7237	lPsec	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/08 15:52

L9	7536	(IPsec "IP sec")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/08 15:53
L10	1393	I3 and I9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/08 15:53
L11	976163	(sa "secure association" "security association")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/08 15:53
L12	480	I10 and I11	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/08 15:53
L13	94557	(endpoint destination) and (router gateway firewall)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/08 15:55
L14	442	I12 and I13	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/08 15:55
S1	3407	destination near address near1 (computer network router gateway)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 14:52
S2	235	(substitut\$3 replac\$5) near address near1 (computer network router gateway)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 14:53
S3	1169	709/236.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 14:54

S4	6445	709/229,245.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 14:54
S5	294	(substitut\$3 replac\$5) near address near1 (destination)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 14:55
S6	7834	(substitut\$3 replac\$5) near address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 14:56
S7	1035190	SSL TLS	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 14:56
S8	29	S1 and (S2 S5 S6) and (S3 S4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 14:58
S9	2	S7 and S8	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 14:59
S10	207	(S2 S5 S6) and (S3 S4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 15:03
S11	931960	mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 15:04
S12	44	S10 and S11	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 15:04


S13	10	("20060045068" "6088725" "6415329" "20040049594" "20060209831").pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 17:09
S14	5	("20060045068" "6088725" "6415329" "20040049594" "20060209831").pn.	US-PGPUB; USPAT	OR	ON	2008/10/27 17:09
S15	336	"ip address" and (cookie near value)	US-PGPUB; USPAT	OR	ON	2008/10/27 17:10
S16	0	S14 and S15	US-PGPUB; USPAT	OR	ON	2008/10/27 17:10
S17	68244	"ip address" or (cookie near value)	US-PGPUB; USPAT	OR	ON	2008/10/27 17:10
S18	4	S14 and S17	US-PGPUB; USPAT	OR	ON	2008/10/27 17:10
S19	720	(cookie near value)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 17:14
S20	1169	709/236.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 17:15
S21	6445	709/229,245.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 17:15
S22	52	(S20 S21) and S19	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 17:15
S23	35	(chang\$3 modif\$4 replac\$5) near (cookie near value)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 17:18
S24	5	(S20 S21) and S23	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 17:19

S25	24067	"address translation" "translation table"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/28 12:27
S26	5	("20060045068" "6088725" "6415329" "20040049594" "20060209831").pn.	US-PGPUB; USPAT	OR	ON	2008/10/28 12:27
S27	3	S26 and S25	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/28 12:27
S28	0	("2001047487" "2001009025"). pn.	US-PGPUB; USPAT	OR	ON	2008/10/28 13:41
S29	2	("20010047487" "20010009025").pn.	US-PGPUB; USPAT	OR	ON	2008/10/28 13:42
S30	5	("6088725" "20020085561" "6377998" "6510154" "6415329").pn.	US-PGPUB; USPAT	OR	ON	2008/10/28 13:44
S31	8063	"address translation table" ((substitut\$3 replac\$6) near address)	US-PGPUB; USPAT	OR	ON	2008/10/28 13:50
S32	4	S30 and S31	US-PGPUB; USPAT	OR	ON	2008/10/28 13:51
S33	1753709	@pd>="20080901" @pppd>="20080901"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/05/28 12:20
S34	797	(cookie near value)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/05/28 12:21
S35	1237	709/236.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/05/28 12:21
S36	6961	709/229,245.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/05/28 12:21

S37	57	(S35 S36) and S34	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/05/28 12:21
S38	7	S37 and S33	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/05/28 12:21
S39	36	(chang\$3 modif\$4 replac\$5) near (cookie near value)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/05/28 12:21
S40	2	S39 and S33	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/05/28 12:21
S41	5	("6088725" "20020085561" "6377998" "6510154" "6415329").pn.	US-PGPUB; USPAT	OR	ON	2009/05/28 12:22
S42	8614	"address translation table" ((substitut\$3 replac\$6) near address)	US-PGPUB; USPAT	OR	ON	2009/05/28 12:22
S43	4	S41 and S42	US-PGPUB; USPAT	OR	ON	2009/05/28 12:22
S44	0	S43 and S33	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/05/28 12:22

9/ 8/ 2009 4:35:06 PM

C:\ Documents and Settings\ jseto\ My Documents\ EAST\ Workspaces\ 10500930.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

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					
	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	✓	✓	✓					

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL (Submitted Only via EFS-Web)

Application Number	10500930	Filing Date	2005-10-19	Docket Number (if applicable)	290.1078USN	Art Unit	2458
First Named Inventor	Sami Vaarala			Examiner Name	Jeffrey K. Seto		

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. The Instruction Sheet for this form is located at WWW.USPTO.GOV

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).

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.

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

Other _____

Enclosed

Amendment/Reply

Information Disclosure Statement (IDS)

Affidavit(s)/ Declaration(s)

Other _____

MISCELLANEOUS

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)

Other _____

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 any underpayment of fees, or credit any overpayments, to
Deposit Account No 060243 _____

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Patent Practitioner Signature

Applicant Signature

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.

Signature of Registered U.S. Patent Practitioner			
Signature	/rfasth/	Date (YYYY-MM-DD)	2009-06-29
Name	Rolf Fasth	Registration Number	36999

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.

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 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.

RF:ss 6/29/09

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
In re application of **EXPEDITED PROCEDURE UNDER 37
CFR 1.114**

Sami Vaarala, Antti Nuopponen Art Unit 2458
Confirmation No. 1571

Serial No. 10/500,930

CERTIFICATE OF MAILING

Filed: 19 October 2005

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

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 **29 June 2009**.

Examiner: Jeffrey K. Seto /rfasth/

Date: 29 June 2009 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 Final Office Action dated 1 June 2009.
- (X) Request for Continued Examination (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

Attorney Docket No. 290.1078USN

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

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:	5604452
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:	29-JUN-2009
Filing Date:	19-OCT-2005
Time Stamp:	14:42:58
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	919
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		AMD.PDF	58595 1c80f3831e2bca202b7b7a43b2d83a5ad279bf66	yes	23
Multipart Description/PDF files in .zip description					
	Document Description		Start		End
	Amendment Submitted/Entered with Filing of CPA/RCE		1		1
	Claims		2		7
	Applicant Arguments/Remarks Made in an Amendment		8		23
Warnings:					
Information:					
2	Request for Continued Examination (RCE)	RCE.PDF	36033 bf476b0cecc3a1440f660179cc0c76193829aa7c	no	3
Warnings:					
This is not a USPTO supplied RCE SB30 form.					
Information:					
3	Miscellaneous Incoming Letter	TRX.PDF	18898 1b8650942ef743629dae6d2c0445b91d7277a7a7	no	1
Warnings:					
Information:					
4	Fee Worksheet (PTO-875)	fee-info.pdf	29760 3c7e65f3077336ac33fe871b6d3ce3e9508c809f	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			143286		

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

10 Filed: 19 October 2005

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

15 Examiner: Jeffrey K. Seto

Date: 29 June 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 1 June
2009. Please amend the above-identified patent application as
follows:

30

In the Claims:

Amend the claims as follows:

5

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:

10

establishing a secure connection between the first computer and the second computer via the intermediate computer, the secure connection extending between 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 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,

25

the intermediate computer substituting the first unique identity with a second unique identity of the secure connection without establishing a new secure connection and

30

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 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
25 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 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 more security associations (SA) and the unique identity being one or more SPI values.

5

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 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.

5

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
10 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
15 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
20 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
25 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
30 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
35 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.

5

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

10

22. (Currently amended) A telecommunication network for secure forwarding of messages, comprising:

15

a first computer, a second computer and an intermediate computer, the first computer and the second computer having a secure connection 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,

20

the first and the second computers having means for performing an IPsec processing, ~~and~~

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 secure connection.

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.

35

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. (Currently amended) 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, 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 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.

35

REMARKS/ARGUMENTS

Reconsideration of the application is respectfully requested.

5 Claims 1-27 are pending in the present invention. No new matter has been added to the application in this response.

1. Rejection of Claims 1-5, 7-10, 22-24 and 26-27 under 35 USC § 102(e).

10

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

In summary, one problem with standard IPSec 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 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. One unique feature of the present invention is that the intermediate

20

25

computer modifies the addresses and SPI values of the same pre-existing secure connection i.e. without requiring the setting up of a new secure connection. In this way, a secure message sent from the first computer to the intermediate
5 computer may be modified 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 of a new secure connection and without involving the second computer.

10

a. The Requisite Steps of Independent Claim 1 Are Neither Taught Nor Suggested in the Cited Art.

15

Claim 1 has been amended to clarify that the secure connection extends between the source address of the first computer as the first end point of the secure connection and the destination address of the second computer as the second end point of the secure connection. The claim has also been modified to clarify that the intermediate computer substitutes
20 the first destination address with the second destination address and substitutes 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. No new matter has been added to the amended
25 claim 1 or any other claim. For example, support may be found on pages 12, 14, 17, 19-21 of the original patent

specification WO 03/063443. It is submitted that such steps are not taught or suggested in the cited references.

On page 3, paragraph 7, the Examiner refers to paragraph 4 and
5 paragraph 24, lines 4-8 of Linnakangas as teaching the step of
secure forwarding of a message from a first computer (local
host 5) to a second computer via an intermediate computer in a
telecommunication network. It should be noted that claim 1
has been amended to clarify that the end points of the secure
10 connection extend between the first computer and the second
computer. Claim 1 has also been amended to require that the
intermediate computer substitutes the first unique identity
with a second unique identity of the same secure connection
without establishing a new secure connection and without
15 involving the second computer.

Applicants submit that Linnakangas completely fails to teach
these additional steps and limitations. Linnakangas' IPsec is
only between the remote host 4 and the router 2. There is no
20 secure connection between the local host 5 and the router 2.
In contrast, the router 2 decrypts, reads and unwraps the
secure message from the remote host 4 to be able to determine
that the message is to be forwarded to the local host 5. This
forwarding is done without implementing IPsec. The Examiner
25 is respectfully requested to show where Linnakangas teaches
that the secure connection extends between the local host 5

and the router 2 also. On page 2, the Examiner writes that "a virtual private network is established to provide secure communication between host 4 and host 5, via router 2 (See par. 24, 4-8). Thus a secure communication is provided
5 between host 5 and router 2."

Linnakangas clearly fails to teach or suggest a secure connection that extends between the source address of the host 4 as a first end point and the destination address of the host
10 5 as the second end point of the secure connection.

Additionally, Linnakangas fails to teach the step of the router 2 substituting the first unique identity with the second unique identity of the secure connection without establishing a new secure connection and without involving the
15 second computer; and the router 2 forwarding the secure message to the second computer in the same secure connection.

In paragraph 24, lines 4-8, Linnakangas explains that "[b]y using IPsec to control communication between the router 2 and
20 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 a secure connection that has end points extending between the host 4 and the host 5. Additionally,
25 "controlling" communication across the route from remote host 4 via router 2 all the way to host 5 does not mean here that

there is a secure connection also between router 2 and host 5. Linnakangas merely mentions controlling the communication, not securing. In other words, the IPSec, defined in the foregoing sentence in Linnakangas as being between the host 4 and the
5 router 2, controls what traffic goes therebetween. The traffic from the host 4 to host 5 goes via this IPSec connection between the host 4 and router 2. It should be noted that the virtual private network in Linnakangas is not secured but merely controlled. There is not really as much
10 need for a secure connection between the router 2 and the host 5 since the connection is within the same LAN. Wikipedia states that a virtual private network (VPN) is a computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger
15 networks (such as the Internet), as opposed to running across a single private network. The Link Layer protocols of the virtual network are said to be tunneled through the transport network. One common application is to secure communications through the public Internet, but a VPN does not need to have
20 explicit security features such as authentication or content encryption and is quite different from a secure connection such as a security association.

Applicants also would like to draw the Examiner's attention to
25 the fact that, in the cited Linnakangas paragraph, the establishment of the secure connection between remote host 4

and router 2 is quite well described, including the exchange of keys etc. However, there is nowhere described any security connection formed between router 2 and host 5, because there is no security connection between router 2 and host 5.

5 Paragraph 24 of Linnakangas merely teaches the remote host 4 negotiating secure associations with the router 2 (lines 9-10 of paragraph 24). There is nothing about forming a secure message in the local host 5 or negotiating secure associations with the local host 5. Even if the communication between the
10 router 2 and the host 5 may be considered quite safe and secure, Linnakangas still completely fails to teach or suggest establishing a secure connection that extends between a source address of the host 4 as a first end point and the destination address of the host 5 as the second end point of the same
15 secure connection.

Applicants cannot see that Linnakangas teaches the required steps of establishing a secure connection between the first computer and the second computer wherein the secure connection
20 extends between 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.

It is submitted that Linnakangas also fails to teach or
25 suggest the step of the intermediate computer, while being in a secure connection between the first computer and the second

computer as required in the first paragraph of the amended claim 1, the intermediate computer substituting the first unique identity with a second unique identity of the same 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 same secure connection.

10 It is submitted that Linnakangas completely fails to teach or suggest the above-outlined steps. Therefore, the rejection of claim 1 under § 102 is improper, and should be removed.

b. Dependent Claims 2-5 and 7-10

15

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 are not taught or suggested in the cited references.

20

2. The Requisite Limitations of Independent Claim 22 Are Neither Taught Nor Suggested in the Cited Art.

As mentioned above, Linnakangas merely shows a secure connection between the remote host 4 and the router 2. Applicants fails to see where Linnakangas teaches a secure

connection that has a source address of the host 4 (the first computer) as a first end point and a destination address of the local host 5 (the second computer) as a second end point. In contrast, the secure connection of Linnakangas merely
5 extends between the host 4 and the router 2. Additionally, Linnakangas fails to teach or suggest means for forwarding the secure message received from the first computer to the second computer in the secure connection. In contrast, Linnakangas merely describes a router 2 that forwards a message in a VPN
10 and an IPsec with end points at the host 4 and the router 2 (but not at the host 5).

It is submitted that Linnakangas fails to teach or suggest all the limitations of the amended claim 22. Therefore, the
15 anticipation rejection of claim 22 under § 102 is improper, and should be removed.

a. Dependent claims 23-24 and 26

20 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.

25 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 a secure connection 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 amended claim 27 also requires that the intermediate computer has means for forwarding the secure messages received from the first computer to the second computer in the secure connection. The amended claim 27 is submitted to be allowable for reasons similar to the reasons put forth for the allowability of the amended claim 1 and claim 22.

It is submitted that Linnakangas fails to teach or suggest all the limitations of the amended claim 27. Therefore, the rejection of claim 27 under § 102 is improper, and should be removed.

4. Rejection of Claims 6, 11-14 and 20-21 under 35 USC § 103(a).

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 in part and overcome in part as follows:

a. The Requisite Steps of Claims 6, 11-14 and 20-21 Are
Neither Taught Nor Suggested in the Cited Art.

5 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.

10 The § 103 rejection is therefore improper and should be
withdrawn.

b. Prima Facie Support for Combination Under § 103 Not
Provided

15
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
20 M.P.E.P. § 2142 has not been provided in the present Office
Action.

As provided in M.P.E.P. § 2142, the Supreme Court in *KSR
International v. Teleflex Inc.*, 82 USPQ2d 1385, 1396 (2007)
25 specified that the analysis supporting a rejection under 35
U.S.C. § 103 should be made explicit. “[R]jections 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
5 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
10 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,
15 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). It seems that the Examiner has completely ignored the arguments put forth in the
20 previous response regarding the Examiner's failure to establish a *prima facie* case of obviousness. Applicants request the Examiner to consider all of the arguments of this response instead of simply copying text from the previous Office action.

25

The Examiner has again merely provided one benefit, or

advantage of the modification as the only rationale provided in the Office Action in support of the instant rejection.

5 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
10 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
15 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.

20 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." Because a *prima facie* conclusion of
25 obviousness has not been provided in the present Office Action, Applicants respectfully request reconsideration and

withdrawal of this ground for rejection as to claim 6.

Similarly, no articulated reasoning is provided for the rejections of claims 11-14 and 20-21. On page 8, lines 5-7, the Examiner merely states it would have been obvious because it "would have broadened the appeal and applicability of the system by allowing mobile units to connect to the network" (emphasis added). On page 9, lines 1-2 and 8-9 of the Office action it is stated that the combination would have been obvious because it "would have added improved security to the system" (emphasis added). It is submitted that none of the above stated general benefits provides the required articulated reasoning to show *prima facie* conclusion of obviousness.

15

The rejections of claims 6, 11-14 and 20-21 under Section 103 are therefore improper and should be removed.

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.

25

a. The Requisite Steps of Claims 15-19 and 25 Are Neither Taught Nor Suggested in the Cited Art.

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 § 103 rejection is therefore improper and should be withdrawn.

10 b. Prima Facie Support for Combination Under § 103 Not Provided

These rejections also lack the required articulated reasoning to establish *prima facie* conclusion of obviousness. The only reasons for obviousness are stated on page 9, last line ("would have added another layer of security within the secure connection" (emphasis added)) and page 10, line 15 ("would have increased the number of security features available in the system" (emphasis added)) are again submitted to be mere general benefits that do not provide the required articulated reasoning to meet the burden of establishing a *prima facie* conclusion of obviousness. Page 12, lines 2-3, of the Office action states that the proposed combination is obvious because it "would have provided increased security and insured that messages where transmitted to the correct destination" (emphasis added). It is assumed that the Examiner meant that

messages "were" transmitted to the correct destination. Again the above statements fail to establish the prima facie case of obviousness since they merely mention benefits and advantages of the proposed combination, as explained above.

5

The rejections of claims 15-19 and 25 under Section 103 are therefore improper and should be removed.

6. Conclusion

10

Based on the foregoing, Applicants respectfully request that the various grounds for rejection in the Office Action be reconsidered and withdrawn with respect to the previously amended form of the claims, and that a Notice of Allowance be
15 issued for the present application to pass to issuance.

20

In the event any further matters remain at issue with respect to the present application, Applicants respectfully request that the Examiner please contact the undersigned below at the
20 telephone number indicated in order to discuss such matter prior to the next action on the merits of this application.

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

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	06/29/2009	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".
 The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
 /PATSY ZIMMERMAN/

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 06/01/2009
FASTH LAW OFFICES (ROLF FASTH)
26 PINECREST PLAZA, SUITE 2
SOUTHERN PINES, NC 28387-4301

EXAMINER

SETO, JEFFREY K

ART UNIT	PAPER NUMBER
----------	--------------

2458

MAIL DATE	DELIVERY MODE
-----------	---------------

06/01/2009

PAPER

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.

DETAILED ACTION

1. Claims 1-27 are pending.

Response to Amendment

2. In response to the amendment filed 1-17-09:
 - a. The objections to claims 1, 17 & 18 are withdrawn; and,
 - b. The rejection of claim 26 under 35 USC 112, 2d paragraph is withdrawn.

Response to Arguments

3. Applicant's arguments filed 1-17-09 have been fully considered but they are not persuasive. In regards to Applicant's argument that Linnakangas only teaches a secure connection between host 4 and router 2, and does not teach a secure connection between host 5 and router 2. Linnakangas teaches that a virtual private network is established to provide secure communications between host 4 and host 5, via router 2 (See par. 24, 4-8). Thus, a secure connection is provided between host 5 and router 2.
4. Regarding Applicant's argument that Linnakangas delivers "plain text" from the router 2 to the host 5. The Examiner has fully reviewed Linnakangas and found no teaching in the reference supporting this assertion.

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:

Art Unit: 2458

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.

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).
2. 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: establishing a secure connection between the first computer and the second computer via the intermediate computer (See par. 24, lines 4-11; wherein message formation is inherent in “communication” and “exchanging user generated traffic”), 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 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

Art Unit: 2458

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, (See par.'s 4 & 24; wherein generating and substituting SPI's is a standard part of IPsec processing and IKE translation), and the intermediate computer forwarding the secure message with the second destination address and the second unique identity to the second computer (See par. 24, line 11).

3. 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).

4. 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).

5. Regarding claim 4, Linnakangas discloses manually performing a preceding distribution of keys to components for forming the IPsec connection (See par. 40, lines 8-12; wherein manual distribution occurs when the IKE module is responding to a request).

6. 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).

Art Unit: 2458

7. 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).

8. 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).

9. 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).

10. 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).

11. Regarding claim 22, Linnakangas teaches a telecommunication network for secure forwarding of messages, comprising: a first computer, a second computer and an intermediate computer, the first and the second computers having a secure connection therebetween via the intermediate computer, the first and the second computers having means for performing an IPSec processing, and the intermediate computer having translation tables to perform IPSec and IKE translation (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).

Art Unit: 2458

12. 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).

13. 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 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).

14. 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).

15. 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:

Art Unit: 2458

(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.

16. 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).

17. 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 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.

18. 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

Art Unit: 2458

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.

19. Regarding claim 12, Linnakangas, in view of AAPA, teach the invention as described in claim 11. Linnakangas further teaches 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 p. 3, par.'s 46-51).

20. 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).

21. 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).

22. 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

Art Unit: 2458

ordinary skill in the art, at the time of the invention, to combine the teachings of AAPA and Linnakangas.

23. 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.

24. 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).

25. 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

Art Unit: 2458

obvious to one of ordinary skill, at the time of the invention, to combine the teachings of Sandhu and Linnakangas.

26. 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 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.

27. 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

Art Unit: 2458

(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).

28. 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).

29. 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 of an IP address taken from a pool of user IP addresses when forming the translation table (See par.'s 56 & 57).

30. 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

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

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

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey Seto whose telephone number is (571)270-7198. The examiner can normally be reached on Monday thru Thursday and alt. Fridays, 9:30 AM-7 PM.

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

Art Unit: 2458

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.

JKS
5/28/2009

/Joseph E. Avellino/
Supervisory Patent Examiner, Art Unit 2458

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1753709	@pd>="20080901" @pppd>="20080901"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/05/28 12:20
L2	797	(cookie near value)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/05/28 12:21
L3	1237	709/236.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/05/28 12:21
L4	6961	709/229,245.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/05/28 12:21
L5	57	(L3 L4) and L2	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/05/28 12:21
L6	7	L5 and l1	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/05/28 12:21
L7	36	(chang\$3 modif\$4 replac\$5) near (cookie near value)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/05/28 12:21
L8	2	L7 and l1	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/05/28 12:21
L9	5	("6088725" "20020085561" "6377998" "6510154" "6415329").pn.	US-PGPUB; USPAT	OR	ON	2009/05/28 12:22

L10	8614	"address translation table" ((substitut\$3 replac\$6) near address)	US-PGPUB; USPAT	OR	ON	2009/05/28 12:22
L11	4	L9 and L10	US-PGPUB; USPAT	OR	ON	2009/05/28 12:22
L12	0	L11 and I1	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/05/28 12:22
S1	3407	destination near address near1 (computer network router gateway)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 14:52
S2	235	(substitut\$3 replac\$5) near address near1 (computer network router gateway)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 14:53
S3	1169	709/236.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 14:54
S4	6445	709/229,245.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 14:54
S5	294	(substitut\$3 replac\$5) near address near1 (destination)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 14:55
S6	7834	(substitut\$3 replac\$5) near address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 14:56
S7	1035190	SSL TLS	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 14:56

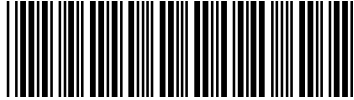
S8	29	S1 and (S2 S5 S6) and (S3 S4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 14:58
S9	2	S7 and S8	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 14:59
S10	207	(S2 S5 S6) and (S3 S4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 15:03
S11	931960	mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 15:04
S12	44	S10 and S11	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 15:04
S13	10	("20060045068" "6088725" "6415329" "20040049594" "20060209831").pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 17:09
S14	5	("20060045068" "6088725" "6415329" "20040049594" "20060209831").pn.	US-PGPUB; USPAT	OR	ON	2008/10/27 17:09
S15	336	"ip address" and (cookie near value)	US-PGPUB; USPAT	OR	ON	2008/10/27 17:10
S16	0	S14 and S15	US-PGPUB; USPAT	OR	ON	2008/10/27 17:10
S17	68244	"ip address" or (cookie near value)	US-PGPUB; USPAT	OR	ON	2008/10/27 17:10
S18	4	S14 and S17	US-PGPUB; USPAT	OR	ON	2008/10/27 17:10
S19	720	(cookie near value)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 17:14

S20	1169	709/236.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 17:15
S21	6445	709/229,245.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 17:15
S22	52	(S20 S21) and S19	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 17:15
S23	35	(chang\$3 modif\$4 replac\$5) near (cookie near value)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 17:18
S24	5	(S20 S21) and S23	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 17:19
S25	24067	"address translation" "translation table"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/28 12:27
S26	5	("20060045068" "6088725" "6415329" "20040049594" "20060209831").pn.	US-PGPUB; USPAT	OR	ON	2008/10/28 12:27
S27	3	S26 and S25	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/28 12:27
S28	0	("2001047487" "2001009025"). pn.	US-PGPUB; USPAT	OR	ON	2008/10/28 13:41
S29	2	("20010047487" "20010009025").pn.	US-PGPUB; USPAT	OR	ON	2008/10/28 13:42
S30	5	("6088725" "20020085561" "6377998" "6510154" "6415329").pn.	US-PGPUB; USPAT	OR	ON	2008/10/28 13:44
S31	8063	"address translation table" ((substitut\$3 replac\$6) near address)	US-PGPUB; USPAT	OR	ON	2008/10/28 13:50

S32	4	S30 and S31	US-PGPUB; USPAT	OR	ON	2008/10/28 13:51
-----	---	-------------	--------------------	----	----	---------------------

5/ 28/ 2009 12:22:22 PM

C:\ Documents and Settings\ jseto\ My Documents\ EAST\ Workspaces\ 10500930.wsp

Index of Claims 	Application/Control No. 10500930	Applicant(s)/Patent Under Reexamination VAARALA ET AL.
	Examiner Jeffrey Seto	Art Unit 2446

✓	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						
	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	✓	✓						

Search Notes 	Application/Control No. 10500930	Applicant(s)/Patent Under Reexamination VAARALA ET AL.
	Examiner Jeffrey Seto	Art Unit 2446

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

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

--	--

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Art Unit 2446

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: 17 January 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 12
November 2008. 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,
10 comprising:
establishing a secure connection between the first computer and the second computer via the intermediate computer,
~~a) forming a message in the first computer or in a computer that is served by the first computer, and in the latter case sending the message to the first computer,~~
15 ~~b)~~ 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,
~~e)~~ sending the secure message from the first computer to the
20 intermediate computer,
~~d)~~ the intermediate computer receiving the secure message and performing a translation by using said destination address and the first unique identity to find an a second destination address to the second computer,
25 ~~e)~~ the intermediate computer substituting the current first destination address with the found second destination address to the second computer,
~~f)~~ the intermediate computer substituting the first unique identity with another a second unique identity, and
30 ~~g)~~ the intermediate computer forwarding the secure message with the second substituted-current destination address and the second substituted unique identity to the second computer.

2. (Currently amended) The method of claim 1 wherein the
35 method further comprises forming the secure message ~~in step b)~~

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
25 second computer.

30 7. (Currently amended) The method of claim 2 wherein the method further comprises sending the message that is sent from the first computer ~~in step e)~~ 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.

35 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.

5 9. (Currently amended) The method of claim 1 wherein the method further comprises performing the matching ~~in step d)~~ by using a translation table stored at the intermediate computer.

10 10. (Currently amended) The method of claim 1 wherein the method further comprises changing both the address and the SPI-value by the intermediate computer ~~in steps e) and f)~~.

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 computer.

25 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.

30 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 IP addresses and cookie values of IKE packets in the intermediate computer.

5 16. (Currently amended) 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,
10 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
15 of the IKE packets.

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

18. (Currently amended) The method of claim 15 wherein the
25 method further comprises carrying out in ~~the~~ 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.

30 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
35 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.

5

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

10 22. (Currently amended) A telecommunication network for secure forwarding of messages, comprising:

~~at least~~ a first computer, a second computer and an intermediate computer, the first computer and the second computer having a secure connection therebetween via the intermediate computer,

15

the first and the second computers having means for performing an IPSec processing, and the intermediate computer having translation tables to perform IPSec and IKE translation.

20

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.

25

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.

30

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

35

address, a destination IP address, initiator and responder cookies between respective computers.

5 26. (Currently amended) 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 ~~second~~ computer.

10 27. (New) 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, the first and the second
15 computers having a secure connection between them via the intermediate computer, and
the intermediate computer having means for performing translation between destination addresses and secure identities for forwarding secure messages received from the
20 first computer to the second computer.

25

REMARKS/ARGUMENTS

5 Reconsideration of the application is respectfully requested.
Claims 1-27 are pending in the present invention. Claim 27
has been added. The new claim 27 is, for example, supported
on page 19, lines 23 - 25; page 13, lines 30 - 32; page 17,
lines 8 - 10, 15 - 16 and 30 - 32; and page 18, lines 1 - 2.
10 No new matter has been added to the application in this
response.

1. Rejection of Claims 1-5, 7-10, 22-24 and 26 under 35 USC §
102(e).

15 Claims 1-5, 7-10, 22-24 and 26 were rejected under Section 102
as being anticipated by Linnakangas. This § 102 rejection is
respectfully traversed.

20 In summary, an important feature of the present invention is
that a secure message may be sent from a first computer to a
second computer even when there is an intermediate computer
therebetween that is part of the same secure connection.

25 a. The Requisite Steps of Independent Claim 1 Are Neither
Taught Nor Suggested in the Cited Art.

Claim 1 has been amended to clarify that the intermediate computer uses the first unique identity to find a second destination address to the second computer. The claim has also been modified to clarify that the intermediate computer
5 substitutes the first destination address with the second destination address and substitutes the first unique identity with a second unique identity prior to sending the secured message to the second computer. No new matter has been added to the amended claim 1 or any other claim. Such steps are not
10 taught or suggested in the cited references.

On page 3, paragraph 7, the Examiner refers to paragraph 24, lines 4-8 as teaching the step of secure forwarding of a message from a first computer (local host 5) to a second
15 computer via an intermediate computer in a telecommunication network. Applicants disagree. Linnakangas completely fails to teach a secure forwarding from the local host 5. The IPSec is only between the remote host 4 and the router 2. There is no secure connection between the local host 5 and the router
20 2. In contrast, the router 2 decrypts, reads and unwraps the secure message from the remote host 4 to be able to determine that the message is to be forwarded (as plain text) to the local host 5. This forwarding is done without implementing IPSec. The Examiner is respectfully requested to show where
25 Linnakangas teaches a secure connection between the local host 5 and the router 2.

The amended claim 1 also requires the step of establishing a secure connection between the first computer and the second computer via the intermediate computer. As indicated above,
5 Linnakangas completely fails to teach or suggest this step.

On page 4, lines 1-4, of the Office action, the Examiner asserts that Linnakangas teaches forming a secure message in the first computer (local host 5). Applicants disagree.
10 Applicants fail to see where Linnakangas is teaching this step. Paragraph 24 of Linnakangas merely teaches the remote host 4 negotiating secure associations with the router 2 (line 9-10 of paragraph 24). There is nothing about forming a secure message in the local host 5 or negotiating secure
15 associations with the local host 5.

On page 4, lines 4-6, of the Office action, the Examiner asserts that Linnakangas teaches the step of sending the secure message from the first computer to the intermediate
20 computer. Applicants disagree. Since the local host 5 does not form any secure message no secure message can be sent from the local host 5. Lines 4-6 of the Office action state "[b]y using IPsec to control communication between the router 2 and the remote hosts 4 (and hence between remote hosts 4 and local
25 hosts 5)." It is important to note that the IPsec is only between the router 2 and the hosts 4.

Applicants cannot see that Linnakangas teaches the required steps of the local host forming a secure message and sending the secure message to the intermediate computer in the cited
5 lines 4-6.

It is submitted that Linnakangas also fails to teach or suggest the step of the intermediate computer, while being in a secure connection between the first computer and the second
10 computer as required in the first paragraph of the amended claim 1, receiving the secure message and performing a translation by using the first unique identity to find a second destination address to the second computer.

Linnakangas router fails to teach the step of receiving a
15 secure message from the local host 5 since the secure connection is only between the router 2 and the remote host 4. As indicated above, no secure messages are sent from the local host 5 to the router 2 since there is no secure connection therebetween. Consequently Linnakangas router 2 also fails to
20 substituting the first address of the secure connection with the second destination address of the same secure connection and substituting the first unique identity with the second unique identity. Finally, Linnakangas fails to teach or suggest the router 2 forwarding the secure message to the
25 second computer since the router 2 never received a secure message from the local host 5 and it is therefore not possible

to forward any secure message.

It is submitted that Linnakangas completely fails to teach or suggest the above-outlined steps. Therefore, the rejection of claim 1 under § 102 is improper, and should be removed.

b. 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 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 a secure connection between the remote host 4 and the router 2 and an un-secure plain text connection between the router 2 and the local host 5. Applicants fails to see where Linnakangas teaches that the local host 5 (first computer) has means for performing an IPSsec processing as mentioned on page 6, lines 1-2 of the current Office action. The Examiner refers to paragraph 24, lines 1-15 of Linnakangas. The cited text section merely teaches "using IPSsec to control communication between the router 2 and the remote hosts 4" and that each

“remote host 4 wishing to participate in the VPN must negotiate at least one pair of SAs (one for sending and one for receiving data) with the router 2 prior to exchanging user generated traffic with the LAN 5.” There is nothing about a
5 secure association between the router 2 and the LAN 5.

The amended claim 22 has now been amended to require that there is a secure connection between the first computer and the second computer via the intermediate computer. It is
10 again submitted that Linnakangas fails to teach or suggest a secure connection between the remote host 4 and the local host 5.

It is submitted that Linnakangas fails to teach or suggest all
15 the limitations of the amended claim 22. Therefore, the anticipation rejection of claim 22 under § 102 is improper, and should be removed.

a. Dependent claims 23-24 and 26

20 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.

25

3. The Requisite Limitations of Independent Claim 27 Are

Neither Taught Nor Suggested in the Cited Art.

5 Similar to claim 22, the new claim 27 requires a secure connection between the first computer and the second computer via the intermediate computer. As indicated above, Linnakangas fails to teach or suggest a secure connection between the remote host 4 and the local host 5.

10 It is submitted that Linnakangas fails to teach or suggest all the limitations of the amended claim 27. Therefore, the rejection of claim 27 under § 102 is improper, and should be removed.

15 4. Rejection of Claims 6, 11-14 and 20-21 under 35 USC § 103(a).

20 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 in part and overcome in part as follows:

25 a. The Requisite Steps of Claims 6, 11-14 and 20-21 Are Neither Taught Nor Suggested in the Cited Art.

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.

5

The § 103 rejection is therefore improper and should be withdrawn.

10 b. Prima Facie Support for Combination Under § 103 Not Provided

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 present Office Action.

20 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]jections 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). Thus, one benefit, or advantage of the modification is 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
5 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
10 obviousness. If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness." Because a *prima facie* conclusion of obviousness has not been provided in the present Office Action, Applicants respectfully request reconsideration and
15 withdrawal of this ground for rejection as to claim 6.

Similarly, no articulated reasoning is provided for the rejections of claims 11-14 and 20-21. On page 8, lines 5-7, the Examiner merely states it would have been obvious because
20 it "would have broadened the appeal and applicability of the system by allowing mobile units to connect to the network" (emphasis added). On page 9, lines 1-2 and 8-9 of the Office action it is stated that the combination would have been obvious because it "would have added improved security to the
25 system" and it "would have added improved security and flexibility to the system" (emphasis added). It is submitted

that none of the above stated general benefits provides the required articulated reasoning to show *prima facie* conclusion of obviousness.

5 The rejections of claims 6, 11-14 and 20-21 under Section 103 are therefore improper and should be removed.

5. Rejection of Claims 15-19 and 25 under 35 USC § 103(a).

10 Claims 15-19 and 25 were rejected under Section 103 as being obvious over Linnakangas in view of Sandhu. This rejection is respectfully traversed.

15 a. The Requisite Steps of Claims 15-19 and 25 Are Neither Taught Nor Suggested in the Cited Art.

20 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 § 103 rejection is therefore improper and should be withdrawn.

25

b. Prima Facie Support for Combination Under § 103 Not Provided

These rejections also lack the required articulated reasoning to establish *prima facie* conclusion of obviousness. The only reasons for obviousness are stated on page 10, line 2 ("would
5 have added another layer of security within the secure connection" (emphasis added)) and page 10, line 17 ("would have increased the number of security features available in the system" (emphasis added)) are again submitted to be mere general benefits that do not provide the required articulated
10 reasoning to meet the burden of establishing a *prima facie* conclusion of obviousness.

The rejections of claims 15-19 and 25 under Section 103 are therefore improper and should be removed.

15

3. Conclusion

Based on the foregoing, Applicants respectfully request that the various grounds for rejection in the Office Action be
20 reconsidered and withdrawn with respect to the previously amended form of the claims, and that a Notice of Allowance be issued for the present application to pass to issuance.

In the event any further matters remain at issue with respect
25 to the present application, Applicants respectfully request that the Examiner please contact the undersigned below at the

RF Attorney Docket No. 290.1078USN 1/17/09 - 20 -

telephone number indicated in order to discuss such matter
prior to the next action on the merits of this application.

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

cc: Lisbeth Soderman, Borenus
(Your ref: S0049US)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Sami Vaarala, Antti Nuopponen

Art Unit 2446
Confirmation No. 1571

Serial No. 10/500,930

CERTIFICATE OF MAILING

Filed: 19 October 2005

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

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 January**
2009.

Examiner: Jeffrey K. Seto

/rfasth/

Date: 17 January 2009

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 12 November 2008.
- (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 Docket No. 290.1078USN

Electronic Acknowledgement Receipt

EFS ID:	4634326
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-JAN-2009
Filing Date:	19-OCT-2005
Time Stamp:	20:18:41
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		AMD.PDF	55571 <small>63971a9b20985a0c42503d8f6c66616579e0d74f2</small>	yes	21

Multipart Description/PDF files in .zip description			
Document Description	Start	End	
Amendment/Req. Reconsideration-After Non-Final Reject	1	1	
Claims	2	7	
Applicant Arguments/Remarks Made in an Amendment	8	21	

Warnings:

Information:

2	Miscellaneous Incoming Letter	TRX.PDF	18503	no	1
			63b5576cc22d006e9bfd726df871179696ff5ef4		

Warnings:

Information:

Total Files Size (in bytes):			74074		
-------------------------------------	--	--	-------	--	--

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	01/17/2009	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 ** 26	= 1	X \$26 =	26	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	26	OR	TOTAL ADD'L FEE	

APPLICATION AS AMENDED – PART II					OTHER THAN SMALL ENTITY				
	(Column 1)	(Column 2)	(Column 3)		SMALL ENTITY	OR			
AMENDMENT		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>	*	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".
 The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
 /BRUCE D. HARRISON/

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: 02/27/2009

BHARRIS1 SALE #00000001 Mailroom Dt: 01/17/2009 060243 10500930
01 FC : 2202 26.00 DA

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		OR	N/A	
<input type="checkbox"/> SEARCH FEE <small>(37 CFR 1.16(k), (l), or (m))</small>	N/A	N/A	N/A		OR	N/A	
<input type="checkbox"/> EXAMINATION FEE <small>(37 CFR 1.16(o), (p), or (q))</small>	N/A	N/A	N/A		OR	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 \$ =		OR	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).				OR		
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT <small>(37 CFR 1.16(j))</small>					OR		
			TOTAL		OR	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	01/17/2009	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)		RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	* 27	Minus ** 26	= 1	X \$26 =	26	OR	X \$ =	
	Independent (37 CFR 1.16(h))	* 3	Minus ***3	= 0	X \$110 =	0	OR	X \$ =	
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))						OR		
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						OR		
					TOTAL ADD'L FEE	26	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 (37 CFR 1.16(i))	*	Minus **	=	X \$ =		OR	X \$ =
	Independent (37 CFR 1.16(h))	*	Minus ***	=	X \$ =		OR	X \$ =
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))						OR	
	<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:
 /SHERRY A. DAVIS/

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 11/12/2008
FASTH LAW OFFICES (ROLF FASTH)
26 PINECREST PLAZA, SUITE 2
SOUTHERN PINES, NC 28387-4301

EXAMINER

SETO, JEFFREY K

ART UNIT	PAPER NUMBER
----------	--------------

2446

MAIL DATE	DELIVERY MODE
-----------	---------------

11/12/2008

PAPER

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.

Office Action Summary	Application No. 10/500,930	Applicant(s) VAARALA ET AL.	
	Examiner Jeffrey Seto	Art Unit 2446	

-- 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 19 October 2005.
- 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) 1-26 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) 1-26 is/are rejected.
- 7) Claim(s) 1, 17 and 18 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 19 October 2005 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. _____.
- 5) Notice of Informal Patent Application
- 6) Other: _____.

DETAILED ACTION

1. Claims 1-26 are pending.

Priority

2. Applicant's claim for the benefit of a prior-filed application under 35 U.S.C. 119(e) or under 35 U.S.C. 120, 121, or 365(c) is acknowledged. Since Applicant has provided an English translation of the foreign application, the effective filing date for this application is 1-22-2002.

Claim Objections

3. Claims 1, 17 & 18 are objected to because of the following informalities:
 - a. Regarding claim 1, "the current destination address" in line 14, lacks antecedent basis. This phrase can be replaced with "the destination address".
 - b. Regarding claims 17 & 18, "the modified IKE protocol" in line 3 of each claim, lacks antecedent basis. Appropriate correction is required.

Claim Rejections - 35 USC § 112

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

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

4. Claim 26 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Art Unit: 2446

5. Regarding claim 26, it is unclear whether “a given second computer” in line 4, is referring to “a second computer”, in line 3 of claim 22, or if applicant is introducing another computer, which would be the fourth computer, into the claim. For examination purposes, “a given second computer” has been considered another computer.

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 only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-5, 7-10, 22-24 & 26 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).

7. 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: a) forming a message in the first computer or in a computer that is served by the first computer, and in the latter case sending the message to the first computer (See par. 24, lines 4-11; wherein message formation is inherent in

Art Unit: 2446

“communication” and “exchanging user generated traffic”), b) in the first computer, forming a secure message by giving the message a unique identity and a destination address (See par.’s 4 & 24; wherein the SPI is the unique identity, and the header inherently includes the destination address), c) sending the secure message from the first computer to the intermediate computer (See par. 24, lines 4-6), d) using said destination address and the unique identity to find an 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), e) substituting the current destination address with the found address to the second computer (See par.’s 4 & 24; wherein address substitution is a standard part of IPSec processing and IKE translation), f) substituting the unique identity with another unique identity (See par.’s 4 & 24; wherein generating and substituting SPI’s is a standard part of IPSec processing and IKE translation), and g) forwarding the secure message with substituted current destination address and substituted unique identity to the second computer (See par. 24, line 11).

8. 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).

9. 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).

10. 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: 2446

8-12; wherein manual distribution occurs when the IKE module is responding to a request).

11. 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).

12. Regarding claim 7, Linnakangas teaches sending the message that is sent from the first computer in step c) 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).

13. 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).

14. 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).

15. Regarding claim 10, Linnakangas teaches changing both the address and the SPI-value by the intermediate computer in steps e) and f) (See par. 24; wherein IPsec includes replacing addresses in accordance with the translation tables, and assigning a new SPI value to every received packet).

16. Regarding claim 22, Linnakangas teaches a telecommunication network for secure forwarding of messages, comprising: at least a first computer, a second

Art Unit: 2446

computer and an intermediate computer, the first and the second computers having means for performing an IPsec processing, and the intermediate computer having translation tables to perform IPsec and IKE translation (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).

17. 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).

18. 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 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).

19. 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).

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.

20. 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).

21. 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 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.

Art Unit: 2446

22. 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.

23. Regarding claim 12, Linnakangas, in view of AAPA, teach the invention as described in claim 11. Linnakangas further teaches 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 p. 3, par.'s 46-51).

24. 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).

25. 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).

26. 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).

Art Unit: 2446

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.

27. 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.

28. 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).

29. 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).

Art Unit: 2446

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.

30. 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 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.

31. Regarding claim 17, Linnakangas in view of Sandhu teach the invention as is described in claim 15. Linnakangas further teaches modifying the IKE protocol between the first computer and the intermediate computer by transmitting the IKE keys from the

Art Unit: 2446

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).

32. 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).

33. 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 of an IP address taken from a pool of user IP addresses when forming the translation table (See par.'s 56 & 57).

34. 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

Art Unit: 2446

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

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey Seto whose telephone number is (571)270-7198. The examiner can normally be reached on Monday thru Thursday and alt. Fridays, 9AM-6:30PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeffrey Pwu can be reached on (571) 273-6798. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2446

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.

JKS

11/5/2008

/Joseph E. Avellino/
Primary Examiner, Art Unit 2446

Notice of References Cited	Application/Control No. 10/500,930	Applicant(s)/Patent Under Reexamination VAARALA ET AL.	
	Examiner Jeffrey Seto	Art Unit 2446	Page 1 of 1

U.S. PATENT DOCUMENTS

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A US-2001/0047487	11-2001	Linnakangas et al.	713/201
*	B US-6,985,953	01-2006	Sandhu et al.	709/229
	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.


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	455	2446	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 type="checkbox"/> Yes <input checked="" type="checkbox"/> No	<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 579	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			

EAST Search History


Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	24067	"address translation" "translation table"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/28 12:27
L2	5	("20060045068" "6088725" "6415329" "20040049594" "20060209831").pn.	US-PGPUB; USPAT	OR	ON	2008/10/28 12:27
L3	3	L2 and I1	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/28 12:27
S1	3407	destination near address near1 (computer network router gateway)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 14:52
S2	235	(substitut\$3 replac\$5) near address near1 (computer network router gateway)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 14:53
S3	1169	709/236.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 14:54
S4	6445	709/229,245.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 14:54
S5	294	(substitut\$3 replac\$5) near address near1 (destination)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 14:55

S6	7834	(substitut\$3 replac\$5) near address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 14:56
S7	1035190	SSL TLS	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 14:56
S8	29	S1 and (S2 S5 S6) and (S3 S4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 14:58
S9	2	S7 and S8	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 14:59
S10	207	(S2 S5 S6) and (S3 S4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 15:03
S11	931960	mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 15:04
S12	44	S10 and S11	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 15:04
S13	10	("20060045068" "6088725" "6415329" "20040049594" "20060209831").pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 17:09
S14	5	("20060045068" "6088725" "6415329" "20040049594" "20060209831").pn.	US-PGPUB; USPAT	OR	ON	2008/10/27 17:09

S15	336	"ip address" and (cookie near value)	US-PGPUB; USPAT	OR	ON	2008/10/27 17:10
S16	0	S14 and S15	US-PGPUB; USPAT	OR	ON	2008/10/27 17:10
S17	68244	"ip address" or (cookie near value)	US-PGPUB; USPAT	OR	ON	2008/10/27 17:10
S18	4	S14 and S17	US-PGPUB; USPAT	OR	ON	2008/10/27 17:10
S19	720	(cookie near value)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 17:14
S20	1169	709/236.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 17:15
S21	6445	709/229,245.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 17:15
S22	52	(S20 S21) and S19	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 17:15
S23	35	(chang\$3 modif\$4 replac \$5) near (cookie near value)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 17:18
S24	5	(S20 S21) and S23	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/10/27 17:19

10/ 28/ 2008 12:42:25 PM

C:\ Documents and Settings\ jseto\ My Documents\ EAST\ Workspaces\ 10500930.wsp


Search Notes 	Application/Control No. 10500930	Applicant(s)/Patent Under Reexamination VAARALA ET AL.
	Examiner Jeffrey Seto	Art Unit 2446

SEARCHED			
Class	Subclass	Date	Examiner
709	236	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

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 2446

✓	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							
	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	✓							



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 3 columns: U.S. APPLICATION NUMBER NO. (10/500,930), FIRST NAMED APPLICANT (Sami Vaarala), ATTY. DOCKET NO. (290.1078USN)

INTERNATIONAL APPLICATION NO. (PCT/FI03/00045)

Table with 2 columns: I.A. FILING DATE (01/21/2003), PRIORITY DATE (01/22/2002)

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

CONFIRMATION NO. 1571
371 ACCEPTANCE LETTER



Date Mailed: 04/17/2006

NOTICE OF ACCEPTANCE OF APPLICATION UNDER 35 U.S.C 371 AND 37 CFR 1.495

The applicant is hereby advised that the United States Patent and Trademark Office in its capacity as a Designated / Elected Office (37 CFR 1.495), has determined that the above identified international application has met the requirements of 35 U.S.C. 371, and is ACCEPTED for national patentability examination in the United States Patent and Trademark Office.

The United States Application Number assigned to the application is shown above and the relevant dates are:

Table with 2 columns: DATE OF RECEIPT OF 35 U.S.C. 371(c)(1), (c)(2) and (c)(4) REQUIREMENTS (10/19/2005), DATE OF COMPLETION OF ALL 35 U.S.C. 371 REQUIREMENTS (10/19/2005)

A Filing Receipt (PTO-103X) will be issued for the present application in due course. THE DATE APPEARING ON THE FILING RECEIPT AS THE " FILING DATE" IS THE DATE ON WHICH THE LAST OF THE 35 U.S.C. 371 (c)(1), (c)(2) and (c)(4) REQUIREMENTS HAS BEEN RECEIVED IN THE OFFICE. THIS DATE IS SHOWN ABOVE. The filing date of the above identified application is the international filing date of the international application (Article 11(3) and 35 U.S.C. 363). Once the Filing Receipt has been received, send all correspondence to the Group Art Unit designated thereon.

The following items have been received:

- Indication of Small Entity Status
• Copy of the International Application filed on 07/08/2004
• Copy of the International Search Report filed on 07/08/2004
• Copy of IPE Report filed on 07/08/2004
• Preliminary Amendments filed on 07/08/2004
• Oath or Declaration filed on 10/19/2005
• Small Entity Statement filed on 07/08/2004
• Request for Immediate Examination filed on 07/08/2004
• U.S. Basic National Fees filed on 07/08/2004
• Priority Documents filed on 07/08/2004
• Power of Attorney filed on 10/19/2005

Applicant is reminded that any communications to the United States Patent and Trademark Office must be mailed to the address given in the heading and include the U.S. application no. shown above (37 CFR 1.5)

WINSTON M ALVARADO
Telephone: (703) 308-9140 EXT 206

PART 3 - OFFICE COPY

FORM PCT/DO/EO/903 (371 Acceptance Notice)



#7

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

In re Application of	:	
VAARALA et al.	:	
Application No.: 10/500,930	:	
PCT No.: PCT/FI03/00045	:	
Int. Filing Date: 21 January 2003	:	
Priority Date: 22 January 2002	:	DECISION
Attorney Docket No.: 290.1078USN	:	
For: METHOD AND SYSTEM FOR	:	
SENDING A MESSAGE THROUGH A	:	
SECURE CONNECTION	:	

This is a decision on applicants' submission of a declaration in the United States Patent and Trademark Office (USPTO) on 19 October 2005.

BACKGROUND

On 15 September 2005, the Office mailed Decision On Petition Under 37 CFR 1.137(b), dismissing applicant's petition as moot and requiring an oath or declaration of the inventors in compliance with 37 CFR 1.497(a)-(b). The decision set a one month, non-extendable time period for reply.

On 19 October 2005, applicants submitted a new declaration, executed by the inventors.

DISCUSSION

The new declaration complies with 37 CFR 1.497(a)-(b) .

CONCLUSION

This application is being forwarded to the National Stage Processing Branch of the Office of PCT Operations for continued processing in accordance with this decision. The application has a date of 19 October 2005 under 35 U.S.C. §371(c)(1), (c)(2) and (c)(4).

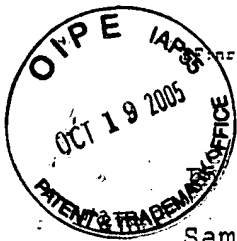
Erin P. Thomson

Erin P. Thomson
Attorney Advisor
PCT Legal Administration

Telephone: 571-272-3292
Facsimile: 571-273-0459

JCO4 Rec'd PCT/PTO 19 OCT 2005

PATENT



10/14/05 290.1078USN

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

re application of Sami Vaarala, Antti Nuopponen

Art Unit. Confirmation No.

Serial No. 10/500,930

CERTIFICATE OF MAILING

Filed: 8 July 2004

I HEREBY CERTIFY THAT THIS PAPER AND THE DOCUMENTS REFERRED TO AS BEING ATTACHED OR ENCLOSED HERewith ARE BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE ON October 14, 2005 AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO: COMMISSIONER FOR PATENTS P.O. BOX 1450, ALEXANDRIA, VA 22313-1450.

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

Examiner:

Rolf Fasth

Date: 14 October 2005

Rolf Fasth
Attorney for Applicant

TRANSMITTAL

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

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

- (X) Copy of Decision On Petition dated 15 September 2005
- (X) Signed Oath or Declaration of the Inventors
- (X) The Commissioner is hereby authorized to charge any additional fees which may be required in connection with the filing of this correspondence, or credit over-payment, to Account No. 06-0243.

Respectfully submitted,
FASTH LAW OFFICES

Rolf Fasth

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

RECEIVED
28 NOV 2005
Legal Staff
International Division

BEST AVAILABLE COPY



15 SEP 2005

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

290.1078 USN

PALETTASH
FASTH LAW OFFICES
629 E. BOCA RATON
PHOENIX, AZ 85022

← HAS BEEN CHANGED.

In re Application of VAARALA et al
Application No.: 10/500,930
PCT Application No.: PCT/FI03/00045
Int. Filing Date: 21 January 2003
Priority Date Claimed: 22 January 2002
Attorney Docket No.: 290.1078USN
For: METHOD AND SYSTEM FOR SENDING A
MESSAGE THROUGH A SECURE CONNECTION

DECISION ON PETITION
UNDER 37 CFR 1.137(b)

This is a decision on applicants' Petition For Revival Under 37 CFR 1.137(b), filed in the United States Patent and Trademark Office (PTO) on 13 June 2005.

BACKGROUND

On 21 January 2003, applicants filed international application PCT/FI03/00045. The international application claims a priority date of 22 January 2002 and designates the United States. A copy of the international application was communicated from the International Bureau to the United States Patent and Trademark Office on 31 July 2003. The deadline for paying the basic national fee in the United States was thirty months from the priority date, that is 22 July 2004.

On 8 July 2004, applicants filed a transmittal letter for entry into the national stage in the United States which was accompanied by, *inter alia*, the U.S. Basic National Fee as required by 35 U.S.C. 371(c)(1), a copy of the international application, and an unexecuted declaration of the inventors.

On 13 December 2004, a Notification of Missing Requirements Under 35 U.S.C. 371 (Form PCT/DO/EO/905) was mailed to applicants, requiring the submission of an executed oath or declaration of the inventors and a surcharge under 37 CFR 1.492(e). This Notification set a two (2) month period for reply, with extensions of time obtainable under 37 CFR 1.136(a).

On 13 June 2005, applicants filed the instant petition for revival accompanied by, *inter alia*, the petition fee of \$750, an executed declaration as required by 35 U.S.C. 371(c)(4), and the surcharge of \$65 for the late declaration.

BEST AVAILABLE COPY

DISCUSSION

Applicants' response filed 13 June 2005 was within the time limits set by the Notification of Missing Requirements, which provided for a two (2) month period for reply, with extensions of time available. Applicants' response was filed in the fourth month, so a four month extension fee of \$795 is required. This fee has been charged to Deposit Account No. 06-0243 as authorized. Applicants' response included an executed declaration as required by 35 U.S.C. 371(c)(4) and the surcharge of \$65 for the late declaration. As such, applicants' reply is timely and the application is not abandoned. Therefore, the petition to revive is moot and the \$750 fee has been credited back to counsel's Deposit Account.

The declaration filed 13 June 2005 is defective because it does not include the entire declaration signed by each inventor. See MPEP 201.03, which states:

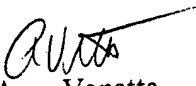
While each inventor need not execute the same oath or declaration, each oath or declaration executed by an inventor must contain a complete listing of all inventors so as to clearly indicate what each inventor believes to be the appropriate inventive entity. Where individual declarations are executed, they must be submitted as individual declarations rather than combined into one declaration.


Thus, applicants' declaration is defective because it is a combined declaration consisting of two individually executed declarations. The declarations must include all of the pages of the declaration signed by each of the inventors.

CONCLUSION

The petition to revive the application abandoned under 37 CFR 1.137(b) is DISMISSED as MOOT.

Applicant is now required to submit a substitute declaration or oath to correct the deficiencies set forth above. Applicant is given **ONE (1) MONTH** from the mailing date of this notice, within which to supply the substitute declaration or oath in order to avoid abandonment. Extensions of time may NOT be obtained under the provisions of 37 CFR 1.136.


Amy Vanatta
PCT Legal Administration Detailee
Telephone: 571-272-6094
Facsimile: 571-273-0419


Boris Milef
PCT Legal Examiner
Office of PCT Legal Administration

Rec'd PCT/PTO 19 OCT 2005

10/500930



10/17/05 390.107805N

COMBINED DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

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

I believe I an original, first and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION, the specification of which was filed as International Patent Application No. PCT/PT03/00045, on 21 January 2003.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information that is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a). If this is a continuation-in-part application filed under the conditions specified in 35 U.S.C. § 120 which discloses and claims subject matter in addition to that disclosed in the prior copending application, I further acknowledge the duty to disclose material information as defined in 37 CFR §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

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

Prior Foreign Application(s)	Priority Claimed
<u>20020112</u> (Number)	<u>Finland</u> (Country)
<u>22 Jan. 2002</u> (Day/Month/Year)	<input checked="" type="checkbox"/> [X] <input type="checkbox"/> [] Yes No

BEST AVAILABLE COPY

Rec'd PCT/PTO 19 OCT 2005
10/500930

RF 10/13/05 290.10/8USM

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

<u>(not applicable)</u>	<u>(n/a)</u>	<u>(not applicable)</u>
(Application Serial No.)	(Filing Date)	(Status: patented, pending, abandoned)

The undersigned hereby authorizes Rolf Fasth, the U.S. attorney named herein, to accept and follow instructions from Innopat Ltd. as to any action to be taken in the Patent and Trademark Office regarding this application without direct communication between Rolf Fasth and the undersigned. In the event of a change in the persons from whom instructions may be taken, Rolf Fasth will be so notified by the undersigned.

I hereby appoint Rolf Fasth, Registration No. 36,999, to prosecute this application, to file a corresponding international application, and to transact all business in the Patent and Trademark Office connected therewith.

Address all telephone calls to Rolf Fasth at telephone number (910) 687-0001; fax number: (910) 295-2152.

Address all correspondence to:

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

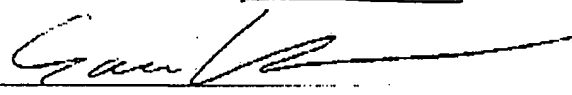
I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment,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

Rec'd PCT/PTO 19 OCT 2005
10/500930

RF 10/13/05 290.10/805N

100

Full name of first joint inventor: Sami Vaarala

Inventor's signature  10/14/05
Date

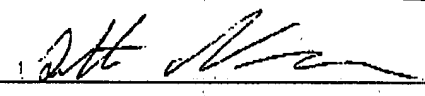
Residence: ~~Helsinki~~ ESPOO, Finland FI X

Citizenship: Finland ✓

Post Office address: ~~Neljas Linja 22A~~ SÄTERINKINNE 8837
FIN-02600 Espoo, Finland
~~FIN-00530 Helsinki, Finland~~

200

Full name of second joint inventor: Antti Nuopponen

Inventor's signature  10/13/05
Date

Residence: Espoo, Finland FI X

Citizenship: Finland ✓

Post Office address: Kaksoiskiventie 7-9 A1
FIN-02760 Espoo, Finland



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 455	GROUP ART UNIT 2617	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

**** SMALL ENTITY ****

Foreign Priority claimed 35 USC 119 (a-d) conditions met Verified and Acknowledged	<input type="checkbox"/> yes <input type="checkbox"/> no <input type="checkbox"/> yes <input type="checkbox"/> no <input type="checkbox"/> Met after Allowance Examiner's Signature _____ Initials _____	STATE OR COUNTRY FINLAND	SHEETS DRAWING 6	TOTAL CLAIMS 26	INDEPENDENT CLAIMS 2
--	--	------------------------------------	----------------------------	---------------------------	--------------------------------

ADDRESS
 33369

TITLE
 Method and system for sending a message through a secure connection

FILING FEE RECEIVED 579	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
-----------------------------------	---	---



15 SEP 2005

UNITED STATES PATENT AND TRADEMARK OFFICE

45

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450
www.uspto.gov

RALF FASTH
FASTH LAW OFFICES
629 E. BOCA RATON
PHOENIX, AZ 85022

In re Application of VAARALA et al :
Application No.: 10/500,930 :
PCT Application No.: PCT/FI03/00045 :
Int. Filing Date: 21 January 2003 : DECISION ON PETITION
Priority Date Claimed: 22 January 2002 : UNDER 37 CFR 1.137(b)
Attorney Docket No.: 290.1078USN :
For: METHOD AND SYSTEM FOR SENDING A :
MESSAGE THROUGH A SECURE CONNECTION :

This is a decision on applicants' Petition For Revival Under 37 CFR 1.137(b), filed in the United States Patent and Trademark Office (PTO) on 13 June 2005.

BACKGROUND

On 21 January 2003, applicants filed international application PCT/FI03/00045. The international application claims a priority date of 22 January 2002 and designates the United States. A copy of the international application was communicated from the International Bureau to the United States Patent and Trademark Office on 31 July 2003. The deadline for paying the basic national fee in the United States was thirty months from the priority date, that is 22 July 2004.

On 8 July 2004, applicants filed a transmittal letter for entry into the national stage in the United States which was accompanied by, *inter alia*, the U.S. Basic National Fee as required by 35 U.S.C. 371(c)(1), a copy of the international application, and an unexecuted declaration of the inventors.

On 13 December 2004, a Notification of Missing Requirements Under 35 U.S.C. 371 (Form PCT/DO/EO/905) was mailed to applicants, requiring the submission of an executed oath or declaration of the inventors and a surcharge under 37 CFR 1.492(e). This Notification set a two (2) month period for reply, with extensions of time obtainable under 37 CFR 1.136(a).

On 13 June 2005, applicants filed the instant petition for revival accompanied by, *inter alia*, the petition fee of \$750, an executed declaration as required by 35 U.S.C. 371(c)(4), and the surcharge of \$65 for the late declaration.

DISCUSSION

Applicants' response filed 13 June 2005 was within the time limits set by the Notification of Missing Requirements, which provided for a two (2) month period for reply, with extensions of time available. Applicants' response was filed in the fourth month, so a four month extension fee of \$795 is required. This fee has been charged to Deposit Account No. 06-0243 as authorized. Applicants' response included an executed declaration as required by 35 U.S.C. 371(c)(4) and the surcharge of \$65 for the late declaration. As such, applicants' reply is timely and the application is not abandoned. Therefore, the petition to revive is moot and the \$750 fee has been credited back to counsel's Deposit Account.

The declaration filed 13 June 2005 is defective because it does not include the entire declaration signed by each inventor. See MPEP 201.03, which states:

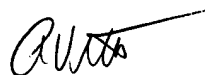
While each inventor need not execute the same oath or declaration, each oath or declaration executed by an inventor must contain a complete listing of all inventors so as to clearly indicate what each inventor believes to be the appropriate inventive entity. Where individual declarations are executed, they must be submitted as individual declarations rather than combined into one declaration.


Thus, applicants' declaration is defective because it is a combined declaration consisting of two individually executed declarations. The declarations must include all of the pages of the declaration signed by each of the inventors.

CONCLUSION

The petition to revive the application abandoned under 37 CFR 1.137(b) is DISMISSED as MOOT.

Applicant is now required to submit a substitute declaration or oath to correct the deficiencies set forth above. Applicant is given **ONE (1) MONTH** from the mailing date of this notice, within which to supply the substitute declaration or oath in order to avoid abandonment. Extensions of time may NOT be obtained under the provisions of 37 CFR 1.136.


Amy Vanatta
PCT Legal Administration Detailee
Telephone: 571-272-6094
Facsimile: 571-273-0419


Boris Milef
PCT Legal Examiner
Office of PCT Legal Administration

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of
Sami Vaarala, Antti Nuopponen

Art Unit
Confirmation No.

Serial No. 10/500,930

CERTIFICATE OF MAILING

Filed: 8 July 2004

I HEREBY CERTIFY THAT THIS PAPER AND THE DOCUMENTS REFERRED TO AS BEING ATTACHED OR ENCLOSED HERewith ARE BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE ON June 9, 2005 AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO: OFFICE OF PETITIONS, MAIL STOP PETITIONS, P.O. BOX 1450, ALEXANDRIA, VA 22313-1450.

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

Examiner:

Date: 9 June 2005

Rolf Fasth
Attorney for Applicant

TRANSMITTAL LETTER

OFFICE OF PETITIONS
MAIL STOP PETITIONS
P.O. Box 1450
Alexandria, VA 22313-1450

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

- (X) Petition for Revival of Application for Patent Abandoned Unintentionally under 37 CFR. 1.137(b)
- (X) Request for Reconsideration of Holding of Abandonment
- (X) Copy of Notice ~~to file Corrected Application Papers~~ **OF MISSING REQUIREMENTS**
- (X) Signed Oath or Declaration of the Inventors
- (X) Check for \$815.00 to cover fees (\$750 for petition to revive and \$65 surcharge for providing oath or declaration later than 30 months from the priority date)
- (X) The Commissioner is hereby authorized to charge any additional fees which may be required in connection with the filing of this correspondence, or credit over-payment, to Account No. 06-0243.

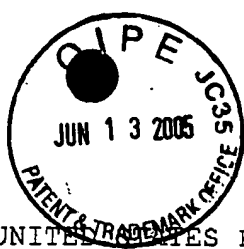
Respectfully submitted,
FASTH LAW OFFICES

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

BEST AVAILABLE COPY





JC10 Rec'd PCT/PTO 13 JUN 2005

RF:sa 6/9/05 290.107BUSN

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of Art Unit

Sami Vaarala, Antti Nuopponen

Serial No. 10/500,930

Filed: 8 July 2004

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

Examiner:

Date: 9 June 2005

CERTIFICATE OF MAILING

I HEREBY CERTIFY THAT THIS PAPER AND THE DOCUMENTS REFERRED TO AS BEING ATTACHED OR ENCLOSED HERewith ARE BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE ON June 9, 2005 AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO: MAIL STOP PETITIONS, COMMISSIONER FOR PATENTS, P.O. BOX 1450, ALEXANDRIA, VA 22323-1450

Rolf Fasth
Attorney for Applicant

REQUEST FOR RECONSIDERATION OF HOLDING OF ABANDONMENT

TO THE COMMISSIONER FOR PATENTS:

The entire delay in filing the required reply from the due date for the reply until the filing of a grantable petition pursuant to 37 1.137(b) was unintentional.

It is requested that any additional fees which are required in connection with this request be charged to Deposit Account No. 06-0243. A duplicate copy of this paper is enclosed.

06/17/2005 MKAYPAGH 00000088 10500930

01 FC:2617

65.00 0P

Respectfully submitted,
FASTH LAW OFFICES

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

BEST AVAILABLE COPY



UNITED STATES PATENT AND TRADEMARK OFFICE

290.1078 USN

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

U.S. APPLICATION NUMBER NO. 10/500,930	FIRST NAMED APPLICANT Sami Vaarala	ATTY. DOCKET NO. 290.1078USN
---	---------------------------------------	---------------------------------

INTERNATIONAL APPLICATION NO. PCT/FI03/00045

I.A. FILING DATE 01/21/2003	PRIORITY DATE 01/22/2002
--------------------------------	-----------------------------

33369
FASTH LAW OFFICES
629 E. BOCA RATON ROAD
PHOENIX, AZ 85022

CONFIRMATION NO. 1571

371 FORMALITIES LETTER



OC000000014733065

Date Mailed: 12/13/2004

NOTIFICATION OF MISSING REQUIREMENTS UNDER 35 U.S.C. 371 IN THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US)

The following items have been submitted by the applicant or the IB to the United States Patent and Trademark Office as a Designated / Elected Office (37 CFR 1.495).

- Indication of Small Entity Status
- Copy of the International Application filed on 07/08/2004
- Copy of the International Search Report filed on 07/08/2004
- Copy of IPE Report filed on 07/08/2004
- Preliminary Amendments filed on 07/08/2004
- Oath or Declaration filed on 07/08/2004
- Small Entity Statement filed on 07/08/2004
- Request for Immediate Examination filed on 07/08/2004
- U.S. Basic National Fees filed on 07/08/2004
- Priority Documents filed on 07/08/2004

The following items **MUST** be furnished within the period set forth below in order to complete the requirements for acceptance under 35 U.S.C. 371:

- Oath or declaration of the inventors, in compliance with 37 CFR 1.497(a) and (b), identifying the application by the International application number and international filing date. The current oath or declaration does not comply with 37 CFR 1.497(a) and (b) in that it:
 - is not executed in accordance with either 37 CFR 1.66 or 37 CFR 1.68.
- \$65 Surcharge for providing the oath or declaration later than 30 months from the priority date (37 CFR 1.492(e)) is required.

SUMMARY OF FEES DUE:

Total additional fees required for this application is \$65 for a Small Entity:

BEST AVAILABLE COPY

- \$65 Late oath or declaration Surcharge.

ALL OF THE ITEMS SET FORTH ABOVE MUST BE SUBMITTED WITHIN TWO (2) MONTHS FROM THE DATE OF THIS NOTICE OR BY 32 MONTHS FROM THE PRIORITY DATE FOR THE APPLICATION, WHICHEVER IS LATER. FAILURE TO PROPERLY RESPOND WILL RESULT IN ABANDONMENT.

The time period set above may be extended by filing a petition and fee for extension of time under the provisions of 37 CFR 1.136(a).

Applicant is reminded that any communications to the United States Patent and Trademark Office must be mailed to the address given in the heading and include the U.S. application no. shown above (37 CFR 1.5)



*A copy of this notice **MUST** be returned with the response.*

WINSTON M ALVARADO

Telephone: (703) 305-6421

PART 1 - ATTORNEY/APPLICANT COPY

U.S. APPLICATION NUMBER NO.	INTERNATIONAL APPLICATION NO.	ATTY. DOCKET NO.
10/500,930	PCT/FI03/00045	290.1078USN

FORM PCT/DO/EO/905 (371 Formalities Notice)

BEST AVAILABLE COPY

Rec'd PCT/PTO 13 JUN 2005

10/500930

RF 6/1/05 200.107802N

COMBINED DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

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

I believe I an original, first and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION, the specification of which was filed as International Patent Application No. PCT/FI03/00045, on 21 January 2003.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information that is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a). If this is a continuation-in-part application filed under the conditions specified in 35 U.S.C. § 120 which discloses and claims subject matter in addition to that disclosed in the prior copending application, I further acknowledge the duty to disclose material information as defined in 37 CFR §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

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

Prior Foreign Application(s)			Priority Claimed
[]	<u>20020112</u>	<u>Finland</u> <u>22 Jan. 2002</u>	[X]
	(Number)	(Country) (Day/Month/Year)	Yes No

RP 6/1/05 230.107805N

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

<u>(not applicable)</u>	<u>(n/a)</u>	<u>(not applicable)</u>
(Application Serial No.)	(Filing Date)	(Status: patented, pending, abandoned)

The undersigned hereby authorizes Rolf Fasth, the U.S. attorney named herein, to accept and follow instructions from Innopat Ltd. as to any action to be taken in the Patent and Trademark Office regarding this application without direct communication between Rolf Fasth and the undersigned. In the event of a change in the persons from whom instructions may be taken, Rolf Fasth will be so notified by the undersigned.

I hereby appoint Rolf Fasth, Registration No. 36,999, to prosecute this application, to file a corresponding international application, and to transact all business in the Patent and Trademark Office connected therewith.

Address all telephone calls to Rolf Fasth at telephone number (602) 993-9099; fax number (602) 942-8364.

Address all correspondence to:

Rolf Fasth
FASTH LAW OFFICES
629 E. Boca Raton
Phoenix, AZ 85022

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

RP 6/1/05 290.1070USN

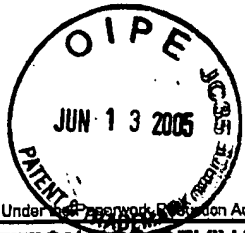
1-00

Full name of first joint inventor:	<u>Sami Vaarala</u>	
Inventor's signature	<u><i>Sami Vaarala</i></u>	<u>1.6.2005</u> Date
Residence:	<u>Helsinki, Finland</u> <i>FIX</i>	
Citizenship:	Finland ✓	
Post Office address:	Saterinrinne 8 B 37 FIN-02600 Espoo, Finland	
Full name of second joint inventor:	Antti Nuopponen	
Inventor's signature	_____	_____ Date
Residence:	Espoo, Finland	
Citizenship:	Finland	
Post Office address:	Kaksoiskiventie 7-9 A1 FIN-02760 Espoo, Finland	

RF 6/1/05 290.107805N

Full name of first joint inventor: Sami Vaarala	
Inventor's signature _____	Date
Residence: Helsinki, Finland	
Citizenship: Finland	
Post Office address: Neljas Linja 22A FIN-00530 Helsinki, Finland	
Full name of second joint inventor: Antti Nuopponen	
Inventor's signature <u><i>Antti Nuopponen</i></u>	7.6.2005 Date
Residence: Espoo, Finland <u>FIX</u>	
Citizenship: Finland <input checked="" type="checkbox"/>	
Post Office address: Kaksoiskiventie 7-9 A1 FIN-02760 Espoo, Finland	

2-00



Rec'd PET/PTO 3 JUN 2005 10/500930

#4

Approved for use through 07/31/2006. OMB 0651-0031 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

PETITION FOR REVIVAL OF AN APPLICATION FOR PATENT ABANDONED UNINTENTIONALLY UNDER 37 CFR 1.137(b)	Docket Number (Optional) 290.1078USN
--	---

First named inventor: SAMI VAARALA

Application No.: 10/500,930

Art Unit:

Filed: 8 JULY 2004

Examiner:

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

Attention: Office of Petitions
Mail Stop Petition
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450
FAX (703) 872-9306

NOTE: If information or assistance is needed in completing this form, please contact Petitions Information at (703) 305-9282.

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

APPLICANT HEREBY PETITIONS FOR REVIVAL OF THIS APPLICATION

NOTE: A grantable petition requires the following items:

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

06/17/2005 MKAYP/IGH 00000088 10500930

02 FC:2453

1. Petition fee

Small entity fee \$ 750.00 (37 CFR 1.17(m)). Applicant claims small entity status. See 37 CFR 1.27.

Other than small entity -- fee \$ _____ (37 CFR 1.17(m))

2. Reply and/or fee

A. The reply and/or fee to the above-noted Office action in the form of STATEMENT THAT DELAY WAS UNINTENTIONAL (identify type of reply):

- has been filed previously on _____
- is enclosed herewith.

B. The issue fee and publication fee (if applicable) of \$ _____

- has been paid previously on _____
- is enclosed herewith.

[Page 1 of 2]

This collection of information is required by 37 CFR 1.137(b). The information is required to obtain or retain a benefit by the publication of the information (as defined 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 average 10 minutes per response, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop Petition, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

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

BEST AVAILABLE COPY

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.

3. Terminal disclaimer with disclaimer fee

- Since this utility/plant application was filed on or after June 8, 1995, no terminal disclaimer is required.
- A terminal disclaimer (and disclaimer fee (37 CFR 1.20(d)) of \$ _____ for a small entity or \$ _____ for other than a small entity) disclaiming the required period of time is enclosed herewith (see PTO/SB/63).

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

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.

<p><u>Rolf Fasth</u> Signature</p> <p>ROLF FASTH Typed or printed name</p> <p>FASTH LAW OFFICES, 26 PINECREST PLAZA, SUITE 2 Address</p> <p>SOUTHERN PINES, NC 28387-4301 Address</p>	<p><u>9 June 2005</u> Date</p> <p>36,999 Registration Number, if applicable</p> <p>910-687-0001 Telephone Number</p>
---	--

- Enclosures: Fee Payment
- Reply
- Terminal Disclaimer Form
- Additional sheets containing statements establishing unintentional delay
- Other: SIGNED DECLARATION

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

I hereby certify that this correspondence is being:

- Deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop Petition, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450.
- Transmitted by facsimile on the date shown below to the United States Patent and Trademark Office as (703) 872-9306.

9 June 2005
Date

Rolf Fasth
Signature

ROLF FASTH
Typed or printed name of person signing certificate

BEST AVAILABLE COPY


UNITED STATES PATENT AND TRADEMARK OFFICE

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

U.S. APPLICATION NUMBER NO. 10/500,930	FIRST NAMED APPLICANT Sami Vaarala	ATTY. DOCKET NO. 290.1078USN
---	---------------------------------------	---------------------------------

INTERNATIONAL APPLICATION NO. PCT/F103/00045

I.A. FILING DATE 01/21/2003	PRIORITY DATE 01/22/2002
--------------------------------	-----------------------------

 33369
 FASTH LAW OFFICES
 629 E. BOCA RATON ROAD
 PHOENIX, AZ 85022

CONFIRMATION NO. 1571
371 FORMALITIES LETTER


OC00000014733065

Date Mailed: 12/13/2004

NOTIFICATION OF MISSING REQUIREMENTS UNDER 35 U.S.C. 371 IN THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US)

The following items have been submitted by the applicant or the IB to the United States Patent and Trademark Office as a Designated / Elected Office (37 CFR 1.495).

- Indication of Small Entity Status
- Copy of the International Application filed on 07/08/2004
- Copy of the International Search Report filed on 07/08/2004
- Copy of IPE Report filed on 07/08/2004
- Preliminary Amendments filed on 07/08/2004
- Oath or Declaration filed on 07/08/2004
- Small Entity Statement filed on 07/08/2004
- Request for Immediate Examination filed on 07/08/2004
- U.S. Basic National Fees filed on 07/08/2004
- Priority Documents filed on 07/08/2004

The following items **MUST** be furnished within the period set forth below in order to complete the requirements for acceptance under 35 U.S.C. 371:

- Oath or declaration of the inventors, in compliance with 37 CFR 1.497(a) and (b), identifying the application by the International application number and international filing date. The current oath or declaration does not comply with 37 CFR 1.497(a) and (b) in that it:
 - is not executed in accordance with either 37 CFR 1.66 or 37 CFR 1.68.
- \$65 Surcharge for providing the oath or declaration later than 30 months from the priority date (37 CFR 1.492(e)) is required.

SUMMARY OF FEES DUE:

Total additional fees required for this application is \$65 for a Small Entity:

- \$65 Late oath or declaration Surcharge.

ALL OF THE ITEMS SET FORTH ABOVE MUST BE SUBMITTED WITHIN TWO (2) MONTHS FROM THE DATE OF THIS NOTICE OR BY 32 MONTHS FROM THE PRIORITY DATE FOR THE APPLICATION, WHICHEVER IS LATER. FAILURE TO PROPERLY RESPOND WILL RESULT IN ABANDONMENT.

The time period set above may be extended by filing a petition and fee for extension of time under the provisions of 37 CFR 1.136(a).

Applicant is reminded that any communications to the United States Patent and Trademark Office must be mailed to the address given in the heading and include the U.S. application no. shown above (37 CFR 1.5)

*A copy of this notice **MUST** be returned with the response.*

WINSTON M ALVARADO

Telephone: (703) 305-6421

PART 2 - OFFICE COPY

U.S. APPLICATION NUMBER NO.	INTERNATIONAL APPLICATION NO.	ATTY. DOCKET NO.
10/500,930	PCT/FI03/00045	290.1078USN

FORM PCT/DO/EO/905 (371 Formalities Notice)

10/500930

DT07 Rec'd PCT/PTO 08 JUL 2004

RF:nr 7/8/04 290.1078USN

EXPRESS MAIL LABEL NO. EU983828392US
Date of Mailing: 8 July 2004

**TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE
(DO/EO/US) CONCERNING FILING UNDER 35 U.S.C. 371**

Attorney Docket No.: 290.1078USN

Int'l. Application No.: PCT/FI03/00045
Int'l. Filing Date: 21 JANUARY 2003
Priority Date Claimed: 22 JANUARY 2002
Title of Invention: METHOD AND SYSTEM FOR SENDING A
MESSAGE THROUGH A SECURE CONNECTION
Applicant(s) for DO/ES/US: Sami Vaarala, Antti Nuopponen

Applicant herewith submits to the United States
Designated/Elected/Office (DO/EO/US) the following items and
other information:

1. This is a FIRST submission of items concerning a filing under 35 U.S.C. 371.
2. This is a SECOND or SUBSEQUENT submission of items concerning a filing under 37 U.S.C. 371.
3. This is an express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. A copy of the International Application as filed (35 U.S.C. 371(c)(2)
 - a. is transmitted herewith (required only if not transmitted by the International Bureau).
 - b. has been transmitted by the International Bureau.
 - c. is not required, as the application was filed in the United States Receiving Office(RO/US).
7. Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
 - a. are transmitted herewith (required only if not transmitted by the International Bureau).
 - b. have been transmitted by the International Bureau.
 - c. have not been made; however, the time limit for making such amendments has NOT expired.
 - d. have not been made and will not be made.
9. An oath or declaration of the inventor (unsigned) (35 U.S.C. 371(c)(4)) (unsigned)
11. An Information Disclosure Statement under 37 C.F.R. 1.97 and 1.98.
12. An assignment document for recording. A cover sheet in

10/500930

DT04 Rec'd PCT/PTO 08 JUL 2004

RP:nr 7/8/04 250.1078USN

EXPRESS MAIL LABEL NO. EU983828392US
Date of Mailing: 8 July 2004

compliance with 37 C.F.R. 3.28 and 3.31 is included.

- 13. A FIRST preliminary amendment.
- 14. Applicant qualifies for Small Entity Status (37 C.F.R. 1.9(f) and 1.27(b)).
- 16. Other items or information: (if any)
- 17. Basic National Filing Fee of \$1080.00 is submitted (Neither international preliminary examination fee (37 C.F.R. 1.482) nor international search fee 37 C.F.R. 1.44.5(a)(2) paid to U.S.P.T.O.).

CLAIMS AS FILED				
For	Number Filed	Number Extra	Basic Fee \$1080.00	Rate
Total Claims	26 - 20	= 0	x \$18.00	= \$108.00
Ind. Claims	2 - 3	= 0	x \$86.00	= \$0.00

- 19. Reduction by 1/2 for filing by small entity, if applicable. Applicant qualifies as small entity.
TOTAL FILING FEE: \$594.00
- 20. Fee for recording the enclosed assignment (37 C.F.R. 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 C.F.R. 3.28, 3.31). \$40.00 per property.
- 21. A check in the amount of \$594.00 to cover the above fee is enclosed.
- 23. The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 06-0243.

Respectfully submitted,

Rolf Fasth
Registration Number 36,999

Send all correspondence to:

Rolf Fasth, Esq.
FASTH LAW OFFICES
629 E. Boca Raton Road
Phoenix, AZ 85022
Telephone: 602-993-9099
Facsimile: 602-942-8364

PLEASE ASSOCIATE THIS
APPLICATION WITH CUSTOMER
NUMBER
33369



33369

TRANSMITTAL LETTER PATENT TRADEMARK OFFICE Page 2 of 2

BEST AVAILABLE COPY

10/500930

DT07 Rec'd PCT/PTO 08 JUL 2004

RF:nr 7/8/04 290.1078USN

EXPRESS MAIL LABEL NO. EU983828392US
Date of Mailing: 8 July 2004

**TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE
(DO/EO/US) CONCERNING FILING UNDER 35 U.S.C. 371**

Attorney Docket No.: 290.1078USN

Int'l. Application No.: PCT/FI03/00045
Int'l. Filing Date: 21 JANUARY 2003
Priority Date Claimed: 22 JANUARY 2002
Title of Invention: METHOD AND SYSTEM FOR SENDING A
MESSAGE THROUGH A SECURE CONNECTION
Applicant(s) for DO/ES/US: Sami Vaarala, Antti Nuopponen

Applicant herewith submits to the United States
Designated/Elected/Office (DO/EO/US) the following items and
other information:

1. This is a FIRST submission of items concerning a filing under 35 U.S.C. 371.
2. This is a SECOND or SUBSEQUENT submission of items concerning a filing under 37 U.S.C. 371.
3. This is an express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. A copy of the International Application as filed (35 U.S.C. 371(c)(2)
 - a. is transmitted herewith (required only if not transmitted by the International Bureau).
 - b. has been transmitted by the International Bureau.
 - c. is not required, as the application was filed in the United States Receiving Office(RO/US).
7. Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
 - a. are transmitted herewith (required only if not transmitted by the International Bureau).
 - b. have been transmitted by the International Bureau.
 - c. have not been made; however, the time limit for making such amendments has NOT expired.
 - d. have not been made and will not be made.
9. An oath or declaration of the inventor (unsigned) (35 U.S.C. 371(c)(4)) (unsigned)
11. An Information Disclosure Statement under 37 C.F.R. 1.97 and 1.98.
12. An assignment document for recording. A cover sheet in

10/500930

DT04 Rec'd PCT/PTO 08 JUL 2004

RP:nr 7/8/04 250.1078USN

EXPRESS MAIL LABEL NO. EU983828392US
Date of Mailing: 8 July 2004

compliance with 37 C.F.R. 3.28 and 3.31 is included.

- 13. A FIRST preliminary amendment.
- 14. Applicant qualifies for Small Entity Status (37 C.F.R. 1.9(f) and 1.27(b)).
- 16. Other items or information: (if any)
- 17. Basic National Filing Fee of \$1080.00 is submitted (Neither international preliminary examination fee (37 C.F.R. 1.482) nor international search fee 37 C.F.R. 1.44.5(a)(2) paid to U.S.P.T.O.).

CLAIMS AS FILED			
For	Number Filed	Number Extra	Basic Fee \$1080.00 Rate
Total Claims	26 - 20	= 0	x \$18.00 = \$108.00
Ind. Claims	2 - 3	= 0	x \$86.00 = \$0.00

- 19. Reduction by 1/2 for filing by small entity, if applicable. Applicant qualifies as small entity.
TOTAL FILING FEE: \$594.00
- 20. Fee for recording the enclosed assignment (37 C.F.R. 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 C.F.R. 3.28, 3.31). \$40.00 per property.
- 21. A check in the amount of \$594.00 to cover the above fee is enclosed.
- 23. The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 06-0243.

Respectfully submitted,

Rolf Fasth
Registration Number 36,999

Send all correspondence to:

Rolf Fasth, Esq.
FASTH LAW OFFICES
629 E. Boca Raton Road
Phoenix, AZ 85022
Telephone: 602-993-9099
Facsimile: 602-942-8364

PLEASE ASSOCIATE THIS APPLICATION WITH CUSTOMER NUMBER 33369



33369

BEST AVAILABLE COPY

METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION

5 TECHNICAL FIELD

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

10

TECHNICAL BACKGROUND

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

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

25 There is a need to protect data and resources from disclosure, to guarantee the authenticity of data, and to protect systems from network based attacks. More in detail, there is a need for confidentiality (protecting the contents of data from being read), integrity (protecting the data from being modified, which is a property that is independent of confidentiality), authentication (obtaining assurance about the actual sender of data), replay protection (guaranteeing that data is fresh, and not a copy of previously sent data), identity protection (keeping the identities of parties exchanging data secret from outsiders), high availability, i.e. denial-of-service protection (ensuring

30

that the system functions even when under attack) and access control. IPSec is a technology providing most of these, but not all of them. (In particular, identity protection is not completely handled by IPSec, and neither is denial-of-service protection.)

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

15

IPSec can encrypt and/or authenticate traffic at IP level. Traffic going in to a WAN is typically compressed and encrypted and traffic coming from a WAN is decrypted and decompressed. IPSec is defined by certain documents, which contain rules for the IPSec architecture. The documents that define IPSec, are, for the time being, the
20 Request For Comments (RFC) series of the Internet Engineering Task Force (IETF), in particular, RFCs 2401-2412.

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

30

Security association (SA) is a key concept in the authentication and the confidentiality mechanisms for IP. A security association is a one-way relationship between a sender

and a receiver that offers security services to the traffic carried on it. If a secure two-way relationship is needed, then two security associations are required. If ESP and AH are combined, or if ESP and/or AH are applied more than once, the term *SA bundle* is used, meaning that two or more SAs are used. Thus, SA bundle refers to one or more
5 SAs applied in sequence, e.g. by first performing an ESP protection, and then an AH protection. The SA bundle is the combination of all SAs used to secure a packet.

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

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

In each IPsec implementation, there is a nominal security association data base
25 (SADB) that defines the parameters associated with each SA. A security association is normally defined by the following parameters. The Sequence Number Counter is a 32-bit value used to generate the sequence number field in AH or ESP headers. The Sequence Counter Overflow is a flag indicating whether overflow of the sequence number counter should generate an auditable event and prevent further transmission
30 of packets on this SA. An Anti-Replay Window is used to determine whether an inbound AH or ESP packet is a replay. AH information involves information about the authentication algorithm, keys and related parameters being used with AH. ESP

information involves information of encryption and authentication algorithms, keys, initialisation vectors, and related parameters being used with IPSec. AH information consists of the authentication algorithm, keys and related parameters being used with AH. ESP information consists of encryption and authentication algorithms, keys, cryptographic initialisation vectors and related parameters being used with ESP. The sixth parameter, Lifetime of this Security Association, is a time-interval and/or byte-count after which this SA must be replaced with a new SA (and new SPI) or terminated plus an indication of which of these actions should occur. IPSec Protocol Mode is either tunnel or transport mode. Maximum Transfer Unit (MTU), an optional feature, defines the maximum size of a packet that can be transmitted without fragmentation. Optionally an MTU discovery protocol may be used to determine the actual MTU for a given route, however, such a protocol is optional.

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

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

Tunnel mode provides protection to the entire IP packet and is usually used for sending messages through more than two components, although tunnel mode may also be used for end-to-end communication between two hosts. Tunnel mode is often used when one or both ends of a SA is a security gateway, such as a firewall or a router that implements IPSec. With tunnel mode, a number of hosts on networks behind firewalls may engage in secure communications without implementing IPSec. The unprotected packets generated by such hosts are tunnelled through external networks by tunnel mode SAs set up by the IPSec software in the firewall or secure router at boundary of the local network.

To achieve this, after the AH or ESP fields are added to the IP packet, the entire packet plus security fields are treated as the payload of a new outer IP packet with a

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

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

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

The key management portion of IPsec involves the determination and distribution of secret keys. The default automated key management protocol for IPsec is referred to as ISAKMP/Oakley and consists of the Oakley key determination protocol and Internet Security Association and Key Management Protocol (ISAKMP). Internet key exchange

(IKE) is a newer name for the ISAKMP/Oakley protocol. IKE is based on the Diffie-Hellman algorithm and supports RSA signature authentication among other modes. IKE is an extensible protocol, and allows future and vendor-specific features to be added without compromising functionality.

5

IPSec has been designed to provide confidentiality, integrity, and replay protection for IP packets. However, IPSec is intended to work with static network topology, where hosts are fixed to certain subnetworks. For instance, when an IPSec tunnel has been formed by using Internet Key Exchange (IKE) protocol, the tunnel endpoints are fixed and remain constant. If IPSec is used with a mobile host, the IKE key exchange will have to be redone from every new visited network. This is problematic, because IKE key exchanges involve computationally expensive Diffie-Hellman key exchange algorithm calculations and possibly RSA calculations. Furthermore, the key exchange requires at least three round trips (six messages) if using the IKE aggressive mode followed by IKE quick mode, and nine messages if using IKE main mode followed by IKE quick mode. This may be a big problem in high latency networks, such as General Packet Radio Service (GPRS) regardless of the computational expenses.

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

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

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

In the scenario, there is a standard IPSec security gateway, which is used by a mobile

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

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

Standard IPsec does e.g. not work through NAT devices at the moment. A standard IPsec NAT traversal protocol is currently being specified, but the security gateway in
20 the scenario might not support an IPsec protocol extended in this way. Furthermore, the current IPsec NAT traversal protocols are not well suited to mobility.

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

A known method of solving some of these problems is based on having an intermediate host between the mobile terminal and the IPsec security gateway. The
30 intermediate host might be a Mobile IP home agent, that provides mobility for the connection between the mobile terminal and the home agent, while the connection from the mobile node to the security gateway is an ordinary IPsec connection. In this

case, packets sent by an application in the mobile client are first processed by IPSec, and then by Mobile IP.

In the general case, this implies both Mobile IP and IPSec header fields for packets exchanged by the mobile terminal and the home agent. The Mobile IP headers are removed by the home agent prior to delivering packets to the security gateway, and added when delivering packets to the mobile terminal. Because of the use of two tunnelling protocols (Mobile IP and IPSec tunnelling), the solution is referred to as "double tunnelling" in this document.

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

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

The mobile host would now establish an IPSec connection between itself and the intermediate host, and would also establish an IPSec connection between itself and the IPSec security gateway. This solution is similar to the first known method, except that two IPSec tunnels are used. It solves a different set of problems – for instance, NAT traversal – but also adds packet size overhead because of double IPSec tunnelling.

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

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

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

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

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

THE OBJECT OF THE INVENTION

30

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

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

SUMMARY OF THE INVENTION

10

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

The advantageous embodiments have the characteristics of the subclaims.

- 25 Preferably, the first computer processes the formed message using a security protocol and encapsulates the message at least in an outer IP header. The outer IP header source address is the current address of the first computer, while the destination address is that of the intermediate computer. The message is then sent to the intermediate computer, which matches the outer IP header address fields together with
30 a unique identifier used by the security protocol, and performs a translation of the outer addresses and the unique identity used by the security protocol. The translated packet is then sent to the second computer, which processes it using the standard security

protocol in question. In the method of the invention, there is no extra encapsulation overhead as in the prior art methods. Also, the intermediate computer does not need to undo the security processing, e.g. decryption, and thus does not compromise security as in the prior art methods.

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

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

25 Thus, the unsecured data packet message is formed by the sending computer, which may or may not be the first computer. The IP header of this packet has IP source and destination address fields (among other things). The packet is encapsulated e.g. wrapped inside a tunnel, and the resulting packet is secured. The secured packet has a new outer IP header, which contains another set of IP source and destination addresses (in the outer header – the inner header is untouched), i.e. there are two
30 outer addresses (source and destination) and two inner addresses. The processed packet has a unique identity, the IPsec SPI value(s).

An essential idea of the invention is to use the standard protocol (IPSec) between the

intermediate computer and the second computer and an "enhanced IPsec protocol" between the first computer and the intermediate computer. IPsec-protected packets are translated by the intermediate computer, without undoing the IPsec processing. This avoids both the overhead of double tunneling, and the security problem involved
5 in using separate tunnels.

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

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

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

In the signalling, e.g. a registration request is sent from the first computer to the intermediate computer which causes the intermediate computer to modify the
30 addresses in the mapping table and thus, the intermediate computer can identify the mobile next time a message is sent. Preferably, as a result of a registration request, a reply registration is sent from the intermediate computer back to the first computer.

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

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

10

Such a protocol can be easily based on e.g. IPsec sequence number field and the replay protection window, which provide a way to detect that packet(s) have been lost. When a receiving host detects missing packets, it can send a request message for those particular packets. The request can of course be piggy-backed on an existing data packet that is being sent to the other host. Another method of doing the retransmissions may be based on using an extra protocol inside which the IPSec packets are wrapped for transmission between the first and intermediate computer. In any case, the second computer remains unaware of such a retransmission protocol.

15

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

25

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

30

translation, preferably by means of mapping tables. The intermediate computer may perform IPSec processing related to other features, such as mobility signalling described above or other enhancements.

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

10

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

20

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

25

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

30

For traffic flowing in the opposite direction, the second partition is used for finding the proper translation table entry, and the first partition for translating the packet fields.

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

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

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

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

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

FIGURES

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

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

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

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

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

5

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

10 DETAILED DESCRIPTION OF THE INVENTION

An example of a telecommunication network of the invention is illustrated in figure 1, comprising a first computer, here a client computer 1 served by an intermediate computer, here as a server 2, and a host computer 4, that is served by the second computer, here a security gateway (SGW) 3. The security gateway supports the standard IPsec protocol and optionally the IKE key exchange protocol. The client computer and the server computer support a modified IPsec and IKE protocol.

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

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

30

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

address and IPSec SPI translations for the packets. These translations accomplish the effect of "double tunnelling" (described in the technical background section), but with the method of the invention the confidentiality of the packets is not compromised, while simultaneously having no extra overhead when compared to standard IPSec.

5 The intermediate computer does not know the cryptographic keys used to encrypt and/or authenticate the packets, and can thus not reveal their contents.

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

15 In the example of figure 1, an IPSec connection is formed between the client computer 1 (the first computer) and the security gateway 3 (the second computer). To create an IPSec tunnel, a SA (or usually a SA bundle) is formed between the respective computers with a preceding key exchange. The key exchange between the first and the second computer can take place manually or it can be performed with an automatic
20 key exchange protocol such as the IKE protocol. For performing said key exchange, a standard IKE protocol is used between the server 2 and the security gateway 3, and a modified IKE protocol is used between the client computer 1 and the server 2. An example of a modified IKE protocol that can be used in the invention is described in connection with figure 4.

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

30 The method of the invention, wherein messages in packet form are sent by routing to the end destination, is generally described in connection with figure 2. It is assumed in

the following description that the IPsec connection between the first and second computer already is formed. The IPsec connection can be set up manually or automatically by e.g. an IKE exchange protocol which is described later.

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

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

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

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

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

The processing of packets in the intermediate computer is based on a translation table i.e. an IPSec translation table shown in figure 3. The table has been divided into two partitions. The left one, identified by the prefix "c-", refers to the network connection between the first computer (host 1 in figure 1) and the intermediate computer (host 2 in figure 1). The right one, identified by the prefix "s-", refers to the network connection between the intermediate computer and the second computer (computer 3 in figure 1). The postfix number ("-1", "-2", or "-3") identifies the host in question. Thus, the address fields ("addr") refer to outer addresses of a packet, while the SPI fields ("SPI") refer to the receiver of packets, which packets were sent with this SPI. Thus, "c-SPI-2" is the SPI value used by host 2 (the intermediate computer) when receiving packets from host 1 (the first computer), and the SPI-value "c-SPI-1" is the SPI-value with which the first computer receives messages and the SPI-value with which the intermediate computer sends messages to the first computer and so on.

In terms of Figure 3, the outer source address would be "c-addr-1" (195.1.2.3), the outer destination address "c-addr-2" (212.90.65.1), while the SPI field would be "c-SPI-2" (0x12341234). The notation 0xNNNNNNNN indicates a 32-bit unsigned integer value, encoded using a hexadecimal notation (base 16). The inner source address is processed by IPSec in the first computer, and would typically be encrypted. In this example, the inner source address would be the static address of the mobile terminal, e.g. 10.0.0.1.

When the intermediate computer receives the packet sent in step 1 described above, it performs an address and SPI translation, ensuring that the security gateway (host 3 of figure 1) can accept the packet. Most of the packet is secured using IPSec, and since the intermediate computer does not have the cryptographic keys to undo the IPSec processing done by the mobile terminal, it cannot decrypt any encrypted portions of the packet but is able to use the outer IP addresses and the incoming SPI value to determine how to modify the outer address and the SPI to suite the second computer, which is the next destination. SPI is now changed to 0x56785678 in the intermediate computer and the address is changed to the address of the second computer. This is done by means of the IPSec translation table of figure 3.

The first row of Figure 3 is a row that the intermediate computer has found that matches the packet in the example, and thus the intermediate computer chooses it for translation. The new outer source address s-addr-2 (212.90.65.1) is substituted for the outer source address c-addr-1 (195.1.2.3), and the new outer destination address s-addr-3 (103.6.5.4) is substituted for the outer destination address c-addr-2 (212.90.65.1). The new SPI value, s-SPI-3 (0x56785678), is substituted for the SPI value c-SPI-2 (0x12341234). If more than one SPI values are used, all the SPI values are substituted similarly. In the example, s-addr-2 and c-addr-2 happen to be the same on both partitions of the table. This is not necessarily so but the intermediate computer might use another address for sending.

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

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

In step 3 of figure 2, the packet is sent from the second computer (corresponding to SGW in figure 1) to host X, having now only the original source IP address 10.0.0.1 and the original destination IP address X in the IP header. Thus, in step 3, host X receives the packet sent by the second computer. Usually, an application process running on host X would generate some return traffic. This would cause an IP packet to be generated and sent to the second computer.

If a packet is sent back from host X to the first computer (corresponding to the client

computer in figure 1), steps analogous to steps 1 - 3 are performed. The packet is thus first sent to the second computer, with the source IP address being X and the destination IP address being 10.0.0.1, in step 4. The generated packet is then received by the second computer. The IPsec policy of the second computer requires that the packet be IPsec-processed using a tunnel mode IPsec SA. This processing is similar to the one in steps 1 and 2. A new, outer IP header is added to the packet in the second computer, after which the resulting packet is secured using the IPsec SA. The outer IP source address is set to s-addr-3 (103.6.5.4) while the outer IP destination address is set to s-addr-2 (212.90.65.1). The SPI field is set to s-SPI-2 (0xc1230012). In step 5, the resulting packet is sent to the address indicated by the new outer IP destination address, s-addr-2, the intermediate computer. The intermediate computer receives the packet and performs a similar address and SPI translation.

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

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

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

The first computer may be a mobile terminal, the outer address of which changes from time to time. The translation table is then modified using some form of signalling messages, as described in the summary section. Upon receiving a request for modifying a translation, the intermediate computer updates the related translation table entry to match the new information supplied by the first computer. The operation of the protocol then proceeds as discussed above.

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

Changes for using AH:

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

15

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

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

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

etc). Thus, the AH integrity check value is now correct.

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

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

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

When the mobile terminal receives the packet, it performs a translation of the current
20 outer addresses and the SPI field for the original ones used by the second computer: s-addr-3 for the outer source address, s-addr-2 for the outer destination address, and s-SPI-2 for the SPI value. This reproduces the packet originally sent by the second computer, except possibly for fields not covered by AH. This operation restores the AH integrity check value to its original, correct value. The AH integrity check is then
25 performed against these fields.

Key exchange considerations

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

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

5

The key exchange must appear as a standard key exchange according to the key exchange protocol supported by the security gateway (the second computer), such as IKE. Also, the overall key exchange performed by the first, intermediate, and second computer must establish not only cryptographic keys, but also the IPSec translation table entries. The overall key exchange protocol should not reveal the IPSec cryptographic keys to the intermediate computer to avoid even the potential for security problems.

10

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

15

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

25

30

The IKE framework supports several "sub-protocols" for phase 1 and phase 2. The required ones are "main mode" for phase 1, and "quick mode" for phase 2. These are

used as illustrations, but the invention is not limited to these sub-protocols of IKE.

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

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

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

25

The overall steps of the protocol are:

1. The first computer initiates the key exchange protocol by sending a message to the intermediate computer. This message is essentially the IKE main mode initiation message, with some modifications required for this application.
- 30 2. The intermediate computer determines which security gateway (second computer) to forward this IKE session to, and also establishes a preliminary IKE translation table entry based on the information available from the message.

3. The security gateway (the second computer) replies to the IKE main mode initiation message.
4. The intermediate computer completes the IKE mapping based on the reply message.
5. The modified IKE protocol run continues through IKE main mode (the phase 1 exchange), which is followed by quick mode (the phase 2 exchange). Extensions of standard IKE messages are used between the first computer and the intermediate computer to accomplish the extra goals required by this modified IKE protocol.

10

In figure 4, the IKE session is described message by message. The following text indicates the contents of each message, and how they are processed by the various hosts. There are six main mode messages in the protocol, named **mm1**, **mm2**, ..., **mm6**, and three quick mode messages, named **qm1**, **qm2**, and **qm3**.

15

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

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

- Local and remote IP address (**c-addr-1**, **c-addr-2**)
- Initiator and responder cookie (**c-icky**, **c-rcky**)
- 25 • IKE identification of the first computer (**c-userid**, e.g. **joe@netseal.com**)

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

- 30 • Local and remote IP address (**s-addr-2**, **s-addr-3**)
- Initiator cookie and responder cookie (**s-icky**, **s-rcky**)

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

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

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

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

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

IKE messages consists of an IKE header, which includes the cookie fields and

message ID field, and of a list of payloads. A payload has a type, and associated information.

5 Figure 4 considers an example of the routing of packets according to the invention considering IPsec security association set-up for distribution of keys. As in the foregoing figure 2, the session begins with sending a packet from the client (first computer) to the server (intermediate computer).

10 The key exchange is initiated by the first computer. Thus, in step 1 of figure 4, the first computer constructs mm1. The IP header of the message contains the following values:

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

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

- Initiator cookie: CKY1 (c-icky)
- Responder cookie: 0 (c-rcky)
- Message ID: 0

20 The message contains the following payloads:

- A Security Association (SA) payload, which contains the IKE phase 1 security policy offers from the first computer.
- The message may contain additional payloads, such as Vendor Identification (VID) payloads, certificate requests/responses, etc.
- 25 - A VID payload can be used to indicate that the first computer supports the protocol described here.

The message tail contains the following information:

- User identification type and value – the c-userid field. These are used by the intermediate computer to choose a security gateway to forward this session to. The identification type may be any of the IKE types, but additional types can be defined. An alternative to this field is to directly indicate the security gateway for forwarding. There are other alternatives
- 30

as well, but these are not essential to the invention.

In step 2, the **mm1** is received by the intermediate computer. The intermediate computer examines the message, and forms the preliminary IKE translation table entry. Figure 5, step 1 illustrates the contents of this preliminary entry. The c-userid field is sent in the **mm1** tail.

The intermediate computer then determines which security gateway to forward this IKE session to. The determination may be based on any available information, static configuration, load balancing, or availability requirements. The presented, simple method is to use the identification information in the **mm1** tail to look up the first matching identification type and value from a table. An example of such a table is presented in Figure 6.

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

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

In addition to determining the security gateway address, the intermediate computer determines which address it uses for communication between itself and the second

computer. The same address as is used for the communication between the first and the intermediate computer may be used, but a new address may also be used. The address can be determined using a table similar to the one in Figure 6, or the table of Figure 6 may be extended to include this address.

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

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

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

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

The IKE header is modified as follows:

- Initiator cookie: CKY2 (s-icky)
- Responder cookie: 0 (s-rcky)
- 20 - Message ID: 0

The message tail is removed. The VID payload that identifies support for this modified protocol is also removed. The mm1 is then forwarded to the second computer.

25 In step 3, the second computer responds with mm2. The IP header of the message contains the following values (step 3 in Figure 4):

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

30 The IKE header contains the following values:

- Initiator cookie: CKY2 (s-icky)
- Responder cookie: CKY3 (s-rcky)

- Message ID: 0

The message contains the following payloads:

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

There is no message tail.

In step 4, the **mm2** is received by the intermediate computer. The intermediate computer updates its IKE translation table based on the received message. Step 3 in Figure 5 illustrates the contents of the translation table entry at this point.

The intermediate computer generates its own responder cookie, **CKY4**, and updates the translation table yet again. Step 4 in Figure 5 illustrates the entry at this point. After this step, the translation table entry is complete, and the address and cookie translations are performed as in steps 1 - 4 for the following messages.

The translated message contains the following IP header fields (Figure 4, step 4)

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

The translated IKE header contains the following fields:

- Initiator cookie: **CKY1** (c-icky)
- Responder cookie: **CKY4** (c-rcky)

The message contains the following payloads:

- The SA payload sent by the second computer.
- Any optional payloads sent by the second computer.

- A VID payload may be added to indicate support of this modified protocol to the first computer.

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

- 5
- Address and/or identification information of the chosen security gateway (the second computer). This information can be used by the client to choose proper authentication information, such as RSA keys.

The message is then forwarded to the first computer.

10

In step 5, the first computer constructs **mm3**. The message contains the following payloads:

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

The message is sent to the intermediate computer.

20

In step 6, the **mm3** is forwarded to the second computer. The contents of the message are not changed, only the IP header addresses and the IKE cookies, in the manner described in steps 1 - 4.

25 In step 7, the second computer receives **mm3** and responds with **mm4**. The message contains the following payloads:

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

In step 8, the **mm4** is forwarded to the first computer.

In step 9, the first computer constructs **mm5**, which is the first encrypted message in the session. All subsequent messages are encrypted using the IKE session keys established from the previous Diffie-Hellman key exchange (the messages **mm3** and **mm4**) by means of hash operations, as described in the IKE specification. Note that the intermediate computer does not possess these keys, and can thus not examine the contents of any subsequent IKE messages. In fact, the intermediate computer has no advantage compared to a hostile attacker if it attempts to decipher the IKE traffic. Instead, the intermediate computer indirectly modifies some fields in the IKE messages by sending a modification request in the IKE message tail to the first computer, which does the requested modifications before IKE encryption processing.

The message contains the following payloads:

- 15 - An Identification (ID) payload, that identifies the first computer to the second computer. This identification may be the same as the identification sent in the **mm1** tail, but may differ from that. These two identifications serve different purposes: the **mm1** tail identification (c-userid) is used to select a security gateway for IKE session forwarding (the second computer), while the ID payload in this message is used by the second computer for IKE authentication purposes, for instance, to select proper RSA authentication keys.
- 20 - A Signature (SIG) or Hash (HASH) payload, that serves as an authenticator. A signature payload is used if RSA- or DSS-based authentication is used, while a hash payload is used for pre-shared key authentication. There are other authentication methods in IKE, and IKE can also be extended with new authentication methods. These are not essential to the invention, and the following text assumes RSA authentication (i.e., use of the signature payload).
- 25 - Possibly optional IKE payloads.
- 30 - Possibly optional IKE payloads.

The message tail contains the following information:

- The SPI value that the first computer wants to use for receiving IPsec-protected messages from the intermediate computer, i.e., the c-SPI-1 value of the IPsec translation table in Figure 3. More than one SPI value could be transmitted here, but for simplicity, the following discussion assumes that only a single SPI is necessary (i.e. only one SA is applied for IPsec traffic processing). Extending the scheme to multiple SPIs is straightforward.

In step 10, the **mm5** is forwarded to the second computer.

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

In step 11, the second computer receives the **mm5** message, and authenticates the user (or the host, depending on what identification type is used). Assuming that the authentication succeeds, the second computer proceeds to authenticate itself to the first computer.

The **mm6** message contains the following payloads:

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

In step 12, the **mm6** is received by the intermediate computer. The intermediate computer does not change the message itself, but adds a tail with the following information:

- The SPI value that the intermediate computer wants the first computer to offer to the second computer in the **qm1** message. Since the intermediate computer cannot access the contents of the IKE messages, this modification request is made using the message tail (see the

discussion of step 9). The SPI value sent matches the s-SPI-2 field of the IPsec translation table of Figure 3.

- The SPI value that the intermediate computer wants the first computer to use for messages sent to itself. This matches the c-SPI-2 field of the IPsec translation table of Figure 3.

5

The resulting message is forwarded to the first computer.

In step 13, the first computer constructs **qm1**, which contains the following IKE payloads:

10

- A Hash (HASH) payload, that serves as an authenticator of the message.
- A Security Association (SA) payload, which contains the IKE phase 2 security policy offers from the first computer, i.e., the IPsec security policy offers. The SA payload contains the SPI value assigned to the first computer in the **mm6** message, i.e., s-SPI-2 in Figure 3.
- Optionally, a Key Exchange (KE) payload, if a new Diffie-Hellman key exchange is to be performed in phase 2 (this depends on the contents of the SA payload).
- A Nonce (NONCE) payload, which contains a random value chosen by the first computer.
- Optionally, two Identification (ID) payloads that indicate the IPsec traffic selectors that the first computer proposes for an IPsec tunnel mode SA. If IPsec transport mode is used, these are not necessary, but they may still be used. They may also be omitted if IPsec tunnel mode is used.

15

20

25

The IKE header is the same as previously, except that the Message ID field now contains a non-zero 32-bit value, that serves as a phase 2 session identifier. This identifier remains constant for the entire quick mode exchange.

30 The message is sent to the intermediate computer.

In step 14, the intermediate computer forwards the **qm1** message to the second

computer.

In step 15, the second computer inspects the security policy offers and other information contained in the **qm1** message, and determines which security policy offer matches its own security policy (the case when no security policies match results in an error notification message).

The second computer responds with **qm2** message, that contains the following payloads:

- 10 - A Hash (HASH) payload, that serves as an authenticator of the message.
- A Security Association (SA) payload, which indicates the security policy offer chosen by the second computer. The message also contains the SPI value that the second computer wants to use when receiving IPsec-protected messages. The SPI value matches s-SPI-3 of the IPsec translation table in Figure 3.
- 15 - Optionally, a Key Exchange (KE) payload, if a new Diffie-Hellman key exchange is to be performed in phase 2.
- A Nonce (NONCE) payload, which contains a random value chosen by the second computer.
- 20 - If Identification (ID) payloads were sent by the first computer, the second computer also sends Identification payloads.

In step 16, the intermediate computer forwards the **qm2** message to the first computer.

In step 17, the first computer constructs **qm3** message, which contains the following payloads:

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

The following information is sent in the message tail:

- 30 - The SPI value sent by the second computer in the **qm2** message. This is sent here, because the intermediate computer cannot decrypt the **qm2** message and look up the SPI from there. The SPI value matches s-SPI-3 of the IPsec translation table in Figure 3.

In step 18, the intermediate computer receives the **qm3** and reads the s-SPI-3 value from the message tail. All the information required to construct the IPsec translation table entry is now gathered, and the entry can be added to the translation table. In particular, the information fields are as follows:

- 5 - c-addr-1: same as c-addr-1 of the IKE session (195.1.2.3).
- c-addr-2: same as c-addr-2 of the IKE session (212.90.65.1).
- c-SPI-1: received in the **mm5** message tail from the first computer.
- c-SPI-2: chosen by the intermediate computer, sent to the first computer in the **mm6** message tail.
- 10 - s-addr-2: same as s-addr-2 of the IKE session (212.90.65.1 in this example, may be different than c-addr-2).
- s-addr-3: same as s-addr-3 of the IKE session (103.6.5.4).
- s-SPI-2: chosen by the intermediate computer, sent to the first computer in **mm6** message tail.
- 15 - s-SPI-3: sent by the second computer in **qm2** to the first computer, which sends it to the intermediate computer in **qm3** message tail.

The intermediate computer forwards the **qm3** message to the second computer, which completes the IKE key exchange, and the IPsec translation table set up.

20

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

25

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

30

Some of these issues are the following:

- The phase 1 used main mode. Any other IKE phase 1 exchange can be used; this changes the details of the protocol but not the essential ideas.
- There are other approaches than the one presented here. One approach is for the first computer to reveal the IKE keys to the intermediate
5 computer, so that the second computer is able to modify the required fields of the message (namely, SPI values).
- The discussion assumes that the first computer initiates the IKE exchange. The opposite direction is possible, too, but requires more considerations.
- The commit bit feature of IKE is not used. Adding that is simple.
- Security gateway selection is based on a table lookup indexed by an
10 identification type/value pair sent by the first computer. Other mechanisms are easy to implement.
- The discussion assumes a successful IKE key exchange. Error cases are easy to handle.
- Phase 1 policy lookup (when processing **mm1** and **mm2** messages) is not based on the identity of the IKE counterpart. This is not a major
15 issue, since the phase 1 security policy can be independent of the counterpart without limiting usability.
- Phase 1 is a pre-requisite for executing the protocol in the example. This can be easily changed by moving some of the "tail" items to phase 2.
- The protocol establishes a pair of SAs, one for each direction, and manages the SPI value modifications of these SAs. It is easy to extend
20 this to cover SA bundles with more than one SA, i.e., SAs applied in sequence (ESP followed by AH, for instance). This requires more than
25 one SPI for each direction, but is easy to add to the protocol described.

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

ART 34 AMDT

39

CLAIMS

1. Method for secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network,
5 characterized by
 - a) forming a message in the first computer or in a computer that is served by the first computer, and in the latter case sending the message to the first computer,
 - b) in the first computer, forming a secure message by giving the message a unique identity and a destination address,
 - 10 c) sending the secure message from the first computer to the intermediate computer,
 - d) using said destination address and the unique identity to find an address to the second computer,
 - e) substituting the current destination address with the found address to the second
15 computer,
 - f) substituting the unique identity with another unique identity,
 - g) forwarding the secure message with substituted current destination address and substituted unique identity to the second computer.
- 20 2. Method of claim 1, characterized in that the secure message is formed in step b) by using an IPSec connection between the first computer and the second computer formed for this purpose in the method.
3. Method of claim 1, characterized in that the secure forwarding of the
25 message is performed by making use of the SSL or TLS protocols.
4. Method of claim 2, characterized in that a preceding distribution of keys to the components for forming the IPSec connection is performed manually.
- 30 5. Method of claim 2, characterized in that a preceding distribution of keys for forming the IPSec connection is performed by an automated key exchange protocol.

BEST AVAILABLE COPY

ORIGINAL DOCUMENT

ART 34 AMDT

40

6. Method of claim 5, characterized in that the automated key exchange protocol used for the preceding distribution of keys for forming the IP Sec connection is performed 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. Method of any of claims 2, 5 or 6, characterized in that the message that is sent from the first computer in step c) is a packet and 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, and other security parameters.
8. Method of any of claims 2, 5 or 6, characterized in that that the IPsec connection is one or more security associations (SA) and the unique identity is one or more SPI values and the other security parameters include one or more sequence numbers.
9. Method of any of claims 1 - 8, characterized in that the matching in step d) is performed by using a translation table stored at the intermediate computer.
10. Method of any of claims 1 - 9, characterized in that both the address and the SPI-value are changed by the intermediate computer in steps e) respective f).
11. Method of any of claims 1 - 10, characterized in that the first computer is a mobile terminal, whereby the mobility is enabled by modifying the translation table at the intermediate computer.
12. Method of claim 11, characterized in that said modification of the translation tables is performed by sending a request for registration of the new address from the first computer to the intermediate computer.

BEST AVAILABLE COPY

ART 34 AMDT

41

13. Method of claim 12, characterized in that a reply to said request for registration is sent from the intermediate computer to the first computer.

14. Method of claim 12 or 13, characterized in that the request for registration and/or reply is authenticated and/or encrypted by IPSec.

15. Method of any of claims 4 -14, characterized in that the key distribution for the secure connections is established 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. Method of claim 15, characterized in that the key exchange distribution is established 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,

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. Method of claim 15 or 16, characterized in that the modified IKE protocol between the first computer and the intermediate computer is modified by transmitting the IKE keys from the first computer to the intermediate computer in order to decrypt and modificate IKE packets.

18. Method of claim 15 or 16, characterized in that in the modified IKE protocol between the first computer and the intermediate computer the modification of the IKE packets is done by the first computer with the intermediate computer requesting such modifications.

BEST AVAILABLE COPY

ART 31 AMDT

42

19. Method of claim 17, characterized in that the address is defined 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. Method of any of claims 1 -19, characterized in that the secure message is sent using IPSec transport mode.

10 21. Method of any of claims 1 -19, characterized in that the secure message is sent using IPSec tunnel mode.

15 22. Telecommunication network for secure forwarding of messages, comprising at least a first computer, a second computer and an intermediate computer, characterized in that the first and the second computers have means to perform IPSec processing, and the intermediate computer have translation tables to perform IPSec and IKE translation.

20 23. Network of claim 22, characterized in that the translation table for IPSec translation comprises IP addresses of the intermediate computer to be matched with IP addresses of the second computer.

25 24. Network of claim 22, characterized in that 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.

30 25. Network of claim 24, characterized in that 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.

BEST AVAILABLE COPY

AMENDED SHEET

17 Mar 04, 17:02

Innopat Oy

+358 9 2517 5378

ANT 34 AVDT

43

26. Network of any of claims 22 - 25, characterized in that there is another translation table for IKE translation containing fields for matching a given user to a given second computer.

BEST AVAILABLE COPY

500,930

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

10/500930

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
31 July 2003 (31.07.2003)

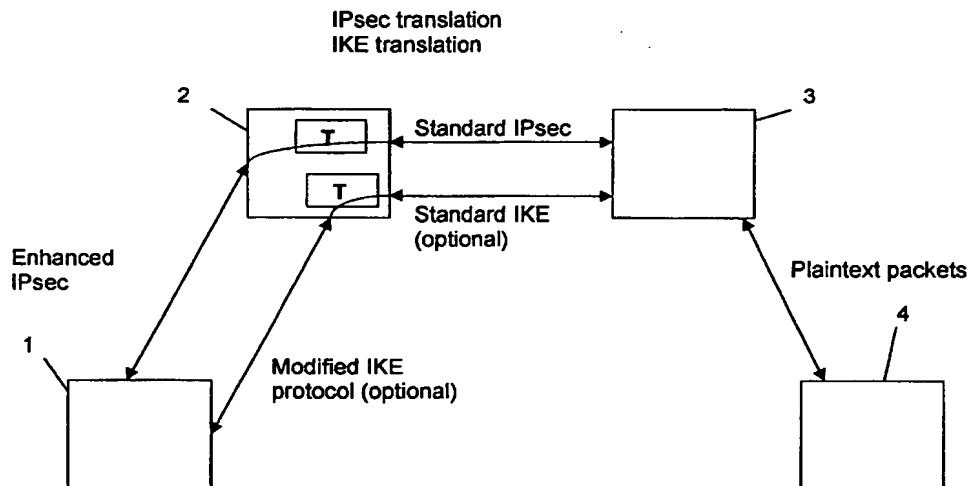
PCT

(10) International Publication Number
WO 03/063443 A1

- (51) International Patent Classification⁷: H04L 29/06, H04Q 7/38 (74) Agent: INNOPAT LTD; P.O. Box 556, FIN-02151 Espoo (FI).
- (21) International Application Number: PCT/FI03/00045 (81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (22) International Filing Date: 21 January 2003 (21.01.2003)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data: 20020112 22 January 2002 (22.01.2002) FI (84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).
- (71) Applicant (for all designated States except US): IN-TRASECURE NETWORKS OY [FI/FI]; PL 38, FIN-02201 Espoo (FI).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): VAARALA, Sami [FI/FI]; Neljäs Linja 22 A, FIN-00530 Helsinki (FI). NUOPPONEN, Antti [FI/FI]; Kaksoiskiventie 7-9 A 1, FIN-02760 Espoo (FI).
- Published:
— with international search report
— before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

[Continued on next page]

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



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

WO 03/063443 A1

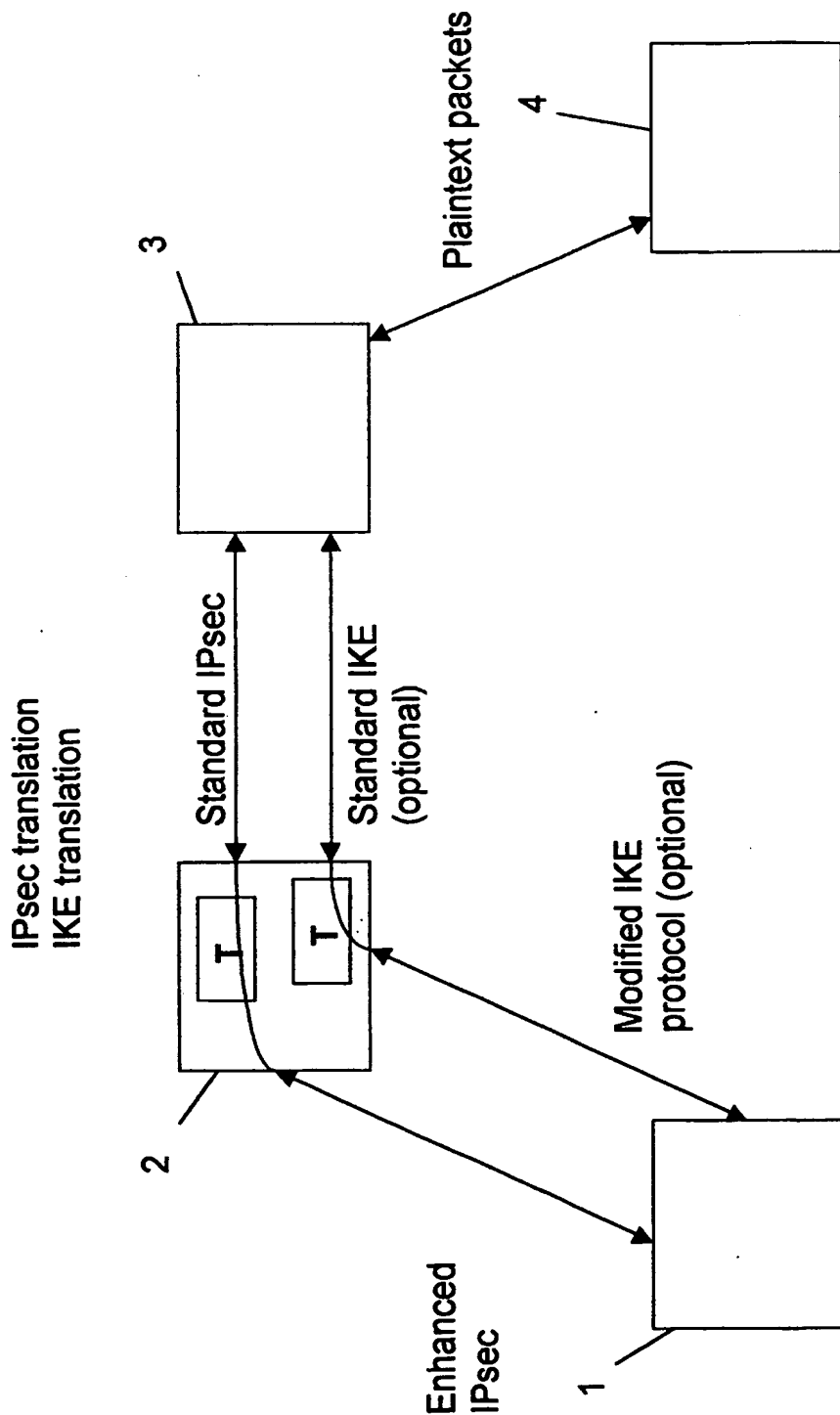


FIG. 1

2 / 6

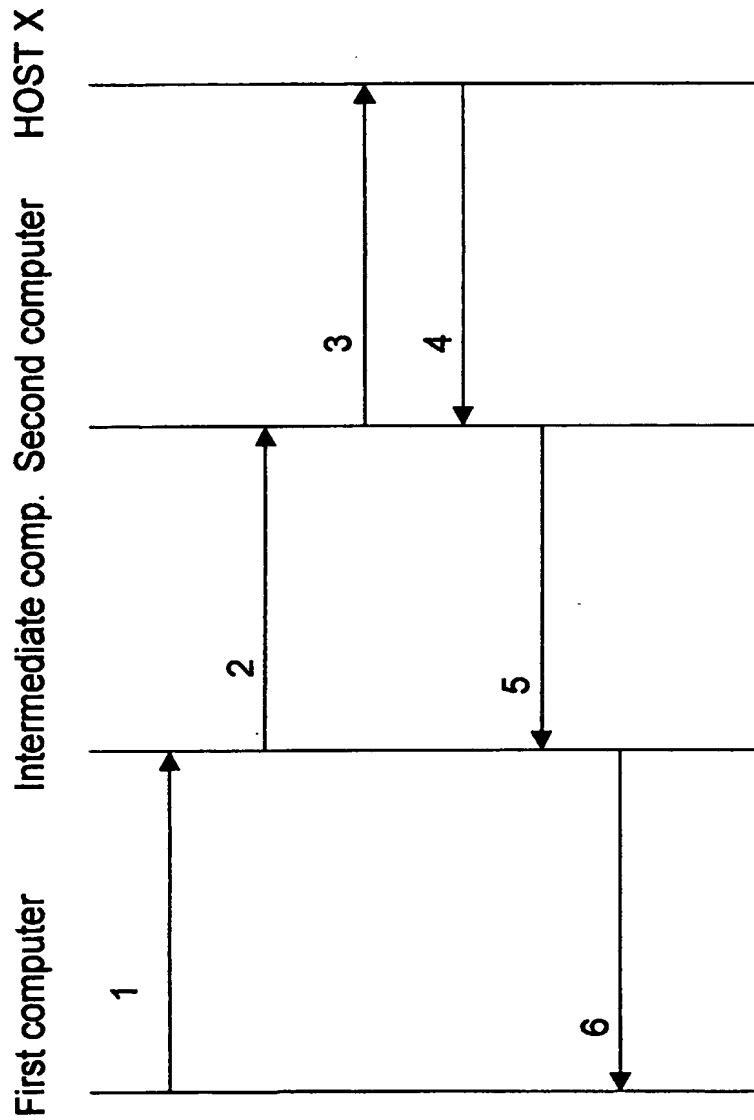


FIG. 2

10/500930

3/6

c-addr-1	c-addr-2	c-SPI-1	c-SPI-2	s-addr-2	s-addr-3	s-SPI-2	s-SPI-3
195.1.2.3	212.90.65.1	0x80000001	0x12341234	212.90.65.1	103.6.5.4	0x1230012	0x56785678
...

FIG. 3

4 / 6

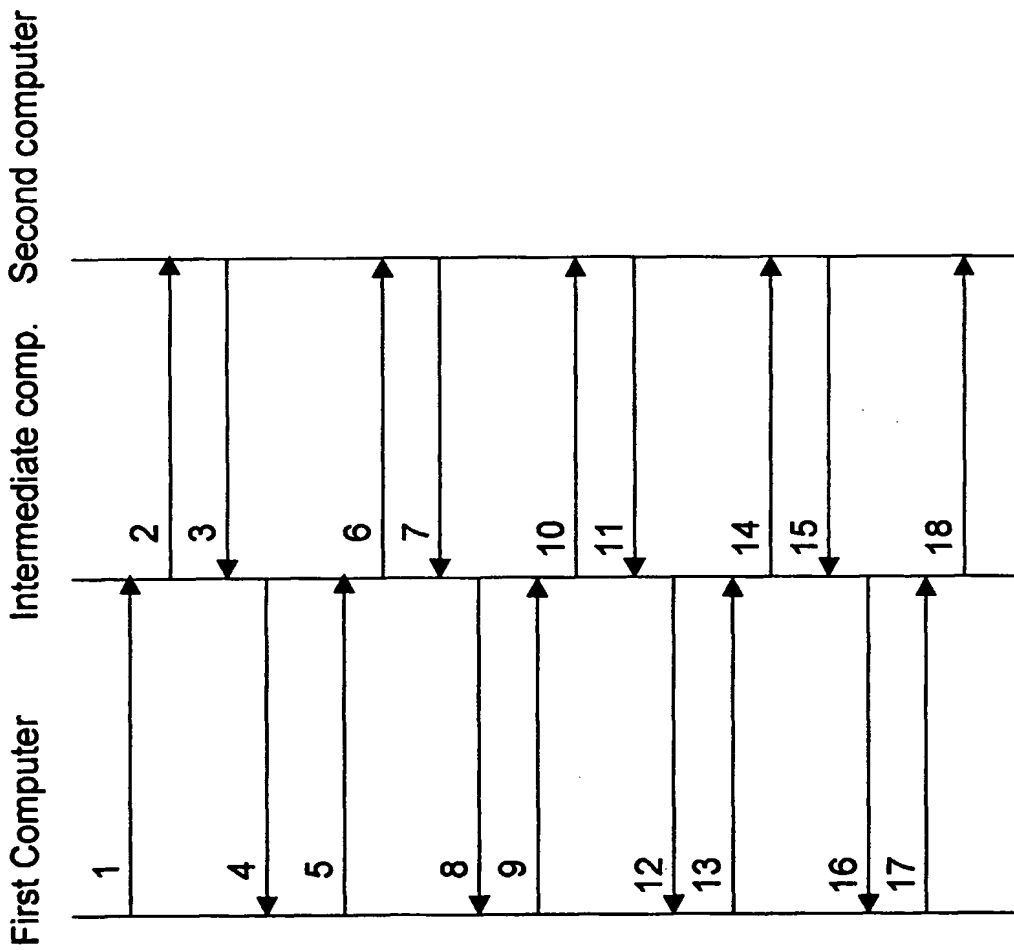


FIG. 4

5/6

Mapping field	Stage 1	Stage 2	Stage 3	Stage 4
c-addr-1	195.1.2.3	195.1.2.3	195.1.2.3	195.1.2.3
c-addr-2	212.90.65.1	212.90.65.1	212.90.65.1	212.90.65.1
c-icky	CKY1	CKY1	CKY1	CKY1
c-rcky	0	0	0	CKY4
c-userid	joe@netseal.com	joe@netseal.com	joe@netseal.com	joe@netseal.com
s-addr-2	n/a	212.90.65.1	212.90.65.1	212.90.65.1
s-addr-3	n/a	103.6.5.4	103.6.5.4	103.6.5.4
s-icky	n/a	CKY2	CKY2	CKY2
s-rcky	n/a	0	CKY3	CKY3

FIG. 5

6/6

Identification type	Identification value	SGW address
User@Fully-Qualified-Domain-Name	<u>*.smith@netseal.com</u>	123.1.2.3
<u>user@Fully-Qualified-Domain-Name</u>	<u>*@netseal.com</u>	103.6.5.4
Distinguished Name	"CN=Sami Vaarala, DC=netseal, DC=com"	122.4.3.2
Fully-Qualified-Domain-Name	host4.roammate.com	123.3.2.1
Employee number and company	"190170 / NetSeal Technologies"	123.4.3.2
...

FIG. 6

Rec'd PCTO 08 JUL 2004

COMBINED DECLARATION AND POWER OF ATTORNEY
FOR PATENT APPLICATION

10/500930

As a below named inventor, I hereby declare that:

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

I believe I an original, first and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION, the specification of which was filed as International Patent Application No. PCT/FI03/00045, on 21 January 2003.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information that is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a). If this is a continuation-in-part application filed under the conditions specified in 35 U.S.C. § 120 which discloses and claims subject matter in addition to that disclosed in the prior copending application, I further acknowledge the duty to disclose material information as defined in 37 CFR §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

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

Prior Foreign Application(s)			Priority Claimed
<u>20020112</u> (Number)	<u>Finland</u> (Country)	<u>22 Jan. 2002</u> (Day/Month/Year)	[X] [] Yes No

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

<u>(not applicable)</u>	<u>(n/a)</u>	<u>(not applicable)</u>
(Application Serial No.)	(Filing Date)	(Status: patented, pending, abandoned)

The undersigned hereby authorizes Rolf Fasth, the U.S. attorney named herein, to accept and follow instructions from Innopat Ltd. as to any action to be taken in the Patent and Trademark Office regarding this application without direct communication between Rolf Fasth and the undersigned. In the event of a change in the persons from whom instructions may be taken, Rolf Fasth will be so notified by the undersigned.

I hereby appoint Rolf Fasth, Registration No. 36,999, to prosecute this application, to file a corresponding international application, and to transact all business in the Patent and Trademark Office connected therewith.

Address all telephone calls to Rolf Fasth at telephone number (602) 993-9099; fax number (602) 942-8364.

Address all correspondence to:

Rolf Fasth
FASTH LAW OFFICES
629 E. Boca Raton
Phoenix, AZ 85022

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

Full name of first joint inventor: Sami Vaarala

Inventor's signature _____

Date

Residence: Helsinki, Finland

Citizenship: Finland

Post Office address: Neljas Linja 22A
FIN-00530 Helsinki, Finland

Full name of second joint inventor: Antti Nuopponen

Inventor's signature _____

Date

Residence: Espoo, Finland

Citizenship: Finland

Post Office address: Kaksoiskiventie 7-9 A1
FIN-02760 Espoo, Finland

PATENT APPLICATION FEE DETERMINATION RECORD
Effective October 1, 2003

Application or Docket Number:
10/500930

CLAIMS AS FILED - PART I

(Column 1) (Column 2)

TOTAL CLAIMS		
FOR	NUMBER FILED	NUMBER EXTRA
TOTAL CHARGEABLE CLAIMS	26 minus 20 =	* -6
INDEPENDENT CLAIMS	2 minus 3 =	*
MULTIPLE DEPENDENT CLAIM PRESENT <input type="checkbox"/>		

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

SMALL ENTITY TYPE

OTHER THAN SMALL ENTITY

RATE	FEE
BASIC FEE	460
XS 9=	54
X43=	
+145=	
TOTAL	514

RATE	FEE
BASIC FEE	
XS18=	
X86=	
-290=	
TOTAL	

CLAIMS AS AMENDED - PART II

(Column 1) (Column 2) (Column 3)

AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
	Total	*	Minus	**	=
	Independent	*	Minus	***	=
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <input type="checkbox"/>				

SMALL ENTITY OR

OTHER THAN SMALL ENTITY

RATE	ADDITIONAL FEE
XS 9=	
X43=	
+145=	
TOTAL ADDIT. FEE	

RATE	ADDITIONAL FEE
XS18=	
X86=	
+290=	
TOTAL ADDIT. FEE	

(Column 1) (Column 2) (Column 3)

AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
	Total	*	Minus	**	=
	Independent	*	Minus	***	=
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <input type="checkbox"/>				

RATE	ADDITIONAL FEE
XS 9=	
X43=	
+145=	
TOTAL ADDIT. FEE	

RATE	ADDITIONAL FEE
XS18=	
X86=	
+290=	
TOTAL ADDIT. FEE	

(Column 1) (Column 2) (Column 3)

AMENDMENT C		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
	Total	*	Minus	**	=
	Independent	*	Minus	***	=
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <input type="checkbox"/>				

RATE	ADDITIONAL FEE
XS 9=	
X43=	
+145=	
TOTAL ADDIT. FEE	

RATE	ADDITIONAL FEE
XS18=	
X86=	
+290=	
TOTAL ADDIT. 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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of Art Unit

5 Sami Vaarala and Antti Nuopponen

Serial No.

10 Filed: Herewith

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

15 Examiner:

Date: 8 July 2004

20

PRELIMINARY AMENDMENT

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

25

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

In the specification:

30 Please add the following paragraph at page 1, line 3
below the title:

--Prior Applications

35 This is a US national phase patent application that
claims priority from PCT/FI03/00045, filed 21 January 2003,
that claims priority from Finnish Patent Application No.
20020112, filed 22 January 2002.--

BEST AVAILABLE COPY

In the Claims:

Amend the claims as follows:

5

1. (Currently amended) ~~Method A method~~ for secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network, ~~characterized by comprising:~~
- 10 ~~characterized by comprising:~~
- a) forming a message in the first computer or in a computer that is served by the first computer, and in the latter case sending the message to the first computer,
 - 15 b) in the first computer, forming a secure message by giving the message a unique identity and a destination address,
 - c) sending the secure message from the first computer to the intermediate computer,
 - d) using said destination address and the unique identity to find an address to the second computer,
 - 20 e) substituting the current destination address with the found address to the second computer,
 - f) substituting the unique identity with another unique identity, and
 - g) forwarding the secure message with substituted current destination address and substituted unique identity to the
 - 25 second computer.
2. (Currently amended) ~~Method of claim 1, characterized in that~~ The method of claim 1 wherein the method
- 30 further comprises forming the secure message is formed in step b) by using an IPsec connection between the first computer and the second computer ~~formed for this purpose in the method.~~
- 35 3. (Currently amended) ~~Method of claim 1, characterized~~

BEST AVAILABLE COPY

~~z-e-d in that~~ The method of claim 1 wherein the method further comprises performing a the secure forwarding of the message ~~is performed~~ by making use of the ~~SSL or TLS~~ protocols.

5

4. (Currently amended) ~~Method of claim 2, characterized~~
~~z-e-d in that~~ The method of claim 2 wherein the method further comprises manually performing a preceding distribution of keys to the ~~components~~ for forming the IPsec connection ~~is performed manually~~.

10

5. (Currently amended) ~~Method of claim 2, characterized~~
~~z-e-d in that~~ The method of claim 2 wherein the method further comprises performing a preceding distribution of keys for forming the IPsec connection ~~is performed~~ by an automated key exchange protocol.

15

6. (Currently amended) ~~Method of claim 5, characterized~~
~~z-e-d in that~~ 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 ~~is performed~~ 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.

20

25

7. (Currently amended) ~~Method of any of claims 2, 5 or 6, characterized~~
~~z-e-d in that~~ The method of claim 2 wherein the method further comprises sending the message that is sent from the first computer in step c) ~~is as~~ a packet ~~and 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, ~~and other~~

30

35

BEST AVAILABLE COPY

~~security parameters.~~

8. (Currently amended) ~~Method of any of claims 2, 5 or 6, c h~~
~~a r a c t e r i z e d i n t h a t~~ The method of claim 1 wherein
5 the method further comprises ~~that~~ the IPsec connection is
being one or more security associations (SA) and the unique
identity is being one or more SPI values ~~and the other~~
~~security parameters include one or more sequence numbers.~~
- 10 9. (Currently amended) ~~Method of any of claims 1 - 8, c h a r~~
~~a c t e r i z e d i n t h a t~~ The method of claim 1 wherein the
method further comprises performing the matching in step d)
is performed by using a translation table stored at the
intermediate computer.
- 15 10. (Currently amended) ~~Method of any of claims 1 - 9, c h a~~
~~r a c t e r i z e d i n t h a t~~ The method of claim 1 wherein
the method further comprises changing both the address and
the SPI-value ~~are changed~~ by the intermediate computer in
20 steps e) respective and f).
- 25 11. (Currently amended) ~~Method of any of claims 1 - 10, c h a~~
~~r a c t e r i z e d i n t h a t~~ The method of claim 1 wherein
the method further comprises the first computer is being a
mobile terminal, whereby so that the mobility is enabled by
modifying the translation table at the intermediate
computer.
- 30 12. (Currently amended) ~~Method of claim 11, c h a r a c t e r~~
~~i z e d i n t h a t~~ The method of claim 11 wherein the method
further comprises performing the said modification of the
translation tables is performed by sending a request for
registration of the new address from the first computer to
the intermediate computer.

35

BEST AVAILABLE COPY

13. (Currently amended) ~~Method of claim 12, characterized~~
~~in that~~ The method of claim 12 wherein the method
further comprises sending a reply to said the request for
registration is sent from the intermediate computer to the
5 first computer.
14. (Currently amended) ~~Method of claim 12 or 13, characterized~~
~~in that~~ The method of claim 12 wherein the
method further comprises authenticating or encrypting by
10 IPSec the request for registration and/or reply is
authenticated and/or encrypted by IPSec.
15. (Currently amended) ~~Method of any of claims 4-14, characterized~~
~~in that~~ The method of claim 4 wherein
15 the method further comprises establishing the key
distribution for the secure connections is established 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.
- 20 16. (Currently amended) ~~Method of claim 15, characterized~~
~~in that~~ The method of claim 15 wherein the method
further comprises establishing the key exchange
distribution is established by
25 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
30 using the translation table to modify IKE packets in flight
by modifying the external IP addresses and possibly IKE
cookies of the IKE packets.
- 35 17. (Currently amended) ~~Method of claim 15 or 16, characterized~~
~~in that~~ The method of claim 15 wherein the

BEST AVAILABLE COPY

- 5 method further comprises modifying the modified IKE protocol between the first computer and the intermediate computer ~~is modified~~ by transmitting the IKE keys from the first computer to the intermediate computer in order to decrypt and ~~modificate~~ modify IKE packets.
18. (Currently amended) ~~Method of claim 15 or 16, characterized in that~~ The method of claim 15 wherein the method further comprises carrying out in the modified IKE protocol between the first computer and the intermediate computer the modification of the IKE packets ~~is done~~ by the first computer with the intermediate computer requesting such modifications.
- 15 19. (Currently amended) ~~Method of claim 17, characterized in that~~ The method of claim 17 wherein the method further comprises defining the address ~~is defined~~ 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 20. (Currently amended) ~~Method of any of claims 1-19, characterized in that~~ The method of claim 1 wherein the method further comprises sending the secure message ~~is sent~~ by using an IPsec transport mode.
- 25 21. (Currently amended) ~~Method of any of claims 1-19, characterized in that~~ The method of claim 1 wherein the method further comprises sending the secure message ~~is sent~~ by using an IPsec tunnel mode.
- 30 22. (Currently amended) ~~Telecommunication~~ A telecommunication network for secure forwarding of messages, comprising:
35 at least a first computer, a second computer and an

BEST AVAILABLE COPY

intermediate computer,

~~characterized in that~~
the first and the second computers ~~have means to perform~~
having means for performing an IPsec processing, and
5 the intermediate computer ~~have~~ having translation tables to
perform IPsec and IKE translation.

23. (Currently amended) ~~Network of claim 22, characterized~~
~~in that~~ The telecommunication network of claim
10 22 wherein the translation table for IPsec translation
~~comprises~~ has IP addresses of the intermediate computer to
be matched with IP addresses of the second computer.

24. (Currently amended) ~~Network of claim 22, characterized~~
15 ~~in that~~ 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
20 computer and the second computer.

25. (Currently amended) ~~Network of claim 24, characterized~~
~~in that~~ The telecommunication network of claim
25 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. (Currently amended) ~~Network of any of claims 22 - 25, characterized~~
30 ~~in that~~ 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 second computer.

BEST AVAILABLE COPY

In the Abstract:

Please add the following abstract on a separate page following the claims:

5

--Abstract

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

10
15
20**BEST AVAILABLE COPY**

REMARKS

Reconsideration of the application is respectfully requested. The specification has been amended to better conform to US patent practice.

5 The claims have been amended to better conform to US patent practice. The claims contain no new matter.

 An abstract has been added to a separate page following the claims. The added abstract contains no new matter.

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

Respectfully submitted,

15 FASTH LAW OFFICES



20 Rolf Fasth
Registration No. 36,999

25 FASTH LAW OFFICES
629 E. Boca Raton
Phoenix, AZ 85022

 Telephone: (602) 993-9099
Facsimile: (602) 942-8364

30 cc: Paivi Soderman, Innopat Ltd.
(Your ref: S0049US)

Helsinki 5.3.2003

Rec'd PCT/PTO 08 JUL 2004

PCT/F 103 00045

10/200930

REC'D 04 APR 2003

WIPO

PCT

ETUOIKEUSTODISTUS
PRIORITY DOCUMENT

Hakija
Applicant

IntraSecure Networks Oy
Espoo

Patentihakemus nro
Patent application no

20020112

Tekemispäivä
Filing date

22.01.2002

Kansainvälinen luokka
International class

H04L

Keksinnön nimitys
Title of invention

"Method and system for sending a message through a secure connection"
(Menetelmä viestin lähettämiseksi turvallisen yhteyden läpi)

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä Patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä, patenttivaatimuksista, tiivistelmästä ja piirustuksista.

This is to certify that the annexed documents are true copies of the description, claims, abstract and drawings originally filed with the Finnish Patent Office.



Marketta Tehikoski
Apulaistarkastaja

Maksu 50 €
Fee 50 EUR

Maksu perustuu kauppa- ja teollisuusministeriön antamaan asetukseen 1027/2001 Patentti- ja rekisterihallituksen maksullisista suoritteista muutoksineen.

The fee is based on the Decree with amendments of the Ministry of Trade and Industry No. 1027/2001 concerning the chargeable services of the National Board of Patents and Registration of Finland.

Osoite: Arkadiankatu 6 A
P.O.Box 1160
FIN-00101 Helsinki, FINLAND

Puhelin: 09 6939 500
Telephone: + 358 9 6939 500

Telefax: 09 6939 5328
Telefax: + 358 9 6939 5328

BEST AVAILABLE COPY

METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION

5 TECHNICAL FIELD

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

10

TECHNICAL BACKGROUND

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

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

25 There is a need to protect data and resources from disclosure, to guarantee the authenticity of data, and to protect systems from network based attacks. More in detail, there is a need for confidentiality (protecting the contents of data from being read), integrity (protecting the data from being modified, which is a property that is independent of confidentiality), authentication (obtaining assurance about the actual sender of data), replay protection (guaranteeing that data is fresh, and not a copy of previously sent data), identity protection (keeping the identities of parties exchanging data secret from outsiders), high availability, i.e. denial-of-service protection (ensuring

that the system functions even when under attack) and access control. IPSec is a technology providing most of these, but not all of them. (In particular, identity protection is not completely handled by IPSec, and neither is denial-of-service protection.)

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

15

IPSec can encrypt and/or authenticate traffic at IP level. Traffic going in to a WAN is typically compressed and encrypted and traffic coming from a WAN is decrypted and decompressed. IPSec is defined by certain documents, which contain rules for the IPSec architecture. The documents that define IPSec, are, for the time being, the Request For Comments (RFC) series of the Internet Engineering Task Force (IETF), in particular, RFCs 2401-2412.

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

Security association (SA) is a key concept in the authentication and the confidentiality mechanisms for IP. A security association is a one-way relationship between a sender

and a receiver that offers security services to the traffic carried on it. If a secure two-way relationship is needed, then two security associations are required. If ESP and AH are combined, or if ESP and/or AH are applied more than once, the term *SA bundle* is used, meaning that two or more SAs are used. Thus, SA bundle refers to one or more SAs applied in sequence, e.g. by first performing an ESP protection, and then an AH protection. The SA bundle is the combination of all SAs used to secure a packet.

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

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

In each IPsec implementation, there is a nominal security association data base (SADB) that defines the parameters associated with each SA. A security association is normally defined by the following parameters. The Sequence Number Counter is a 32-bit value used to generate the sequence number field in AH or ESP headers. The Sequence Counter Overflow is a flag indicating whether overflow of the sequence number counter should generate an auditable event and prevent further transmission of packets on this SA. An Anti-Replay Window is used to determine whether an inbound AH or ESP packet is a replay. AH information involves information about the authentication algorithm, keys and related parameters being used with AH. ESP

information involves information of encryption and authentication algorithms, keys, initialisation vectors, and related parameters being used with IPSec. AH information consists of the authentication algorithm, keys and related parameters being used with AH. ESP information consists of encryption and authentication algorithms, keys, cryptographic initialisation vectors and related parameters being used with ESP. The sixth parameter, Lifetime of this Security Association, is a time-interval and/or byte-count after which this SA must be replaced with a new SA (and new SPI) or terminated plus an indication of which of these actions should occur. IPSec Protocol Mode is either tunnel or transport mode. Maximum Transfer Unit (MTU), an optional feature, defines the maximum size of a packet that can be transmitted without fragmentation. Optionally an MTU discovery protocol may be used to determine the actual MTU for a given route, however, such a protocol is optional.

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

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

Tunnel mode provides protection to the entire IP packet and is usually used for sending messages through more than two components, although tunnel mode may also be used for end-to-end communication between two hosts. Tunnel mode is often used when one or both ends of a SA is a security gateway, such as a firewall or a router that implements IPSec. With tunnel mode, a number of hosts on networks behind firewalls may engage in secure communications without implementing IPSec. The unprotected packets generated by such hosts are tunnelled through external networks by tunnel mode SAs set up by the IPSec software in the firewall or secure router at boundary of the local network.

To achieve this, after the AH or ESP fields are added to the IP packet, the entire packet plus security fields are treated as the payload of a new outer IP packet with a

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

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

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

The key management portion of IPsec involves the determination and distribution of secret keys. The default automated key management protocol for IPsec is referred to as ISAKMP/Oakley and consists of the Oakley key determination protocol and Internet Security Association and Key Management Protocol (ISAKMP). Internet key exchange

(IKE) is a newer name for the ISAKMP/Oakley protocol. IKE is based on the Diffie-Hellman algorithm and supports RSA signature authentication among other modes. IKE is an extensible protocol, and allows future and vendor-specific features to be added without compromising functionality.

5

IPSec has been designed to provide confidentiality, integrity, and replay protection for IP packets. However, IPSec is intended to work with static network topology, where hosts are fixed to certain subnetworks. For instance; when an IPSec tunnel has been formed by using Internet Key Exchange (IKE) protocol, the tunnel endpoints are fixed and remain constant. If IPSec is used with a mobile host, the IKE key exchange will have to be redone from every new visited network. This is problematic, because IKE key exchanges involve computationally expensive Diffie-Hellman key exchange algorithm calculations and possibly RSA calculations. Furthermore, the key exchange requires at least three round trips (six messages) if using the IKE aggressive mode followed by IKE quick mode, and nine messages if using IKE main mode followed by IKE quick mode. This may be a big problem in high latency networks, such as General Packet Radio Service (GPRS) regardless of the computational expenses.

10
15

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

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

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

In the scenario, there is a standard IPSec security gateway, which is used by a mobile

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

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

Standard IPsec does e.g. not work through NAT devices at the moment. A standard IPsec NAT traversal protocol is currently being specified, but the security gateway in the scenario might not support an IPsec protocol extended in this way. Furthermore, the current IPsec NAT traversal protocols are not well suited to mobility.

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

A known method of solving some of these problems is based on having an intermediate host between the mobile terminal and the IPsec security gateway. The intermediate host might be a Mobile IP home agent, that provides mobility for the connection between the mobile terminal and the home agent, while the connection from the mobile node to the security gateway is an ordinary IPsec connection. In this

case, packets sent by an application in the mobile client are first processed by IPSec, and then by Mobile IP.

In the general case, this implies both Mobile IP and IPSec header fields for packets exchanged by the mobile terminal and the home agent. The Mobile IP headers are removed by the home agent prior to delivering packets to the security gateway, and added when delivering packets to the mobile terminal. Because of the use of two tunnelling protocols (Mobile IP and IPSec tunnelling), the solution is referred to as "double tunnelling" in this document.

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

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

The mobile host would now establish an IPSec connection between itself and the intermediate host, and would also establish an IPSec connection between itself and the IPSec security gateway. This solution is similar to the first known method, except that two IPSec tunnels are used. It solves a different set of problems – for instance, NAT traversal – but also adds packet size overhead because of double IPSec tunnelling.

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

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

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

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

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

30 THE OBJECT OF THE INVENTION

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

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

SUMMARY OF THE INVENTION

10

The method and system of the invention enable secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network. It is mainly characterized in that a message is formed in the first computer or in a computer that is served by the first computer, and in the latter

15 case, sending the message to the first computer. In the first computer, a secure message is then formed by giving the message a unique identity and a destination address. The message is sent from the first computer to the intermediate computer, whereafter said destination address and the unique identity are used to find an

20 address to the second computer. The current destination address is substituted with the found address to the second computer, and the unique identity is substituted with another unique identity. Then the message is forwarded to the second computer.

The advantageous embodiments have the characteristics of the subclaims.

- 25 Preferably, the first computer processes the formed message using a security protocol and encapsulates the message at least in an outer IP header. The outer IP header source address is the current address of the first computer, while the destination address is that of the intermediate computer. The message is then sent to the intermediate computer, which matches the outer IP header address fields together with
- 30 a unique identifier used by the security protocol, and performs a translation of the outer addresses and the unique identity used by the security protocol. The translated packet is then sent to the second computer, which processes it using the standard security

protocol in question. In the method of the invention, there is no extra encapsulation overhead as in the prior art methods. Also, the intermediate computer does not need to undo the security processing, e.g. decryption, and thus does not compromise security as in the prior art methods.

5

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

10

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

15

20

25

30

Thus, the unsecured data packet message is formed by the sending computer, which may or may not be the first computer. The IP header of this packet has IP source and destination address fields (among other things). The packet is encapsulated e.g. wrapped inside a tunnel, and the resulting packet is secured. The secured packet has a new outer IP header, which contains another set of IP source and destination addresses (in the outer header – the inner header is untouched), i.e. there are two outer addresses (source and destination) and two inner addresses. The processed packet has a unique identity, the IPsec SPI value(s).

An essential idea of the invention is to use the standard protocol (IPsec) between the

intermediate computer and the second computer and an "enhanced IPsec protocol" between the first computer and the intermediate computer. IPsec-protected packets are translated by the intermediate computer, without undoing the IPsec processing. This avoids both the overhead of double tunneling, and the security problem involved
5 in using separate tunnels.

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

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

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

In the signalling, e.g. a registration request is sent from the first computer to the intermediate computer which causes the intermediate computer to modify the addresses in the mapping table and thus, the intermediate computer can identify the mobile
30 next time a message is sent. Preferably, as a result of a registration request, a reply registration is sent from the intermediate computer back to the first computer.

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

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

10

Such a protocol can be easily based on e.g. IPsec sequence number field and the replay protection window, which provide a way to detect that packet(s) have been lost. When a receiving host detects missing packets, it can send a request message for those particular packets. The request can of course be piggy-backed on an existing data packet that is being sent to the other host. Another method of doing the retransmissions may be based on using an extra protocol inside which the IPsec packets are wrapped for transmission between the first and intermediate computer. In any case, the second computer remains unaware of such a retransmission protocol.

15

20
25

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

30

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

translation, preferably by means of mapping tables. The intermediate computer may perform IPSec processing related to other features, such as mobility signalling described above or other enhancements.

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

10

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

Each translation table consists of entries that are divided into two partitions. The first
 20 partition contains information fields related to the connection between the first computer and the intermediate computer, while the second partition contains information fields related to the connection between the intermediate computer and the
 25 second computer.

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

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

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

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

In the following, the invention is described more in detail by using figures by means of some embodiment examples to carry out the invention. The invention is not restricted to the details of the figures and accompanying text, or any existing protocols, such as the currently standardised IPSec or IKE.
20

Especially, the invention can be concerned with other kinds of telecommunication networks wherein the method of the invention can be applied than that of the figures.
25

FIGURES

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

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

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

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

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

5

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

10 **DETAILED DESCRIPTION OF THE INVENTION**

An example of a telecommunication network of the invention is illustrated in figure 1, comprising a first computer, here a client computer 1 served by an intermediate computer, here as a server 2, and a host computer 4, that is served by the second computer, here a security gateway (SGW) 3. The security gateway supports the standard IPSec protocol and optionally the IKE key exchange protocol. The client computer and the server computer support a modified IPSec and IKE protocol.

15

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

20

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

25

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

30

address and IPsec SPI translations for the packets. These translations accomplish the effect of "double tunnelling" (described in the technical background section), but with the method of the invention the confidentiality of the packets is not compromised, while simultaneously having no extra overhead when compared to standard IPsec.

- 5 The intermediate computer does not know the cryptographic keys used to encrypt and/or authenticate the packets, and can thus not reveal their contents.

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

- 15 In the example of figure 1, an IPsec connection is formed between the client computer 1 (the first computer) and the security gateway 3 (the second computer). To create an IPsec tunnel, a SA (or usually a SA bundle) is formed between the respective computers with a preceding key exchange. The key exchange between the first and the second computer can take place manually or it can be performed with an automatic key exchange protocol such as the IKE protocol. For performing said key exchange, a standard IKE protocol is used between the server 2 and the security gateway 3, and a modified IKE protocol is used between the client computer 1 and the server 2. An example of a modified IKE protocol that can be used in the invention is described in connection with figure 4.

20
25 Messages to be sent to the host terminal 4 from the client computer 1 are first sent to the server 2, wherein an IPsec translation and an IKE translation takes place. After that the message can be sent to the security gateway 3, which sends the message further in plain text to the host terminal 4.

30 The method of the invention, wherein messages in packet form are sent by routing to the end destination, is generally described in connection with figure 2. It is assumed in

the following description that the IPSec connection between the first and second computer already is formed. The IPSec connection can be set up manually or automatically by e.g. an IKE exchange protocol which is described later.

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

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

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

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

20
25
30
In said processing, a new IP header is constructed for the packet, with so-called outer IP addresses. The outer source address of the packet can be the same as the inner IP address – i.e., the address of the mobile terminal – but can be different, if the mobile terminal is visiting a network. The outer source address corresponds to the care-of address obtained by the mobile terminal from the visited network, in this case. The outer destination address is the address of the intermediate computer. In addition to the new IP header, an ESP header is added, when using IPSec ESP mode. The SPI field of the ESP header added by the IPSec processing are set to the SPI value that the intermediate computer uses for receiving packets from the mobile terminal. In general, there may be more than one SPI field in a packet.

The processing of packets in the intermediate computer is based on a translation table i.e. an IPSec translation table shown in figure 3. The table has been divided into two partitions. The left one, identified by the prefix "c-", refers to the network connection between the first computer (host 1 in figure 1) and the intermediate computer (host 2 in figure 1). The right one, identified by the prefix "s-", refers to the network connection between the intermediate computer and the second computer (computer 3 in figure 1). The postfix number ("-1", "-2", or "-3") identifies the host in question. Thus, the address fields ("addr") refer to outer addresses of a packet, while the SPI fields ("SPI") refer to the receiver of packets, which packets were sent with this SPI. Thus, "c-SPI-2" is the SPI value used by host 2 (the intermediate computer) when receiving packets from host 1 (the first computer), and the SPI-value "c-SPI-1" is the SPI-value with which the first computer receives messages and the SPI-value with which the intermediate computer sends messages to the first computer and so on.

In terms of Figure 3, the outer source address would be "c-addr-1" (195.1.2.3), the outer destination address "c-addr-2" (212.90.65.1), while the SPI field would be "c-SPI-2" (0x12341234). The notation 0xNNNNNNNNN indicates a 32-bit unsigned integer value, encoded using a hexadecimal notation (base 16). The inner source address is processed by IPSec in the first computer, and would typically be encrypted. In this example, the inner source address would be the static address of the mobile terminal, e.g. 10.0.0.1.

When the intermediate computer receives the packet sent in step 1 described above, it performs an address and SPI translation, ensuring that the security gateway (host 3 of figure 1) can accept the packet. Most of the packet is secured using IPSec, and since the intermediate computer does not have the cryptographic keys to undo the IPSec processing done by the mobile terminal, it cannot decrypt any encrypted portions of the packet but is able to use the outer IP addresses and the incoming SPI value to determine how to modify the outer address and the SPI to suite the second computer, which is the next destination. SPI is now changed to 0x56785678 in the intermediate computer and the address is changed to the address of the second computer. This is done by means of the IPSec translation table of figure 3.

The first row of Figure 3 is a row that the intermediate computer has found that matches the packet in the example, and thus the intermediate computer chooses it for translation. The new outer source address s-addr-2 (212.90.65.1) is substituted for the outer source address c-addr-1 (195.1.2.3), and the new outer destination address s-addr-3 (103.6.5.4) is substituted for the outer destination address c-addr-2 (212.90.65.1). The new SPI value, s-SPI-3 (0x56785678), is substituted for the SPI value c-SPI-2 (0x12341234). If more than one SPI values are used, all the SPI values are substituted similarly. In the example, s-addr-2 and c-addr-2 happen to be the same on both partitions of the table. This is not necessarily so but the intermediate computer might use another address for sending.

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

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

In step 3 of figure 2, the packet is sent from the second computer (corresponding to SGW in figure 1) to host X, having now only the original source IP address 10.0.0.1 and the original destination IP address X in the IP header. Thus, in step 3, host X receives the packet sent by the second computer. Usually, an application process running on host X would generate some return traffic. This would cause an IP packet to be generated and sent to the second computer.

If a packet is sent back from host X to the first computer (corresponding to the client.

computer in figure 1), steps analogous to steps 1 - 3 are performed. The packet is thus first sent to the second computer, with the source IP address being X and the destination IP address being 10.0.0.1, in step 4. The generated packet is then received by the second computer. The IPsec policy of the second computer requires that the packet be IPsec-processed using a tunnel mode IPsec SA. This processing is similar to the one in steps 1 and 2. A new, outer IP header is added to the packet in the second computer, after which the resulting packet is secured using the IPsec SA. The outer IP source address is set to s-addr-3 (103.6.5.4) while the outer IP destination address is set to s-addr-2 (212.90.65.1). The SPI field is set to s-SPI-2 (0xc1230012).

5 In step 5, the resulting packet is sent to the address indicated by the new outer IP destination address, s-addr-2, the intermediate computer. The intermediate computer receives the packet and performs a similar address and SPI translation.

10

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

15

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

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

25

The first computer may be a mobile terminal, the outer address of which changes from time to time. The translation table is then modified using some form of signalling messages, as described in the summary section. Upon receiving a request for modifying a translation, the intermediate computer updates the related translation table entry to match the new information supplied by the first computer. The operation of the protocol then proceeds as discussed above.

30

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

Changes for using AH:

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

15

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

20
25 After computing the AH integrity check value, the outer addresses and the SPI value are replaced with the values used between the first computer and the intermediate computer: c-addr-1 for the outer source address, c-addr-2 for the outer destination address, and c-SPI-2 for the SPI.

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

etc). Thus, the AH integrity check value is now correct.

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

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

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

When the mobile terminal receives the packet, it performs a translation of the current outer addresses and the SPI field for the original ones used by the second computer: s-addr-3 for the outer source address, s-addr-2 for the outer destination address, and s-SPI-2 for the SPI value. This reproduces the packet originally sent by the second computer, except possibly for fields not covered by AH. This operation restores the AH integrity check value to its original, correct value. The AH integrity check is then performed against these fields.

Key exchange considerations

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

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

5

The key exchange must appear as a standard key exchange according to the key exchange protocol supported by the security gateway (the second computer), such as IKE. Also, the overall key exchange performed by the first, intermediate, and second computer must establish not only cryptographic keys, but also the IPSec translation table entries. The overall key exchange protocol should not reveal the IPSec cryptographic keys to the intermediate computer to avoid even the potential for security problems.

10

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

15

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

20

25

30

The IKE framework supports several "sub-protocols" for phase 1 and phase 2. The required ones are "main mode" for phase 1, and "quick mode" for phase 2. These are

used as illustrations, but the invention is not limited to these sub-protocols of IKE.

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

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

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

The overall steps of the protocol are:

1. The first computer initiates the key exchange protocol by sending a message to the intermediate computer. This message is essentially the IKE main mode initiation message, with some modifications required for this application.
2. The intermediate computer determines which security gateway (second computer) to forward this IKE session to, and also establishes a preliminary IKE translation table entry based on the information available from the message.

3. The security gateway (the second computer) replies to the IKE main mode initiation message.
4. The intermediate computer completes the IKE mapping based on the reply message.
5. The modified IKE protocol run continues through IKE main mode (the phase 1 exchange), which is followed by quick mode (the phase 2 exchange). Extensions of standard IKE messages are used between the first computer and the intermediate computer to accomplish the extra goals required by this modified IKE protocol.

10 In figure 4, the IKE session is described message by message. The following text indicates the contents of each message, and how they are processed by the various hosts. There are six main mode messages in the protocol, named **mm1**, **mm2**, ..., **mm6**, and three quick mode messages, named **qm1**, **qm2**, and **qm3**.

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

- 20 The IKE translation table partition for the connection between the first computer and the intermediate computer is as follows (the field name in Figure 5 is given in parentheses):
- Local and remote IP address (**c-addr-1**, **c-addr-2**)
 - Initiator and responder cookie (**c-icky**, **c-rcky**)
 - IKE identification of the first computer (**c-userid**, e.g. **joe@netseal.com**)

- 25 The IKE translation table partition for the connection between the intermediate computer and the second computer is as follows (the field name in Figure 5 is given in parentheses):
- 30 • Local and remote IP address (**s-addr-2**, **s-addr-3**)
 - Initiator cookie and responder cookie (**s-icky**, **s-rcky**)

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

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

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

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

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

IKE messages consists of an IKE header, which includes the cookie fields and

message ID field, and of a list of payloads. A payload has a type, and associated information.

5 Figure 4 considers an example of the routing of packets according to the invention considering IPsec security association set-up for distribution of keys. As in the foregoing figure 2, the session begins with sending a packet from the client (first computer) to the server (intermediate computer).

10 The key exchange is initiated by the first computer. Thus, in step 1 of figure 4, the first computer constructs mm1. The IP header of the message contains the following values:

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

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

- Initiator cookie: CKY1 (c-icky)
- Responder cookie: 0 (c-rcky)
- Message ID: 0

20 The message contains the following payloads:

- A Security Association (SA) payload, which contains the IKE phase 1 security policy offers from the first computer.
- The message may contain additional payloads, such as Vendor Identification (VID) payloads, certificate requests/responses, etc.
- A VID payload can be used to indicate that the first computer supports the protocol described here.

The message tail contains the following information:

- User identification type and value – the c-userid field. These are used by the intermediate computer to choose a security gateway to forward this session to. The identification type may be any of the IKE types, but additional types can be defined. An alternative to this field is to directly indicate the security gateway for forwarding. There are other alternatives

as well, but these are not essential to the invention.

In step 2, the **mm1** is received by the intermediate computer. The intermediate computer examines the message, and forms the preliminary IKE translation table entry. Figure 5, step 1 illustrates the contents of this preliminary entry. The c-userid field is sent in the **mm1** tail.

The intermediate computer then determines which security gateway to forward this IKE session to. The determination may be based on any available information, static configuration, load balancing, or availability requirements. The presented, simple method is to use the identification information in the **mm1** tail to look up the first matching identification type and value from a table. An example of such a table is presented in Figure 6.

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

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

In addition to determining the security gateway address, the intermediate computer determines which address it uses for communication between itself and the second

computer. The same address as is used for the communication between the first and the intermediate computer may be used, but a new address may also be used. The address can be determined using a table similar to the one in Figure 6, or the table of Figure 6 may be extended to include this address.

5

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

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

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

15

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

The IKE header is modified as follows:

- Initiator cookie: CKY2 (s-icky)
- Responder cookie: 0 (s-rcky)
- Message ID: 0

20

The message tail is removed. The VID payload that identifies support for this modified protocol is also removed. The mm1 is then forwarded to the second computer.

25

In step 3, the second computer responds with mm2. The IP header of the message contains the following values (step 3 in Figure 4):

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

30

The IKE header contains the following values:

- Initiator cookie: CKY2 (s-icky)
- Responder cookie: CKY3 (s-rcky)

- Message ID: 0

The message contains the following payloads:

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

There is no message tail.

In step 4, the **mm2** is received by the intermediate computer. The intermediate computer updates its IKE translation table based on the received message. Step 3 in Figure 5 illustrates the contents of the translation table entry at this point.

The intermediate computer generates its own responder cookie, CKY4, and updates the translation table yet again. Step 4 in Figure 5 illustrates the entry at this point. After this step, the translation table entry is complete, and the address and cookie translations are performed as in steps 1 - 4 for the following messages.

The translated message contains the following IP header fields (Figure 4, step 4)

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

The translated IKE header contains the following fields:

- Initiator cookie: CKY1 (c-icky)
- Responder cookie: CKY4 (c-rcky)

The message contains the following payloads:

- The SA payload sent by the second computer.
- Any optional payloads sent by the second computer.

- A VID payload may be added to indicate support of this modified protocol to the first computer.

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

- 5
- Address and/or identification information of the chosen security gateway (the second computer). This information can be used by the client to choose proper authentication information, such as RSA keys.

The message is then forwarded to the first computer.

10

In step 5, the first computer constructs **mm3**. The message contains the following payloads:

- 15
- A Key Exchange (KE) payload, that contains Diffie-Hellman key exchange data of the first computer.
 - A Nonce (NONCE) payload, that contains a random number chosen by the first computer.
 - Possibly optional IKE payloads.

The message is sent to the intermediate computer.

20

In step 6, the **mm3** is forwarded to the second computer. The contents of the message are not changed, only the IP header addresses and the IKE cookies, in the manner described in steps 1 - 4.

25

In step 7, the second computer receives **mm3** and responds with **mm4**. The message contains the following payloads:

- 30
- A Key Exchange (KE) payload, that contains Diffie-Hellman key exchange data of the second computer.
 - A Nonce (NONCE) payload, that contains a random number chosen by the second computer.
 - Possibly optional IKE payloads.

In step 8, the **mm4** is forwarded to the first computer.

In step 9, the first computer constructs **mm5**, which is the first encrypted message in the session. All subsequent messages are encrypted using the IKE session keys established from the previous Diffie-Hellman key exchange (the messages **mm3** and **mm4**) by means of hash operations, as described in the IKE specification. Note that the intermediate computer does not possess these keys, and can thus not examine the contents of any subsequent IKE messages. In fact, the intermediate computer has no advantage compared to a hostile attacker if it attempts to decipher the IKE traffic. Instead, the intermediate computer indirectly modifies some fields in the IKE messages by sending a modification request in the IKE message tail to the first computer, which does the requested modifications before IKE encryption processing.

The message contains the following payloads:

- An Identification (ID) payload, that identifies the first computer to the second computer. This identification may be the same as the identification sent in the **mm1** tail, but may differ from that. These two identifications serve different purposes: the **mm1** tail identification (c-userid) is used to select a security gateway for IKE session forwarding (the second computer), while the ID payload in this message is used by the second computer for IKE authentication purposes, for instance, to select proper RSA authentication keys.
- A Signature (SIG) or Hash (HASH) payload, that serves as an authenticator. A signature payload is used if RSA- or DSS-based authentication is used, while a hash payload is used for pre-shared key authentication. There are other authentication methods in IKE, and IKE can also be extended with new authentication methods. These are not essential to the invention, and the following text assumes RSA authentication (i.e., use of the signature payload).
- Possibly optional IKE payloads.

The message tail contains the following information:

- The SPI value that the first computer wants to use for receiving IPsec-protected messages from the intermediate computer, i.e., the c-SPI-1 value of the IPsec translation table in Figure 3. More than one SPI value could be transmitted here, but for simplicity, the following discussion assumes that only a single SPI is necessary (i.e. only one SA is applied for IPsec traffic processing). Extending the scheme to multiple SPIs is straightforward.

In step 10, the **mm5** is forwarded to the second computer.

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

In step 11, the second computer receives the **mm5** message, and authenticates the user (or the host, depending on what identification type is used). Assuming that the authentication succeeds, the second computer proceeds to authenticate itself to the first computer.

The **mm6** message contains the following payloads:

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

In step 12, the **mm6** is received by the intermediate computer. The intermediate computer does not change the message itself, but adds a tail with the following information:

- The SPI value that the intermediate computer wants the first computer to offer to the second computer in the **qm1** message. Since the intermediate computer cannot access the contents of the IKE messages, this modification request is made using the message tail (see the

discussion of step 9). The SPI value sent matches the s-SPI-2 field of the IPsec translation table of Figure 3.

- The SPI value that the intermediate computer wants the first computer to use for messages sent to itself. This matches the c-SPI-2 field of the IPsec translation table of Figure 3.

5

The resulting message is forwarded to the first computer.

In step 13, the first computer constructs **qm1**, which contains the following IKE payloads:

10

- A Hash (HASH) payload, that serves as an authenticator of the message.
- A Security Association (SA) payload, which contains the IKE phase 2 security policy offers from the first computer, i.e., the IPsec security policy offers. The SA payload contains the SPI value assigned to the first computer in the **mm6** message, i.e., s-SPI-2 in Figure 3.
- Optionally, a Key Exchange (KE) payload, if a new Diffie-Hellman key exchange is to be performed in phase 2 (this depends on the contents of the SA payload).
- A Nonce (NONCE) payload, which contains a random value chosen by the first computer.
- Optionally, two Identification (ID) payloads that indicate the IPsec traffic selectors that the first computer proposes for an IPsec tunnel mode SA. If IPsec transport mode is used, these are not necessary, but they may still be used. They may also be omitted if IPsec tunnel mode is used.

15

20

22

24

26

28

25

The IKE header is the same as previously, except that the Message ID field now contains a non-zero 32-bit value, that serves as a phase 2 session identifier. This identifier remains constant for the entire quick mode exchange.

30

32

34

36

38

40

42

The message is sent to the intermediate computer.

In step 14, the intermediate computer forwards the **qm1** message to the second

computer.

In step 15, the second computer inspects the security policy offers and other information contained in the **qm1** message, and determines which security policy offer matches its own security policy (the case when no security policies match results in an error notification message).

The second computer responds with **qm2** message, that contains the following payloads:

- 10 - A Hash (HASH) payload, that serves as an authenticator of the message.
- A Security Association (SA) payload, which indicates the security policy offer chosen by the second computer. The message also contains the SPI value that the second computer wants to use when receiving IPsec-protected messages. The SPI value matches s-SPI-3 of the IPsec translation table in Figure 3.
- 15 - Optionally, a Key Exchange (KE) payload, if a new Diffie-Hellman key exchange is to be performed in phase 2.
- A Nonce (NONCE) payload, which contains a random value chosen by the second computer.
- If Identification (ID) payloads were sent by the first computer, the second computer also sends Identification payloads.

In step 16, the intermediate computer forwards the **qm2** message to the first computer.

In step 17, the first computer constructs **qm3** message, which contains the following payloads:

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

The following information is sent in the message tail:

- The SPI value sent by the second computer in the **qm2** message. This is sent here, because the intermediate computer cannot decrypt the **qm2** message and look up the SPI from there. The SPI value matches s-SPI-3 of the IPsec translation table in Figure 3.

In step 18, the intermediate computer receives the **qm3** and reads the s-SPI-3 value from the message tail. All the information required to construct the IPsec translation table entry is now gathered, and the entry can be added to the translation table. In particular, the information fields are as follows:

- 5 - c-addr-1: same as c-addr-1 of the IKE session (195.1.2.3).
- c-addr-2: same as c-addr-2 of the IKE session (212.90.65.1).
- c-SPI-1: received in the **mm5** message tail from the first computer.
- c-SPI-2: chosen by the intermediate computer, sent to the first computer in the **mm6** message tail.
- 10 - s-addr-2: same as s-addr-2 of the IKE session (212.90.65.1 in this example, may be different than c-addr-2).
- s-addr-3: same as s-addr-3 of the IKE session (103.6.5.4).
- s-SPI-2: chosen by the intermediate computer, sent to the first computer in **mm6** message tail.
- 15 - s-SPI-3: sent by the second computer in **qm2** to the first computer, which sends it to the intermediate computer in **qm3** message tail.

The intermediate computer forwards the **qm3** message to the second computer, which completes the IKE key exchange, and the IPsec translation table set up.

20
25
The IPsec cryptographic keys established using the modified IKE key exchange presented above are either derived from the Diffie-Hellman key exchange performed in IKE main mode, or from the (optional) Diffie-Hellman key exchange performed in quick mode. In both cases, the intermediate computer has no access to the shared secret established using the Diffie-Hellman algorithm. In fact, the intermediate computer has no advantage when compared to a random, hostile attacker.

30
The above presentation was simplified and exemplified to increase clarity of the presentation. There are several issues not discussed, but these issues are not essential to the invention.

Some of these issues are the following:

- The phase 1 used main mode. Any other IKE phase 1 exchange can be used; this changes the details of the protocol but not the essential ideas.
- There are other approaches than the one presented here. One approach is for the first computer to reveal the IKE keys to the intermediate computer, so that the second computer is able to modify the required fields of the message (namely, SPI values).
- The discussion assumes that the first computer initiates the IKE exchange. The opposite direction is possible, too, but requires more considerations.
- The commit bit feature of IKE is not used. Adding that is simple.
- Security gateway selection is based on a table lookup indexed by an identification type/value pair sent by the first computer. Other mechanisms are easy to implement.
- The discussion assumes a successful IKE key exchange. Error cases are easy to handle.
- Phase 1 policy lookup (when processing mm1 and mm2 messages) is not based on the identity of the IKE counterpart. This is not a major issue, since the phase 1 security policy can be independent of the counterpart without limiting usability.
- Phase 1 is a pre-requisite for executing the protocol in the example. This can be easily changed by moving some of the "tail" items to phase 2.
- The protocol establishes a pair of SAs, one for each direction, and manages the SPI value modifications of these SAs. It is easy to extend this to cover SA bundles with more than one SA, i.e., SAs applied in sequence (ESP followed by AH, for instance). This requires more than one SPI for each direction, but is easy to add to the protocol described.

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

CLAIMS

1. Method for secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network, characterized by
- 5 a) forming a message in the first computer or in a computer that is served by the first computer, and in the latter case sending the message to the first computer,
- b) in the first computer, forming a secure message by giving the message a unique identity and a destination address,
- 10 c) sending the message from the first computer to the intermediate computer,
- d) using said destination address and the unique identity to find an address to the second computer,
- e) substituting the current destination address with the found address to the second computer,
- 15 f) substituting the unique identity with another unique identity,
- g) forwarding the message to the second computer.
2. Method of claim 1, characterized in that the secure forwarding of the message is performed by making use of the IPSec protocols, whereby the secure message is formed in step b) by using an IPSec connection between the first computer and the second computer formed for this purpose in the method.
- 20
3. Method of claim 1, characterized in that the secure forwarding of the message is performed by making use of the SSL or TLS protocols.
- 25
4. Method of claim 2, characterized in that a preceding distribution of keys to the components for forming the IPSec connection is performed manually.
5. Method of claim 2, characterized in that a preceding distribution of keys for forming the IPSec connection is performed by an automated key exchange protocol.
- 30

6. Method of claim 5, characterized in that the automated key exchange protocol between the first computer and the second computer is performed by means of a modified IKE key exchange protocol between the first computer and the intermediate computer and a standard IKE key exchange protocol between the intermediate computer and the second computer.

5

7. Method of any of claims 2, 5 or 6, characterized in that the message that is sent from the first computer in step c) is a packet and 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, a unique identity, and other security parameters.

10

8. Method of any of claims 2, 5 or 6, characterized in that that the IPSec connection is one or more security associations (SA) and the unique identity is one or more SPI values and the other security parameters include the sequence number(s).

15

9. Method of any of claims 1 – 8, characterized in that the matching in step d) is performed by means of a translation table stored at the intermediate computer.

10. Method of any of claims 1 - 9, characterized in that both the address and the SPI-value are changed by the intermediate computer in steps e) respective f).

11. Method of any of claims 1 - 10, characterized in that the first computer is a mobile terminal, whereby the mobility is enabled by modifying the translation table at the intermediate computer.

12. Method of claim 11, characterized in that said modification of the translation tables is performed by sending a request for registration of the new address from the first computer to the intermediate computer, and optionally, by sending a registration reply from the intermediate computer to the first computer.

25

30

13. Method of claim 12, characterized in that the registration and/or reply is authenticated and/or encrypted by IPSec.

5 14. Method of any of claims 4 -13, characterized in that the key distribution for the secure connections is established 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.

10 15. Method of claim 14, characterized in that the key exchange distribution is established 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,
using a translation table to modify IKE packets in flight by modifying the external IP addresses and possibly IKE cookies of the IKE packets.

20 16. Method of claim 14 or 15, characterized in that the modified IKE protocol between the first computer and the intermediate computer is modified such that the
25 IKE keys are transmitted from the first computer to the intermediate computer for decryption and modification of IKE packets.

30 17. Method of claim 14 or 15, characterized in that in the modified IKE protocol between the first computer and the intermediate computer the modification of the
35 IKE packets is done by the first computer with the intermediate computer requesting such modifications.

40 18. Method of claim 16, characterized in that the address is defined so that the first computer is identified for the second computer by the intermediate computer by
45 means of an IP address taken from a pool of user IP addresses when forming the translation table.

19. Method of any of claims 1 -18, characterized in that the secure message is sent using IPSec transport mode.

5 20. Method of any of claims 1 -18, characterized in that the secure message is sent using IPSec tunnel mode.

21. Telecommunication network for secure forwarding of messages, comprising at least a first computer, a second computer and an intermediate computer, characterized in that
10 the first and the second computers have means to perform IPSec processing, and the intermediate computer have means to perform IPSec translation.

22. Network of claim 21, characterized in that the intermediate computer furthermore has means to perform IKE translation.

15 23. Network of claim 21 or 22, characterized in that the means to perform IPSec translation and IKE translation consists of translation tables.

20 24. Network of claim 22, characterized in that the translation table for IPSec translation comprising IP addresses of the intermediate computer to be matched with IP addresses of the second computer.

25 25. Network of claim 22, characterized in that one of the mapping 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.

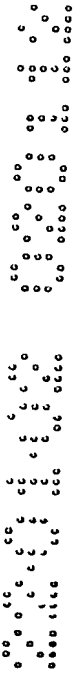
30 26. Network of claim 25, characterized in that both partitions of the mapping table for IKE translation contains translation fields for the source IP address, the destination IP address, initiator and responder cookies between respective computers.

ABSTRACT

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

10 whereafter said destination address and the unique identity are used to find an address to the second computer. The current destination address is substituted with the found address to the second computer, and the unique identity is substituted with another unique identity. Then the message is forwarded to the second computer.

15 FIG. 1



1/6
LG

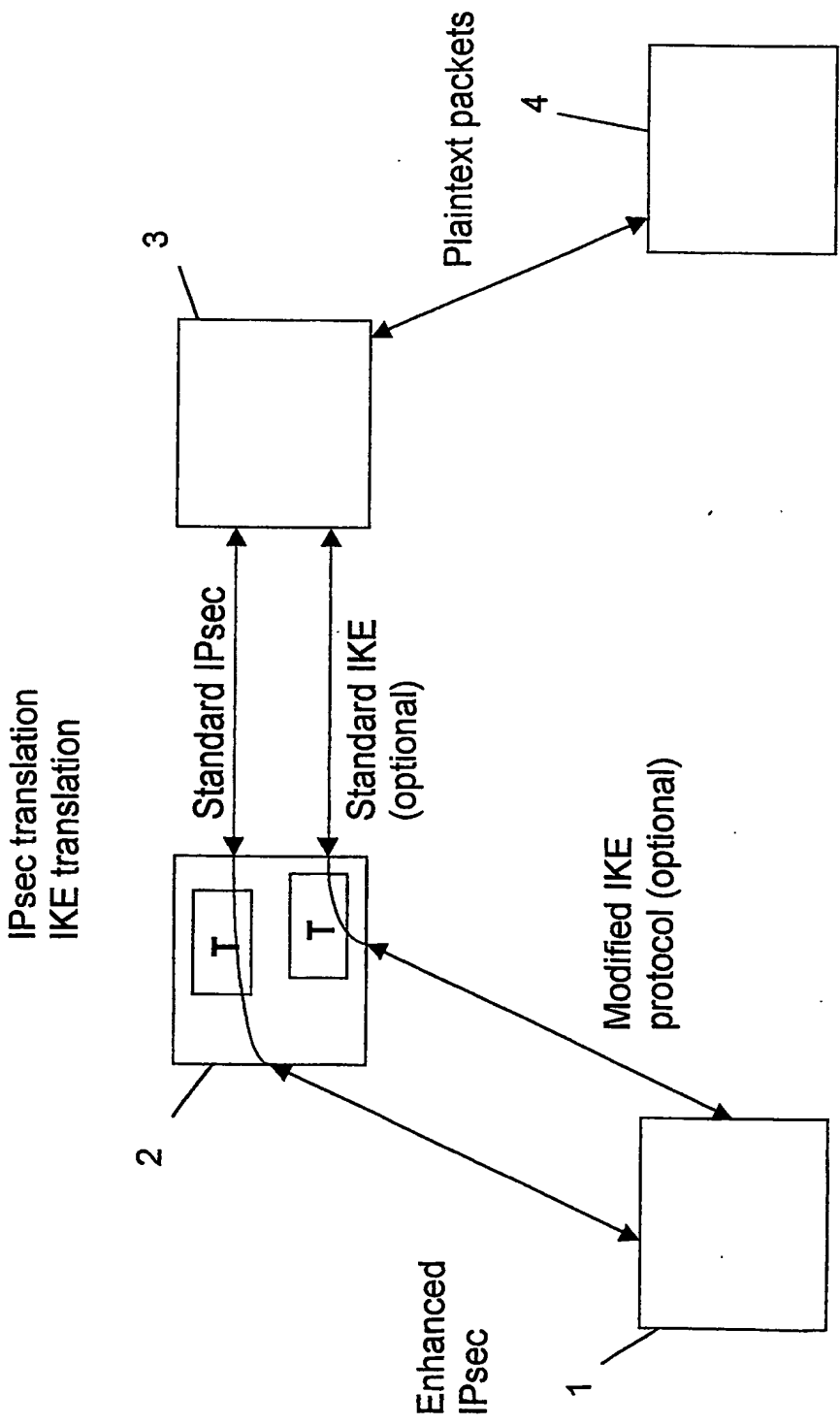


FIG. 1

2/6
L6

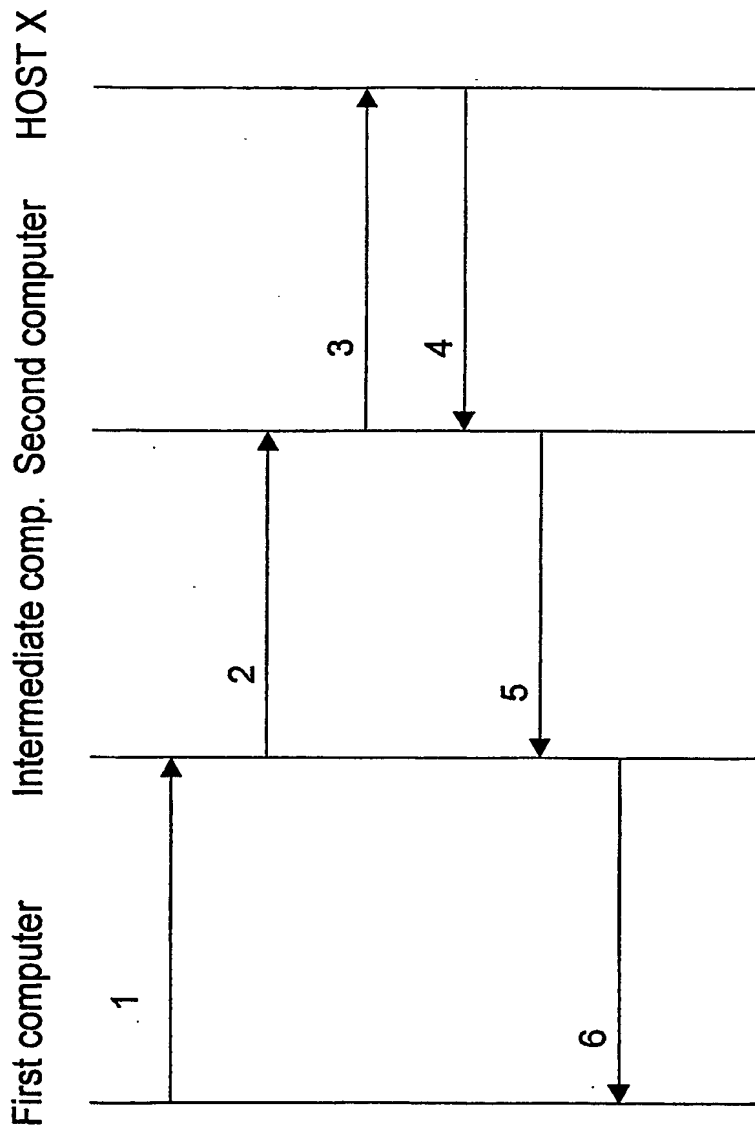


FIG. 2

4/6
L6

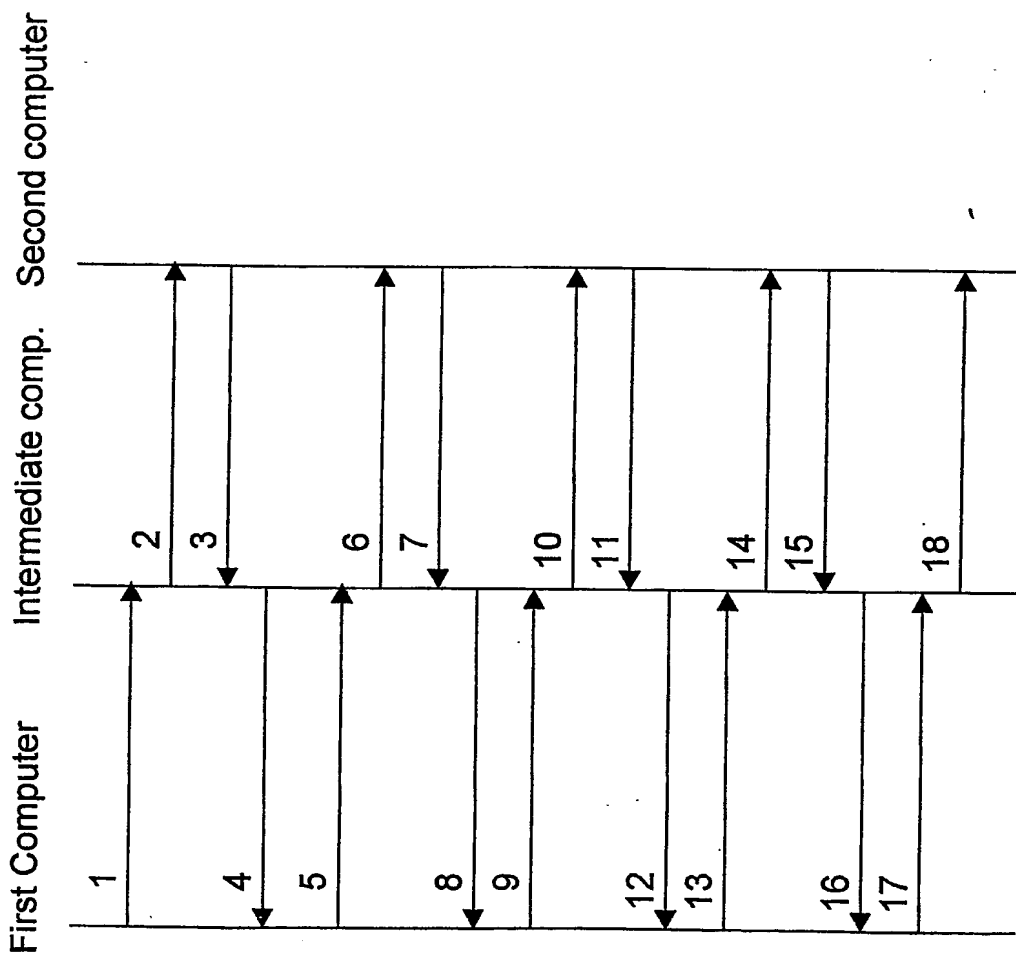
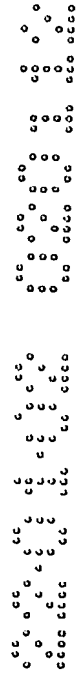


FIG. 4



Mapping field	Stage 1	Stage 2	Stage 3	Stage 4
c-addr-1	195.1.2.3	195.1.2.3	195.1.2.3	195.1.2.3
c-addr-2	212.90.65.1	212.90.65.1	212.90.65.1	212.90.65.1
c-icky	CKY1	CKY1	CKY1	CKY1
c-rcky	0	0	0	CKY4
c-userid	joe@netseal.com	joe@netseal.com	joe@netseal.com	joe@netseal.com
s-addr-2	n/a	212.90.65.1	212.90.65.1	212.90.65.1
s-addr-3	n/a	103.6.5.4	103.6.5.4	103.6.5.4
s-icky	n/a	CKY2	CKY2	CKY2
s-rcky	n/a	0	CKY3	CKY3

5/6
L6

FIG. 5

6/6

LG

Identification type	Identification value	SGW address
User@Fully-Qualified-Domain-Name	<u>*.smith@netseal.com</u>	123.1.2.3
<u>user@Fully-Qualified-Domain-Name</u>	<u>*@netseal.com</u>	103.6.5.4
Distinguished Name	"CN=Sami Vaarala, DC=netseal, DC=com"	122.4.3.2
Fully-Qualified-Domain-Name	host4.roammate.com	123.3.2.1
Employee number and company	"190170 / NetSeal Technologies"	123.4.3.2
...

FIG. 6

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT OR DRAWING
- BLURRED OR ILLEGIBLE TEXT OR DRAWING
- SKEWED/SLANTED IMAGES
- COLOR OR BLACK AND WHITE PHOTOGRAPHS
- GRAY SCALE DOCUMENTS
- LINES OR MARKS ON ORIGINAL DOCUMENT
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

DO/EO WORKSHEET

U.S. Appl. No. 10/0930

International

F103/00045

Application filed by: 20 months 30 months

WIPO PUBLICATION INFORMATION:

Publication No.: WO 03/063443 Publication Language: English
Publication Date: 31 Jul 03 Not Published: U.S. only designated
 EP request

SEARCHING & INDEXING
National Sta
Paralegal Sr
7031 305-3

INTERNATIONAL APPLICATION PAPERS IN THE APPLICATION FILE

- International Application (RECORD COPY)
- Article 19 Amendments
- PCT/IB/331
- PCT/IPEA/409 INER (PCT/IPEA/416 on front)
- Annexes to 409
- Priority Document (s) No. 1
- International Appl. on Double Sided Paper (CO)
- Request form PCT/RO/101
- PCT/ISA/210 - Search Report
- Search Report References
- Other: _____

RECEIPTS FROM THE APPLICANT (other than checked above):

- Basic National Fee (paid or authorized to charge)
- Preliminary Amendment(s) Filed on: 07/08/04
- Description
- Information Disclosure Statement(s) Filed on: _____
- Claims
- Assignment Document
- Words in the Drawing Figure(s)
- Power of Attorney/ Change of Address
- Article 19 Amendments
- Substitute Specification Filed on: _____
- Annexes to 409
- entered not entered
- Oath/ Declaration (executed)
- Verified Small Status Claim
(if submitted after Receipt Date - Is it timely? Y/N)
- DNA Diskette
- Other: _____

NOTES:

35 U.S.C. 371 - Receipt of Request (PTO-1390)

Date Acceptable Oath/ Declaration Received

Date Complete 35 U.S.C. 371

102(e) Date

Date of Completion of DO/EO 906 - Notification of Missing 102(e) Requirements

Date of Completion of DO/EO 907 - Notification of Acceptance for 102(e) Date

Date of Completion of DO/EO 911 - Application Accepted Under 35 U.S.C. 111

Date of Completion of DO/EO 905 - Notification of Missing Requirements

Date of Completion of DO/EO 916 - Notification of Defective Response

Date of Completion of DO/EO 903 - Notification of Acceptance

07/08/04

10/19/05

10/19/05

10/19/05

12/10/04

04/08/06

PCT

07/500930
REC'D 19 APR 2004

INTERNATIONAL PRELIMINARY EXAMINATION REPORT PCT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference S0049PCT	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/PEA/416)	
International application No. PCT/FI 03/00045	International filing date (day/month/year) 21.01.2003	Priority date (day/month/year) 22.01.2002
International Patent Classification (IPC) or both national classification and IPC H04L29/06		
Applicant INTRASECURE NETWORKS OY et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.



2. This REPORT consists of a total of 5 sheets, including this cover sheet.

This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 5 sheets.

3. This report contains indications relating to the following items:

- I Basis of the opinion
- II Priority
- III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV Lack of unity of invention
- V Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI Certain documents cited
- VII Certain defects in the international application
- VIII Certain observations on the international application

Date of submission of the demand 19.08.2003	Date of completion of this report 16.04.2004
Name and mailing address of the international preliminary examining authority:  European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized Officer Kopp, K Telephone No. +49 89 2399-7833 

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. PCT/FI 03/00045

I. Basis of the report

1. With regard to the **elements** of the international application (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17)*):

Description, Pages

1-38 as originally filed

Claims, Numbers

1-26 filed with telefax on 17.03.2004

Drawings, Sheets

1/6-6/6 as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language: , which is:

- the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
 - the language of publication of the international application (under Rule 48.3(b)).
 - the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).
3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:
- contained in the international application in written form.
 - filed together with the international application in computer readable form.
 - furnished subsequently to this Authority in written form.
 - furnished subsequently to this Authority in computer readable form.
 - The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
 - The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

- the description, pages:
- the claims, Nos.:
- the drawings, sheets:

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. **PCT/FI 03/00045**

5. This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)).

(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes: Claims	3,6,11,12,13,14,15,16,17,18,19,20,21
	No: Claims	1,2,4,5,7,8,9,10,22,23,24,25,26
Inventive step (IS)	Yes: Claims	
	No: Claims	1-26
Industrial applicability (IA)	Yes: Claims	1-26
	No: Claims	

2. Citations and explanations

see separate sheet

Re Item V

Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. The following documents (D) are mentioned:

- D1: US 2001/047487 A1 (LINNAKANGAS TOMMI ET AL) 29 November 2001 (2001-11-29)
- D2: US 2001/009025 A1 (AHONEN PASI MATTI KALEVI) 19 July 2001 (2001-07-19)
- D3: WO 00 78008 A (SSH COMM SECURITY LTD ;KIVINEN TERO (FI); YLOENEN TATU (FI)) 21 December 2000 (2000-12-21)
- D4: US 2001/020273 A1 (MURAKAWA YASUSHI) 6 September 2001 (2001-09-06)

2. Claim 22 lacks novelty (Article 33(2) PCT).

2.1 Document D1, which is considered to represent the most relevant state of the art for claim 1, discloses according to the subject-matter of claim 1:

- Telecommunication network for secure forwarding of messages, comprising at least a first computer, a second computer and an intermediate computer (paragraph 24, lines 4-8)

characterized in that

- the first and the second computers have means to perform IPSec processing (paragraph 24, lines 4-8),
- and the intermediate computer have translation tables to perform IPSec and IKE translation (paragraph 24, lines 11-15).

3. The features of independent claim 22 are also disclosed in any of D2 (see e.g. figures 1, 5; paragraphs 4, 5, 48), D3 (see e.g. page 3, line 24 - page 4, line 10; page 9, lines 7 - 13; figures 1a, 1b, 3) and D4 (see e.g. paragraphs 71-76).

4. If novelty were disputable based on minor differences of interpretation, it is pointed out that the subject-matter of claim 22 would still not involve an inventive step (Article 33(3) PCT).

5. The subject-matter of independent method claim 1 corresponds to the subject-matter of independent apparatus claim 22. Thus, claim 1 also lacks novelty (Article 33(2) PCT).

6. Dependent claims do not contain any subject-matter which, in combination with the subject-matter to which they refer, meet the requirements of the PCT in respect of novelty and inventive step (Article 33(2) and (3) PCT). They are either disclosed in D1 (e.g. "the secure message is formed by using an IPSec connection between the first computer and the second computer"; "preceding distribution of keys for forming the IPSec connection is performed by an automated key exchange protocol"), in D2 (e.g. "the request for registration is encrypted") or common measures (e.g. "forwarding of the message is performed by making use of the SSL or TLS protocols"; "the secure message is sent using IPSec tunnel mode"; "the secure message is sent using IPSec transport mode") obvious for a person skilled in the art.

REPLACED BY
ART 34 AMDT

10/500930

CLAIMS

1. Method for secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network,
5 c h a r a c t e r i z e d b y
- a) forming a message in the first computer or in a computer that is served by the first computer, and in the latter case sending the message to the first computer,
 - b) in the first computer, forming a secure message by giving the message a unique identity and a destination address,
 - 10 c) sending the message from the first computer to the intermediate computer,
 - d) using said destination address and the unique identity to find an address to the second computer,
 - e) substituting the current destination address with the found address to the second computer,
 - 15 f) substituting the unique identity with another unique identity,
 - g) forwarding the message to the second computer.
2. Method of claim 1, c h a r a c t e r i z e d in that the secure forwarding of the message is performed by making use of the IPSec protocols, whereby the secure
20 message is formed in step b) by using an IPSec connection between the first computer and the second computer formed for this purpose in the method.
3. Method of claim 1, c h a r a c t e r i z e d in that the secure forwarding of the message is performed by making use of the SSL or TLS protocols.
- 25
4. Method of claim 2, c h a r a c t e r i z e d in that a preceding distribution of keys to the components for forming the IPSec connection is performed manually.
5. Method of claim 2, c h a r a c t e r i z e d in that a preceding distribution of keys for
30 forming the IPSec connection is performed by an automated key exchange protocol.

- 5 6. Method of claim 5, characterized in that the automated key exchange protocol between the first computer and the second computer is performed by means of a modified IKE key exchange protocol between the first computer and the intermediate computer and a standard IKE key exchange protocol between the intermediate computer and the second computer.
- 10 7. Method of any of claims 2, 5 or 6, characterized in that the message that is sent from the first computer in step c) is a packet and 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, a unique identity, and other security parameters.
- 15 8. Method of any of claims 2, 5 or 6, characterized in that that the IPSec connection is one or more security associations (SA) and the unique identity is one or more SPI values and the other security parameters include the sequence number(s).
- 20 9. Method of any of claims 1 – 8, characterized in that the matching in step d) is performed by means of a translation table stored at the intermediate computer.
- 25 10. Method of any of claims 1 - 9, characterized in that both the address and the SPI-value are changed by the intermediate computer in steps e) respective f).
- 30 11. Method of any of claims 1 - 10, characterized in that the first computer is a mobile terminal, whereby the mobility is enabled by modifying the translation table at the intermediate computer.
12. Method of claim 11, characterized in that said modification of the translation tables is performed by sending a request for registration of the new address from the first computer to the intermediate computer, and optionally, by sending a registration reply from the intermediate computer to the first computer.

**REPLACED BY
PART 34 AMDT**

13. Method of claim 12, characterized in that the registration and/or reply is authenticated and/or encrypted by IPSec.
14. Method of any of claims 4 -13, characterized in that the key distribution for the secure connections is established 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.
15. Method of claim 14, characterized in that the key exchange distribution is established 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,
using a translation table to modify IKE packets in flight by modifying the external IP addresses and possibly IKE cookies of the IKE packets.
16. Method of claim 14 or 15, characterized in that the modified IKE protocol between the first computer and the intermediate computer is modified such that the IKE keys are transmitted from the first computer to the intermediate computer for decryption and modification of IKE packets.
17. Method of claim 14 or 15, characterized in that in the modified IKE protocol between the first computer and the intermediate computer the modification of the IKE packets is done by the first computer with the intermediate computer requesting such modifications.
18. Method of claim 16, characterized in that the address is defined 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.

19. Method of any of claims 1 -18, characterized in that the secure message is sent using IPSec transport mode.
20. Method of any of claims 1 -18, characterized in that the secure message is sent using IPSec tunnel mode.
21. Telecommunication network for secure forwarding of messages, comprising at least a first computer, a second computer and an intermediate computer, characterized in that the first and the second computers have means to perform IPSec processing, and the intermediate computer have means to perform IPSec translation.
22. Network of claim 21, characterized in that the intermediate computer furthermore has means to perform IKE translation.
23. Network of claim 21 or 22, characterized in that the means to perform IPSec translation and IKE translation consists of translation tables.
24. Network of claim 22, characterized in that the translation table for IPSec translation comprising IP addresses of the intermediate computer to be matched with IP addresses of the second computer.
25. Network of claim 22, characterized in that one of the mapping 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.
26. Network of claim 25, characterized in that both partitions of the mapping table for IKE translation contains translation fields for the source IP address, the destination IP address, initiator and responder cookies between respective computers.

REPLACED BY
PART 3A AMBT

27. Network of claim 28, characterized in that there is another translation table for IKE translation containing fields for matching a given user to a given second computer.

10/500930

500,930

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
31 July 2003 (31.07.2003)

PCT

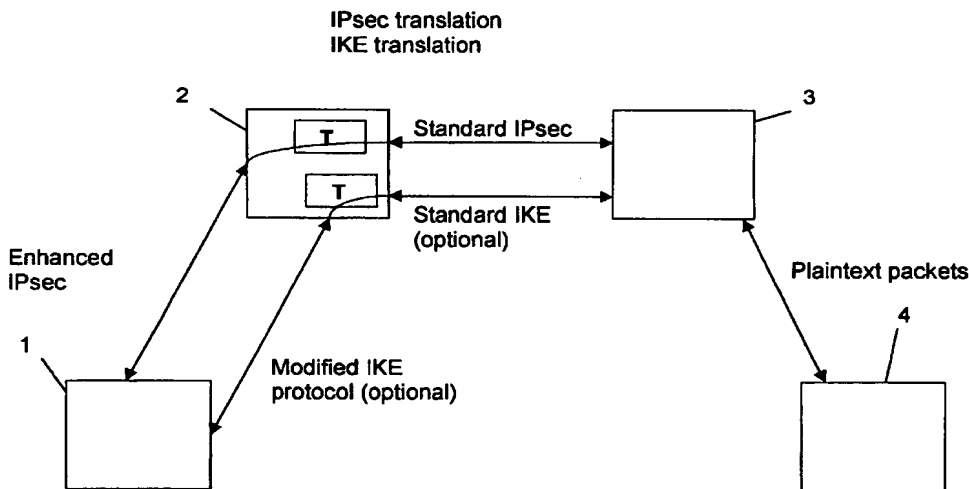
(10) International Publication Number
WO 03/063443 A1

- (51) International Patent Classification⁷: H04L 29/06, H04Q 7/38
- (74) Agent: INNOPAT LTD; P.O. Box 556, FIN-02151 Espoo (FI).
- (21) International Application Number: PCT/FI03/00045
- (81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (22) International Filing Date: 21 January 2003 (21.01.2003)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data: 20020112 22 January 2002 (22.01.2002) FI
- (84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).
- (71) Applicant (*for all designated States except US*): IN-TRASECURE NETWORKS OY [FI/FI]; PL 38, FIN-02201 Espoo (FI).
- (72) Inventors; and
- (75) Inventors/Applicants (*for US only*): VAARALA, Sami [FI/FI]; Neljäs Linja 22 A, FIN-00530 Helsinki (FI). NUOPPONEN, Antti [FI/FI]; Kaksoiskiventie 7-9 A 1, FIN-02760 Espoo (FI).

Published:
 — with international search report
 — before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

[Continued on next page]

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



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

WO 03/063443 A1

WO 03/063443 A1



For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION

5 TECHNICAL FIELD

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

10

TECHNICAL BACKGROUND

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

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

25 There is a need to protect data and resources from disclosure, to guarantee the authenticity of data, and to protect systems from network based attacks. More in detail, there is a need for confidentiality (protecting the contents of data from being read), integrity (protecting the data from being modified, which is a property that is independent of confidentiality), authentication (obtaining assurance about the actual
30 sender of data), replay protection (guaranteeing that data is fresh, and not a copy of previously sent data), identity protection (keeping the identities of parties exchanging data secret from outsiders), high availability, i.e. denial-of-service protection (ensuring

that the system functions even when under attack) and access control. IPSec is a technology providing most of these, but not all of them. (In particular, identity protection is not completely handled by IPSec, and neither is denial-of-service protection.)

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

15
IPSec can encrypt and/or authenticate traffic at IP level. Traffic going in to a WAN is typically compressed and encrypted and traffic coming from a WAN is decrypted and decompressed. IPSec is defined by certain documents, which contain rules for the IPSec architecture. The documents that define IPSec, are, for the time being, the Request For Comments (RFC) series of the Internet Engineering Task Force (IETF), in particular, RFCs 2401-2412.

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

30 Security association (SA) is a key concept in the authentication and the confidentiality mechanisms for IP. A security association is a one-way relationship between a sender

and a receiver that offers security services to the traffic carried on it. If a secure two-way relationship is needed, then two security associations are required. If ESP and AH are combined, or if ESP and/or AH are applied more than once, the term *SA bundle* is used, meaning that two or more SAs are used. Thus, SA bundle refers to one or more SAs applied in sequence, e.g. by first performing an ESP protection, and then an AH protection. The SA bundle is the combination of all SAs used to secure a packet.

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

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

In each IPsec implementation, there is a nominal security association data base (SADB) that defines the parameters associated with each SA. A security association is normally defined by the following parameters. The Sequence Number Counter is a 32-bit value used to generate the sequence number field in AH or ESP headers. The Sequence Counter Overflow is a flag indicating whether overflow of the sequence number counter should generate an auditable event and prevent further transmission of packets on this SA. An Anti-Replay Window is used to determine whether an inbound AH or ESP packet is a replay. AH information involves information about the authentication algorithm, keys and related parameters being used with AH. ESP

information involves information of encryption and authentication algorithms, keys, initialisation vectors, and related parameters being used with IPsec. AH information consists of the authentication algorithm, keys and related parameters being used with AH. ESP information consists of encryption and authentication algorithms, keys, cryptographic initialisation vectors and related parameters being used with ESP. The sixth parameter, Lifetime of this Security Association, is a time-interval and/or byte-count after which this SA must be replaced with a new SA (and new SPI) or terminated plus an indication of which of these actions should occur. IPsec Protocol Mode is either tunnel or transport mode. Maximum Transfer Unit (MTU), an optional feature, defines the maximum size of a packet that can be transmitted without fragmentation. Optionally an MTU discovery protocol may be used to determine the actual MTU for a given route, however, such a protocol is optional.

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

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

Tunnel mode provides protection to the entire IP packet and is usually used for sending messages through more than two components, although tunnel mode may also be used for end-to-end communication between two hosts. Tunnel mode is often used when one or both ends of a SA is a security gateway, such as a firewall or a router that implements IPsec. With tunnel mode, a number of hosts on networks behind firewalls may engage in secure communications without implementing IPsec. The unprotected packets generated by such hosts are tunnelled through external networks by tunnel mode SAs set up by the IPsec software in the firewall or secure router at boundary of the local network.

To achieve this, after the AH or ESP fields are added to the IP packet, the entire packet plus security fields are treated as the payload of a new outer IP packet with a

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

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

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

The key management portion of IPSec involves the determination and distribution of secret keys. The default automated key management protocol for IPSec is referred to as ISAKMP/Oakley and consists of the Oakley key determination protocol and Internet Security Association and Key Management Protocol (ISAKMP). Internet key exchange

(IKE) is a newer name for the ISAKMP/Oakley protocol. IKE is based on the Diffie-Hellman algorithm and supports RSA signature authentication among other modes. IKE is an extensible protocol, and allows future and vendor-specific features to be added without compromising functionality.

5

IPSec has been designed to provide confidentiality, integrity, and replay protection for IP packets. However, IPSec is intended to work with static network topology, where hosts are fixed to certain subnetworks. For instance, when an IPSec tunnel has been formed by using Internet Key Exchange (IKE) protocol, the tunnel endpoints are fixed and remain constant. If IPSec is used with a mobile host, the IKE key exchange will have to be redone from every new visited network. This is problematic, because IKE key exchanges involve computationally expensive Diffie-Hellman key exchange algorithm calculations and possibly RSA calculations. Furthermore, the key exchange requires at least three round trips (six messages) if using the IKE aggressive mode followed by IKE quick mode, and nine messages if using IKE main mode followed by IKE quick mode. This may be a big problem in high latency networks, such as General Packet Radio Service (GPRS) regardless of the computational expenses.

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

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

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

30

In the scenario, there is a standard IPSec security gateway, which is used by a mobile

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

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

Standard IPsec does e.g. not work through NAT devices at the moment. A standard IPsec NAT traversal protocol is currently being specified, but the security gateway in
20 the scenario might not support an IPsec protocol extended in this way. Furthermore, the current IPsec NAT traversal protocols are not well suited to mobility.

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

A known method of solving some of these problems is based on having an intermediate host between the mobile terminal and the IPsec security gateway. The
30 intermediate host might be a Mobile IP home agent, that provides mobility for the connection between the mobile terminal and the home agent, while the connection from the mobile node to the security gateway is an ordinary IPsec connection. In this

case, packets sent by an application in the mobile client are first processed by IPSec, and then by Mobile IP.

In the general case, this implies both Mobile IP and IPSec header fields for packets exchanged by the mobile terminal and the home agent. The Mobile IP headers are removed by the home agent prior to delivering packets to the security gateway, and added when delivering packets to the mobile terminal. Because of the use of two tunnelling protocols (Mobile IP and IPSec tunnelling), the solution is referred to as "double tunnelling" in this document.

10

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

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

20 The mobile host would now establish an IPSec connection between itself and the intermediate host, and would also establish an IPSec connection between itself and the IPSec security gateway. This solution is similar to the first known method, except that two IPSec tunnels are used. It solves a different set of problems – for instance, NAT traversal – but also adds packet size overhead because of double IPSec tunnelling.

25

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

30

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

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

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

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

30 THE OBJECT OF THE INVENTION

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

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

SUMMARY OF THE INVENTION

10

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

The advantageous embodiments have the characteristics of the subclaims.

- 25 Preferably, the first computer processes the formed message using a security protocol and encapsulates the message at least in an outer IP header. The outer IP header source address is the current address of the first computer, while the destination address is that of the intermediate computer. The message is then sent to the intermediate computer, which matches the outer IP header address fields together with
30 a unique identifier used by the security protocol, and performs a translation of the outer addresses and the unique identity used by the security protocol. The translated packet is then sent to the second computer, which processes it using the standard security

protocol in question. In the method of the invention, there is no extra encapsulation overhead as in the prior art methods. Also, the intermediate computer does not need to undo the security processing, e.g. decryption, and thus does not compromise security as in the prior art methods.

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

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

25 Thus, the unsecured data packet message is formed by the sending computer, which may or may not be the first computer. The IP header of this packet has IP source and destination address fields (among other things). The packet is encapsulated e.g. wrapped inside a tunnel, and the resulting packet is secured. The secured packet has a new outer IP header, which contains another set of IP source and destination addresses (in the outer header – the inner header is untouched), i.e. there are two
30 outer addresses (source and destination) and two inner addresses. The processed packet has a unique identity, the IPsec SPI value(s).

An essential idea of the invention is to use the standard protocol (IPsec) between the

intermediate computer and the second computer and an "enhanced IPsec protocol" between the first computer and the intermediate computer. IPsec-protected packets are translated by the intermediate computer, without undoing the IPsec processing. This avoids both the overhead of double tunneling, and the security problem involved in using separate tunnels.

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

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

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

In the signalling, e.g. a registration request is sent from the first computer to the intermediate computer which causes the intermediate computer to modify the addresses in the mapping table and thus, the intermediate computer can identify the mobile next time a message is sent. Preferably, as a result of a registration request, a reply registration is sent from the intermediate computer back to the first computer.

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

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

10

Such a protocol can be easily based on e.g. IPsec sequence number field and the replay protection window, which provide a way to detect that packet(s) have been lost. When a receiving host detects missing packets, it can send a request message for those particular packets. The request can of course be piggy-backed on an existing data packet that is being sent to the other host. Another method of doing the retransmissions may be based on using an extra protocol inside which the IPSec packets are wrapped for transmission between the first and intermediate computer. In any case, the second computer remains unaware of such a retransmission protocol.

15

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

25

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

30

translation, preferably by means of mapping tables. The intermediate computer may perform IPSec processing related to other features, such as mobility signalling described above or other enhancements.

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

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

- 20 Each translation table consists of entries that are divided into two partitions. The first partition contains information fields related to the connection between the first computer and the intermediate computer, while the second partition contains information fields related to the connection between the intermediate computer and the second computer.

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

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

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

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

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

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

25

FIGURES

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

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

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

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

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

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

10 DETAILED DESCRIPTION OF THE INVENTION

An example of a telecommunication network of the invention is illustrated in figure 1, comprising a first computer, here a client computer 1 served by an intermediate computer, here as a server 2, and a host computer 4, that is served by the second
15 computer, here a security gateway (SGW) 3. The security gateway supports the standard IPSec protocol and optionally the IKE key exchange protocol. The client computer and the server computer support a modified IPSec and IKE protocol.

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

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

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

address and IPSec SPI translations for the packets. These translations accomplish the effect of "double tunnelling" (described in the technical background section), but with the method of the invention the confidentiality of the packets is not compromised, while simultaneously having no extra overhead when compared to standard IPSec.

5 The intermediate computer does not know the cryptographic keys used to encrypt and/or authenticate the packets, and can thus not reveal their contents.

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

15 In the example of figure 1, an IPSec connection is formed between the client computer 1 (the first computer) and the security gateway 3 (the second computer). To create an IPSec tunnel, a SA (or usually a SA bundle) is formed between the respective computers with a preceding key exchange. The key exchange between the first and the second computer can take place manually or it can be performed with an automatic
20 key exchange protocol such as the IKE protocol. For performing said key exchange, a standard IKE protocol is used between the server 2 and the security gateway 3, and a modified IKE protocol is used between the client computer 1 and the server 2. An example of a modified IKE protocol that can be used in the invention is described in connection with figure 4.

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

30 The method of the invention, wherein messages in packet form are sent by routing to the end destination, is generally described in connection with figure 2. It is assumed in

the following description that the IPsec connection between the first and second computer already is formed. The IPsec connection can be set up manually or automatically by e.g. an IKE exchange protocol which is described later.

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

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

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

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

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

The processing of packets in the intermediate computer is based on a translation table i.e. an IPSec translation table shown in figure 3. The table has been divided into two partitions. The left one, identified by the prefix "c-", refers to the network connection between the first computer (host 1 in figure 1) and the intermediate computer (host 2 in figure 1). The right one, identified by the prefix "s-", refers to the network connection between the intermediate computer and the second computer (computer 3 in figure 1). The postfix number ("-1", "-2", or "-3") identifies the host in question. Thus, the address fields ("addr") refer to outer addresses of a packet, while the SPI fields ("SPI") refer to the receiver of packets, which packets were sent with this SPI. Thus, "c-SPI-2" is the SPI value used by host 2 (the intermediate computer) when receiving packets from host 1 (the first computer), and the SPI-value "c-SPI-1" is the SPI-value with which the first computer receives messages and the SPI-value with which the intermediate computer sends messages to the first computer and so on.

In terms of Figure 3, the outer source address would be "c-addr-1" (195.1.2.3), the outer destination address "c-addr-2" (212.90.65.1), while the SPI field would be "c-SPI-2" (0x12341234). The notation 0xNNNNNNNN indicates a 32-bit unsigned integer value, encoded using a hexadecimal notation (base 16). The inner source address is processed by IPSec in the first computer, and would typically be encrypted. In this example, the inner source address would be the static address of the mobile terminal, e.g. 10.0.0.1.

When the intermediate computer receives the packet sent in step 1 described above, it performs an address and SPI translation, ensuring that the security gateway (host 3 of figure 1) can accept the packet. Most of the packet is secured using IPSec, and since the intermediate computer does not have the cryptographic keys to undo the IPSec processing done by the mobile terminal, it cannot decrypt any encrypted portions of the packet but is able to use the outer IP addresses and the incoming SPI value to determine how to modify the outer address and the SPI to suite the second computer, which is the next destination. SPI is now changed to 0x56785678 in the intermediate computer and the address is changed to the address of the second computer. This is done by means of the IPSec translation table of figure 3.

The first row of Figure 3 is a row that the intermediate computer has found that matches the packet in the example, and thus the intermediate computer chooses it for translation. The new outer source address s-addr-2 (212.90.65.1) is substituted for the outer source address c-addr-1 (195.1.2.3), and the new outer destination address s-addr-3 (103.6.5.4) is substituted for the outer destination address c-addr-2 (212.90.65.1). The new SPI value, s-SPI-3 (0x56785678), is substituted for the SPI value c-SPI-2 (0x12341234). If more than one SPI values are used, all the SPI values are substituted similarly. In the example, s-addr-2 and c-addr-2 happen to be the same on both partitions of the table. This is not necessarily so but the intermediate computer might use another address for sending.

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

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

In step 3 of figure 2, the packet is sent from the second computer (corresponding to SGW in figure 1) to host X, having now only the original source IP address 10.0.0.1 and the original destination IP address X in the IP header. Thus, in step 3, host X receives the packet sent by the second computer. Usually, an application process running on host X would generate some return traffic. This would cause an IP packet to be generated and sent to the second computer.

If a packet is sent back from host X to the first computer (corresponding to the client

computer in figure 1), steps analogous to steps 1 - 3 are performed. The packet is thus first sent to the second computer, with the source IP address being X and the destination IP address being 10.0.0.1, in step 4. The generated packet is then received by the second computer. The IPsec policy of the second computer requires that the packet be IPsec-processed using a tunnel mode IPsec SA. This processing is similar to the one in steps 1 and 2. A new, outer IP header is added to the packet in the second computer, after which the resulting packet is secured using the IPsec SA. The outer IP source address is set to s-addr-3 (103.6.5.4) while the outer IP destination address is set to s-addr-2 (212.90.65.1). The SPI field is set to s-SPI-2 (0xc1230012). In step 5, the resulting packet is sent to the address indicated by the new outer IP destination address, s-addr-2, the intermediate computer. The intermediate computer receives the packet and performs a similar address and SPI translation.

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

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

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

The first computer may be a mobile terminal, the outer address of which changes from time to time. The translation table is then modified using some form of signalling messages, as described in the summary section. Upon receiving a request for modifying a translation, the intermediate computer updates the related translation table entry to match the new information supplied by the first computer. The operation of the protocol then proceeds as discussed above.

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

Changes for using AH:

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

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

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

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

etc). Thus, the AH integrity check value is now correct.

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

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

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

When the mobile terminal receives the packet, it performs a translation of the current outer addresses and the SPI field for the original ones used by the second computer: s-addr-3 for the outer source address, s-addr-2 for the outer destination address, and s-SPI-2 for the SPI value. This reproduces the packet originally sent by the second computer, except possibly for fields not covered by AH. This operation restores the AH integrity check value to its original, correct value. The AH integrity check is then performed against these fields.

Key exchange considerations

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

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

5

The key exchange must appear as a standard key exchange according to the key exchange protocol supported by the security gateway (the second computer), such as IKE. Also, the overall key exchange performed by the first, intermediate, and second computer must establish not only cryptographic keys, but also the IPSec translation table entries. The overall key exchange protocol should not reveal the IPSec cryptographic keys to the intermediate computer to avoid even the potential for security problems.

10

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

15

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

25

30

The IKE framework supports several "sub-protocols" for phase 1 and phase 2. The required ones are "main mode" for phase 1, and "quick mode" for phase 2. These are

used as illustrations, but the invention is not limited to these sub-protocols of IKE.

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

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

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

25

The overall steps of the protocol are:

1. The first computer initiates the key exchange protocol by sending a message to the intermediate computer. This message is essentially the IKE main mode initiation message, with some modifications required for this application.
- 30 2. The intermediate computer determines which security gateway (second computer) to forward this IKE session to, and also establishes a preliminary IKE translation table entry based on the information available from the message.

3. The security gateway (the second computer) replies to the IKE main mode initiation message.
4. The intermediate computer completes the IKE mapping based on the reply message.
5. The modified IKE protocol run continues through IKE main mode (the phase 1 exchange), which is followed by quick mode (the phase 2 exchange). Extensions of standard IKE messages are used between the first computer and the intermediate computer to accomplish the extra goals required by this modified IKE protocol.

10

In figure 4, the IKE session is described message by message. The following text indicates the contents of each message, and how they are processed by the various hosts. There are six main mode messages in the protocol, named **mm1**, **mm2**, ..., **mm6**, and three quick mode messages, named **qm1**, **qm2**, and **qm3**.

15

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

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

- Local and remote IP address (c-addr-1, c-addr-2)
- Initiator and responder cookie (c-icky, c-rcky)
- 25 • IKE identification of the first computer (c-userid, e.g. joe@netseal.com)

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

- 30 • Local and remote IP address (s-addr-2, s-addr-3)
- Initiator cookie and responder cookie (s-icky, s-rcky).

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

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

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

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

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

IKE messages consists of an IKE header, which includes the cookie fields and

message ID field, and of a list of payloads. A payload has a type, and associated information.

5 Figure 4 considers an example of the routing of packets according to the invention considering IPsec security association set-up for distribution of keys. As in the foregoing figure 2, the session begins with sending a packet from the client (first computer) to the server (intermediate computer).

10 The key exchange is initiated by the first computer. Thus, in step 1 of figure 4, the first computer constructs **mm1**. The IP header of the message contains the following values:

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

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

- Initiator cookie: CKY1 (c-icky)
- Responder cookie: 0 (c-rcky)
- Message ID: 0

20 The message contains the following payloads:

- A Security Association (SA) payload, which contains the IKE phase 1 security policy offers from the first computer.
- The message may contain additional payloads, such as Vendor Identification (VID) payloads, certificate requests/responses, etc.
- 25 - A VID payload can be used to indicate that the first computer supports the protocol described here.

The message tail contains the following information:

- User identification type and value – the c-userid field. These are used by the intermediate computer to choose a security gateway to forward this session to. The identification type may be any of the IKE types, but additional types can be defined. An alternative to this field is to directly indicate the security gateway for forwarding. There are other alternatives
- 30

as well, but these are not essential to the invention.

In step 2, the **mm1** is received by the intermediate computer. The intermediate computer examines the message, and forms the preliminary IKE translation table entry. Figure 5, step 1 illustrates the contents of this preliminary entry. The c-userid field is sent in the **mm1** tail.

The intermediate computer then determines which security gateway to forward this IKE session to. The determination may be based on any available information, static configuration, load balancing, or availability requirements. The presented, simple method is to use the identification information in the **mm1** tail to look up the first matching identification type and value from a table. An example of such a table is presented in Figure 6.

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

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

In addition to determining the security gateway address, the intermediate computer determines which address it uses for communication between itself and the second

computer. The same address as is used for the communication between the first and the intermediate computer may be used, but a new address may also be used. The address can be determined using a table similar to the one in Figure 6, or the table of Figure 6 may be extended to include this address.

5

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

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

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

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

The IKE header is modified as follows:

- Initiator cookie: CKY2 (s-icky)
- Responder cookie: 0 (s-rcky)
- 20 - Message ID: 0

The message tail is removed. The VID payload that identifies support for this modified protocol is also removed. The mm1 is then forwarded to the second computer.

25 In step 3, the second computer responds with mm2. The IP header of the message contains the following values (step 3 in Figure 4):

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

30 The IKE header contains the following values:

- Initiator cookie: CKY2 (s-icky)
- Responder cookie: CKY3 (s-rcky)

- Message ID: 0

The message contains the following payloads:

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

There is no message tail.

In step 4, the mm2 is received by the intermediate computer. The intermediate computer updates its IKE translation table based on the received message. Step 3 in Figure 5 illustrates the contents of the translation table entry at this point.

The intermediate computer generates its own responder cookie, CKY4, and updates the translation table yet again. Step 4 in Figure 5 illustrates the entry at this point. After this step, the translation table entry is complete, and the address and cookie translations are performed as in steps 1 - 4 for the following messages.

The translated message contains the following IP header fields (Figure 4, step 4)

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

The translated IKE header contains the following fields:

- Initiator cookie: CKY1 (c-icky)
- Responder cookie: CKY4 (c-rcky)

The message contains the following payloads:

- The SA payload sent by the second computer.
- Any optional payloads sent by the second computer.

- A VID payload may be added to indicate support of this modified protocol to the first computer.

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

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

The message is then forwarded to the first computer.

10

In step 5, the first computer constructs **mm3**. The message contains the following payloads:

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

The message is sent to the intermediate computer.

20

In step 6, the **mm3** is forwarded to the second computer. The contents of the message are not changed, only the IP header addresses and the IKE cookies, in the manner described in steps 1 - 4.

25 In step 7, the second computer receives **mm3** and responds with **mm4**. The message contains the following payloads:

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

In step 8, the **mm4** is forwarded to the first computer.

In step 9, the first computer constructs **mm5**, which is the first encrypted message in the session. All subsequent messages are encrypted using the IKE session keys established from the previous Diffie-Hellman key exchange (the messages **mm3** and **mm4**) by means of hash operations, as described in the IKE specification. Note that the intermediate computer does not possess these keys, and can thus not examine the contents of any subsequent IKE messages. In fact, the intermediate computer has no advantage compared to a hostile attacker if it attempts to decipher the IKE traffic. Instead, the intermediate computer indirectly modifies some fields in the IKE messages by sending a modification request in the IKE message tail to the first computer, which does the requested modifications before IKE encryption processing.

The message contains the following payloads:

- 15 - An Identification (ID) payload, that identifies the first computer to the second computer. This identification may be the same as the identification sent in the **mm1** tail, but may differ from that. These two identifications serve different purposes: the **mm1** tail identification (c-userid) is used to select a security gateway for IKE session forwarding (the second computer), while the ID payload in this message is used by the second computer for IKE authentication purposes, for instance, to select proper RSA authentication keys.
- 20 - A Signature (SIG) or Hash (HASH) payload, that serves as an authenticator. A signature payload is used if RSA- or DSS-based authentication is used, while a hash payload is used for pre-shared key authentication. There are other authentication methods in IKE, and IKE can also be extended with new authentication methods. These are not essential to the invention, and the following text assumes RSA authentication (i.e., use of the signature payload).
- 25 - Possibly optional IKE payloads.
- 30 - Possibly optional IKE payloads.

The message tail contains the following information:

- The SPI value that the first computer wants to use for receiving IPsec-protected messages from the intermediate computer, i.e., the c-SPI-1 value of the IPsec translation table in Figure 3. More than one SPI value could be transmitted here, but for simplicity, the following discussion assumes that only a single SPI is necessary (i.e. only one SA is applied for IPsec traffic processing). Extending the scheme to multiple SPIs is straightforward.

5

In step 10, the **mm5** is forwarded to the second computer.

10

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

15

In step 11, the second computer receives the **mm5** message, and authenticates the user (or the host, depending on what identification type is used). Assuming that the authentication succeeds, the second computer proceeds to authenticate itself to the first computer.

20

The **mm6** message contains the following payloads:

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

25

In step 12, the **mm6** is received by the intermediate computer. The intermediate computer does not change the message itself, but adds a tail with the following information:

30

- The SPI value that the intermediate computer wants the first computer to offer to the second computer in the **qm1** message. Since the intermediate computer cannot access the contents of the IKE messages, this modification request is made using the message tail (see the

discussion of step 9). The SPI value sent matches the s-SPI-2 field of the IPsec translation table of Figure 3.

- The SPI value that the intermediate computer wants the first computer to use for messages sent to itself. This matches the c-SPI-2 field of the IPsec translation table of Figure 3.

5

The resulting message is forwarded to the first computer.

In step 13, the first computer constructs **qm1**, which contains the following IKE payloads:

10

- A Hash (HASH) payload, that serves as an authenticator of the message.
- A Security Association (SA) payload, which contains the IKE phase 2 security policy offers from the first computer, i.e., the IPsec security policy offers. The SA payload contains the SPI value assigned to the first computer in the **mm6** message, i.e., s-SPI-2 in Figure 3.
- Optionally, a Key Exchange (KE) payload, if a new Diffie-Hellman key exchange is to be performed in phase 2 (this depends on the contents of the SA payload).
- A Nonce (NONCE) payload, which contains a random value chosen by the first computer.
- Optionally, two Identification (ID) payloads that indicate the IPsec traffic selectors that the first computer proposes for an IPsec tunnel mode SA. If IPsec transport mode is used, these are not necessary, but they may still be used. They may also be omitted if IPsec tunnel mode is used.

15

20

25

The IKE header is the same as previously, except that the Message ID field now contains a non-zero 32-bit value, that serves as a phase 2 session identifier. This identifier remains constant for the entire quick mode exchange.

30 The message is sent to the intermediate computer.

In step 14, the intermediate computer forwards the **qm1** message to the second

computer.

In step 15, the second computer inspects the security policy offers and other information contained in the **qm1** message, and determines which security policy offer matches its own security policy (the case when no security policies match results in an error notification message).

The second computer responds with **qm2** message, that contains the following payloads:

- 10 - A Hash (HASH) payload, that serves as an authenticator of the message.
- A Security Association (SA) payload, which indicates the security policy offer chosen by the second computer. The message also contains the SPI value that the second computer wants to use when receiving IPsec-protected messages. The SPI value matches s-SPI-3 of the IPsec translation table in Figure 3.
- 15 - Optionally, a Key Exchange (KE) payload, if a new Diffie-Hellman key exchange is to be performed in phase 2.
- A Nonce (NONCE) payload, which contains a random value chosen by the second computer.
- 20 - If Identification (ID) payloads were sent by the first computer, the second computer also sends Identification payloads.

In step 16, the intermediate computer forwards the **qm2** message to the first computer.

In step 17, the first computer constructs **qm3** message, which contains the following payloads:

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

The following information is sent in the message tail:

- 30 - The SPI value sent by the second computer in the **qm2** message. This is sent here, because the intermediate computer cannot decrypt the **qm2** message and look up the SPI from there. The SPI value matches s-SPI-3 of the IPsec translation table in Figure 3.

In step 18, the intermediate computer receives the **qm3** and reads the **s-SPI-3** value from the message tail. All the information required to construct the IPsec translation table entry is now gathered, and the entry can be added to the translation table. In particular, the information fields are as follows:

- 5 - **c-addr-1**: same as **c-addr-1** of the IKE session (195.1.2.3).
- **c-addr-2**: same as **c-addr-2** of the IKE session (212.90.65.1).
- **c-SPI-1**: received in the **mm5** message tail from the first computer.
- **c-SPI-2**: chosen by the intermediate computer, sent to the first computer in the **mm6** message tail.
- 10 - **s-addr-2**: same as **s-addr-2** of the IKE session (212.90.65.1 in this example, may be different than **c-addr-2**).
- **s-addr-3**: same as **s-addr-3** of the IKE session (103.6.5.4).
- **s-SPI-2**: chosen by the intermediate computer, sent to the first computer in **mm6** message tail.
- 15 - **s-SPI-3**: sent by the second computer in **qm2** to the first computer, which sends it to the intermediate computer in **qm3** message tail.

The intermediate computer forwards the **qm3** message to the second computer, which completes the IKE key exchange, and the IPsec translation table set up.

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

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

Some of these issues are the following:

- The phase 1 used main mode. Any other IKE phase 1 exchange can be used; this changes the details of the protocol but not the essential ideas.
- There are other approaches than the one presented here. One approach is for the first computer to reveal the IKE keys to the intermediate computer, so that the second computer is able to modify the required fields of the message (namely, SPI values).
- The discussion assumes that the first computer initiates the IKE exchange. The opposite direction is possible, too, but requires more considerations.
- The commit bit feature of IKE is not used. Adding that is simple.
- Security gateway selection is based on a table lookup indexed by an identification type/value pair sent by the first computer. Other mechanisms are easy to implement.
- The discussion assumes a successful IKE key exchange. Error cases are easy to handle.
- Phase 1 policy lookup (when processing **mm1** and **mm2** messages) is not based on the identity of the IKE counterpart. This is not a major issue, since the phase 1 security policy can be independent of the counterpart without limiting usability.
- Phase 1 is a pre-requisite for executing the protocol in the example. This can be easily changed by moving some of the "tail" items to phase 2.
- The protocol establishes a pair of SAs, one for each direction, and manages the SPI value modifications of these SAs. It is easy to extend this to cover SA bundles with more than one SA, i.e., SAs applied in sequence (ESP followed by AH, for instance). This requires more than one SPI for each direction, but is easy to add to the protocol described.

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

CLAIMS

1. Method for secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network,
5 c h a r a c t e r i z e d b y
- a) forming a message in the first computer or in a computer that is served by the first computer, and in the latter case sending the message to the first computer,
 - b) in the first computer, forming a secure message by giving the message a unique identity and a destination address,
 - 10 c) sending the message from the first computer to the intermediate computer,
 - d) using said destination address and the unique identity to find an address to the second computer,
 - e) substituting the current destination address with the found address to the second computer,
 - 15 f) substituting the unique identity with another unique identity,
 - g) forwarding the message to the second computer.
2. Method of claim 1, c h a r a c t e r i z e d in that the secure forwarding of the message is performed by making use of the IPSec protocols, whereby the secure
20 message is formed in step b) by using an IPSec connection between the first computer and the second computer formed for this purpose in the method.
3. Method of claim 1, c h a r a c t e r i z e d in that the secure forwarding of the message is performed by making use of the SSL or TLS protocols.
25
4. Method of claim 2, c h a r a c t e r i z e d in that a preceding distribution of keys to the components for forming the IPSec connection is performed manually.
5. Method of claim 2, c h a r a c t e r i z e d in that a preceding distribution of keys for
30 forming the IPSec connection is performed by an automated key exchange protocol.

- 5 6. Method of claim 5, characterized in that the automated key exchange protocol between the first computer and the second computer is performed by means of a modified IKE key exchange protocol between the first computer and the intermediate computer and a standard IKE key exchange protocol between the intermediate computer and the second computer.
- 10 7. Method of any of claims 2, 5 or 6, characterized in that the message that is sent from the first computer in step c) is a packet and 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, a unique identity, and other security parameters.
- 15 8. Method of any of claims 2, 5 or 6, characterized in that that the IPSec connection is one or more security associations (SA) and the unique identity is one or more SPI values and the other security parameters include the sequence number(s).
- 20 9. Method of any of claims 1 – 8, characterized in that the matching in step d) is performed by means of a translation table stored at the intermediate computer.
10. Method of any of claims 1 - 9, characterized in that both the address and the SPI-value are changed by the intermediate computer in steps e) respective f).
- 25 11. Method of any of claims 1 - 10, characterized in that the first computer is a mobile terminal, whereby the mobility is enabled by modifying the translation table at the intermediate computer.
- 30 12. Method of claim 11, characterized in that said modification of the translation tables is performed by sending a request for registration of the new address from the first computer to the intermediate computer, and optionally, by sending a registration reply from the intermediate computer to the first computer.

13. Method of claim 12, characterized in that the registration and/or reply is authenticated and/or encrypted by IPSec.
14. Method of any of claims 4 -13, characterized in that the key distribution for the secure connections is established 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.
15. Method of claim 14, characterized in that the key exchange distribution is established 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,
using a translation table to modify IKE packets in flight by modifying the external IP addresses and possibly IKE cookies of the IKE packets.
16. Method of claim 14 or 15, characterized in that the modified IKE protocol between the first computer and the intermediate computer is modified such that the IKE keys are transmitted from the first computer to the intermediate computer for decryption and modification of IKE packets.
17. Method of claim 14 or 15, characterized in that in the modified IKE protocol between the first computer and the intermediate computer the modification of the IKE packets is done by the first computer with the intermediate computer requesting such modifications.
18. Method of claim 16, characterized in that the address is defined 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.

19. Method of any of claims 1 -18, characterized in that the secure message is sent using IPSec transport mode.
20. Method of any of claims 1 -18, characterized in that the secure message is sent using IPSec tunnel mode.
21. Telecommunication network for secure forwarding of messages, comprising at least a first computer, a second computer and an intermediate computer, characterized in that the first and the second computers have means to perform IPSec processing, and the intermediate computer have means to perform IPSec translation.
22. Network of claim 21, characterized in that the intermediate computer furthermore has means to perform IKE translation.
23. Network of claim 21 or 22, characterized in that the means to perform IPSec translation and IKE translation consists of translation tables.
24. Network of claim 22, characterized in that the translation table for IPSec translation comprising IP addresses of the intermediate computer to be matched with IP addresses of the second computer.
25. Network of claim 22, characterized in that one of the mapping 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.
26. Network of claim 25, characterized in that both partitions of the mapping table for IKE translation contains translation fields for the source IP address, the destination IP address, initiator and responder cookies between respective computers.

27. Network of claim 28, characterized in that there is another translation table for IKE translation containing fields for matching a given user to a given second computer.

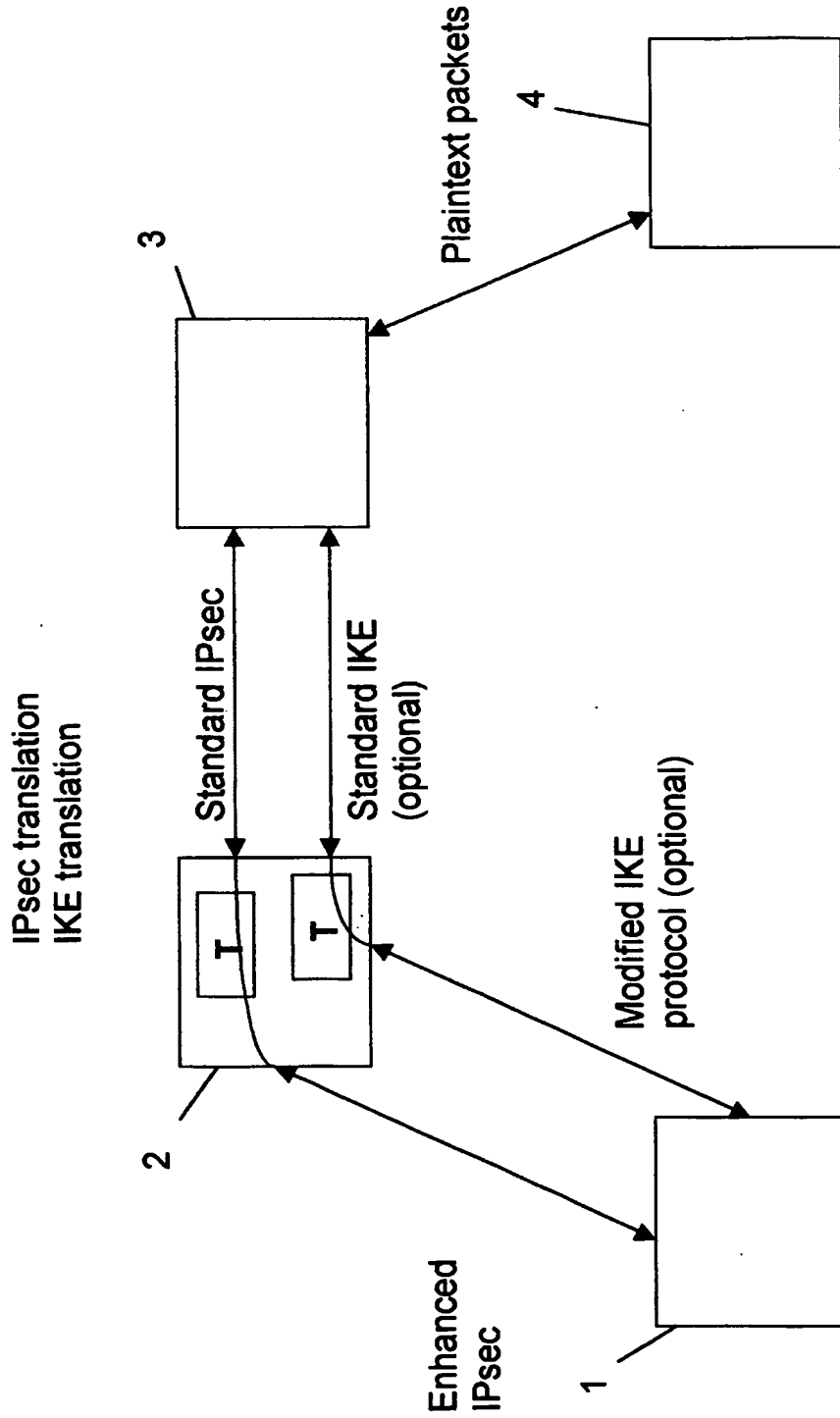


FIG. 1

2 / 6

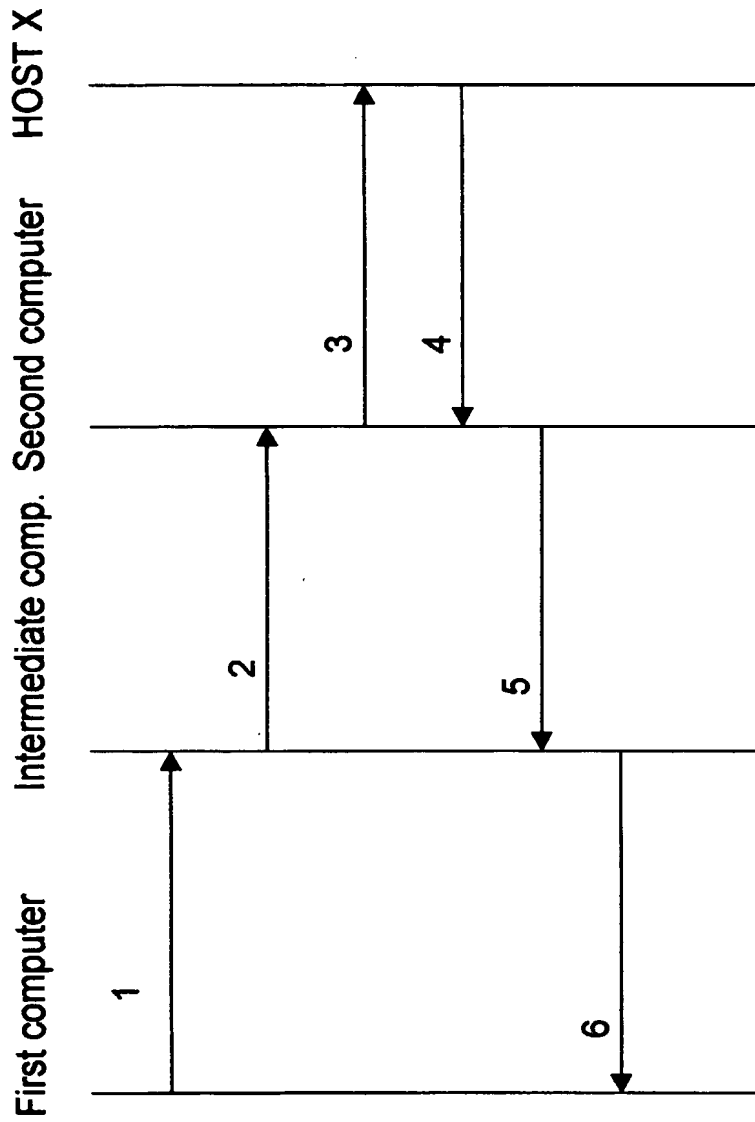


FIG. 2

c-addr-1	c-addr-2	c-SPI-1	c-SPI-2	s-addr-2	s-addr-3	s-SPI-2	s-SPI-3
195.1.2.3	212.90.65.1	0x80000001	0x12341234	212.90.65.1	103.6.5.4	0x1230012	0x56785678
...

3 / 6

FIG. 3

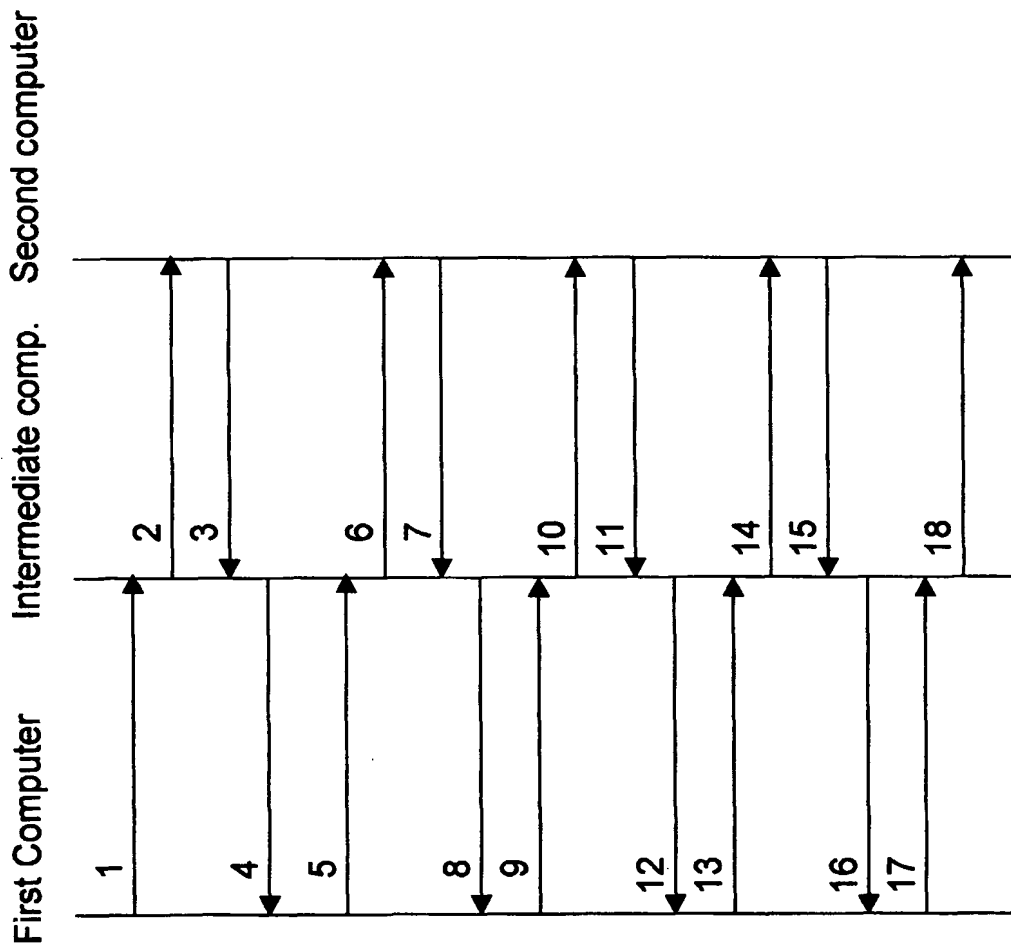


FIG. 4

Mapping field	Stage 1	Stage 2	Stage 3	Stage 4
c-addr-1	195.1.2.3	195.1.2.3	195.1.2.3	195.1.2.3
c-addr-2	212.90.65.1	212.90.65.1	212.90.65.1	212.90.65.1
c-icky	CKY1	CKY1	CKY1	CKY1
c-rcky	0	0	0	CKY4
c-userid	joe@netseal.com	joe@netseal.com	joe@netseal.com	joe@netseal.com
s-addr-2	n/a	212.90.65.1	212.90.65.1	212.90.65.1
s-addr-3	n/a	103.6.5.4	103.6.5.4	103.6.5.4
s-icky	n/a	CKY2	CKY2	CKY2
s-rcky	n/a	0	CKY3	CKY3

FIG. 5

6/6

Identification type	Identification value	SGW address
User@Fully-Qualified-Domain-Name	<u>*.smith@netseal.com</u>	123.1.2.3
<u>user@Fully-Qualified-Domain-Name</u>	<u>*@netseal.com</u>	103.6.5.4
Distinguished Name	"CN=Sami Vaarala, DC=netseal, DC=com"	122.4.3.2
Fully-Qualified-Domain-Name	host4.roammate.com	123.3.2.1
Employee number and company	"190170 / NetSeal Technologies"	123.4.3.2
...

FIG. 6

INTERNATIONAL SEARCH REPORT

International Application No
PCT/03/00045

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2001/047487 A1 (LINNAKANGAS TOMMI ET AL) 29 November 2001 (2001-11-29) paragraph [0006] - paragraph [0019] paragraph [0024] - paragraph [0029] paragraph [0033] paragraph [0040] paragraph [0062] abstract; claims 1-7; figures 1-3	1-10, 21-27
Y	---	1-27
Y	US 2001/009025 A1 (AHONEN PASI MATTI KALEVI) 19 July 2001 (2001-07-19) paragraph [0001] - paragraph [0008] paragraph [0018] - paragraph [0028] paragraph [0133] - paragraph [0137] paragraph [0145] - paragraph [0149] paragraph [0158] - paragraph [0164] abstract; claims 1-5,14,15; figures 1-4 ---	1-27
	-/--	

Further documents are listed in the continuation of box C.

Patent family members are listed in annex.

Special categories of cited documents:

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

5 May 2003

Date of mailing of the international search report

28 MAY 2003

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

NABIL SEBAA/JA A

INTERNATIONAL SEARCH REPORT

International Application No

PCT/FI 03/00045

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2001/020273 A1 (MURAKAWA YASUSHI) 6 September 2001 (2001-09-06) paragraph [0028] - paragraph [0035] abstract; claims 6,7; figures 1-3,8 ---	1-27
P,A	US 2002/147820 A1 (YOKOTE AKI) 10 October 2002 (2002-10-10) abstract; claims 1-3 ---	1-27
A	EP 1 094 682 A (ERICSSON TELEFON AB L M) 25 April 2001 (2001-04-25) paragraph [0027] - paragraph [0038]; claims 1,2,12-15; figures 1,3,4 ---	1-27
A	WO 00 78008 A (SSH COMM SECURITY LTD ;KIVINEN TERO (FI); YLOENEN TATU (FI)) 21 December 2000 (2000-12-21) page 3, line 24 - line 30 page 4, line 1 - line 10 abstract; claims 1-8; figure 3 -----	1-27

Information on patent family members

In International Application No
 .../EP 03/00045

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2001047487	A1 29-11-2001	GB 2365717 A AU 5690101 A EP 1284076 A2 WO 0191413 A2	20-02-2002 03-12-2001 19-02-2003 29-11-2001
US 2001009025	A1 19-07-2001	GB 2364477 A AU 2895801 A WO 0154379 A1	23-01-2002 31-07-2001 26-07-2001
US 2001020273	A1 06-09-2001	JP 2001160828 A CA 2327531 A1	12-06-2001 03-06-2001
US 2002147820	A1 10-10-2002	JP 2003051818 A US 2002157024 A1	21-02-2003 24-10-2002
EP 1094682	A 25-04-2001	EP 1094682 A1 AU 1133001 A CA 2388114 A1 WO 0131877 A2	25-04-2001 08-05-2001 03-05-2001 03-05-2001
WO 0078008	A 21-12-2000	AU 5225000 A EP 1186146 A1 WO 0078008 A1 JP 2003502913 T	02-01-2001 13-03-2002 21-12-2000 21-01-2003

BEST AVAILABLE COPY

PATENT APPLICATION FEE DETERMINATION RECORD
Effective October 1, 2003

Application or Docket Number:

10/500930

CLAIMS AS FILED - PART I

	(Column 1)	(Column 2)
TOTAL CLAIMS		
FOR	NUMBER FILED	NUMBER EXTRA
TOTAL CHARGEABLE CLAIMS	26 minus 20 =	-6
INDEPENDENT CLAIMS	2 minus 3 =	
MULTIPLE DEPENDENT CLAIM PRESENT <input type="checkbox"/>		

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

CLAIMS AS AMENDED - PART II

	(Column 1)	(Column 2)	(Column 3)
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
	Total	Minus	=
	Independent	Minus	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <input type="checkbox"/>			

	(Column 1)	(Column 2)	(Column 3)
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
	Total	Minus	=
	Independent	Minus	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <input type="checkbox"/>			

	(Column 1)	(Column 2)	(Column 3)
AMENDMENT C	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
	Total	Minus	=
	Independent	Minus	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <input type="checkbox"/>			

- * 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.

SMALL ENTITY TYPE

OR OTHER THAN SMALL ENTITY

RATE	FEE		RATE	FEE
BASIC FEE	400	OR	BASIC FEE	
XS 9=	54	OR	XS18=	
X43=		OR	X86=	
+145=		OR	-290=	
TOTAL	514	OR	TOTAL	

SMALL ENTITY OR

OTHER THAN SMALL ENTITY

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
XS 9=		OR	XS18=	
X43=		OR	X86=	
+145=		OR	+290=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
XS 9=		OR	XS18=	
X43=		OR	X86=	
+145=		OR	+290=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
XS 9=		OR	XS18=	
X43=		OR	X86=	
+145=		OR	+290=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	