DT02 Rec'd PCT/PTO 26 MAR 2004

RF:nz 3/26/04 290.1052USN

EXPRESS MAIL LABEL NO. ER625088509US
Date of Mailing: 26 March 2004

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

Attorney Docket No.: 290.1052USN

Int'l. Application No.:	PCT/FI02/00770
Int'l. Filing Date:	27 SEPTEMBER 2002
Priority Date Claimed:	28 SEPTEMBER 2001
Title of Invention:	METHOD AND NETWORK FOR ENSURING SECURE FORWARDING OF MESSAGES
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. [X] 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. [X] 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. [X] A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.

5. [X] 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. [X] 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. [X] 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. [X] 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. [X] An oath or declaration of the inventor (unsigned) (35 U.S.C. 371(c)(4)).

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

RF:nr 3/26/04 290.1052USN

EXPRESS MAIL LABEL NO. ER625088509US
Date of Mailing: 26 March 2004

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

13. [X] A FIRST preliminary amendment.

14. [X] 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. [X] 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	10 - 20	= 0	x $18.00 = $0.00
Ind. Claims	1 - 3	= 0	x $86.00 = $0.00

19. [X] Reduction by 1/2 for filing by small entity, if applicable. Applicant qualifies as small entity.
TOTAL FILING FEE: **$540.00**

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. [X] A check in the amount of **$540.00** to cover the above fee is enclosed.

23. [X] 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

RF:nz 3/26/04 290.1052USN

EXPRESS MAIL LABEL NO. ER625088509US
Date of Mailing: 26 March 2004

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

Attorney Docket No.: 290.1052USN

Int'l. Application No.:	PCT/FI02/00770
Int'l. Filing Date:	27 SEPTEMBER 2002
Priority Date Claimed:	28 SEPTEMBER 2001
Title of Invention:	METHOD AND NETWORK FOR ENSURING SECURE FORWARDING OF MESSAGES
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. [X] 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. [X] 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. [X] A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.

5. [X] 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. [X] 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. [X] 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. [X] 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. [X] An oath or declaration of the inventor (unsigned) (35 U.S.C. 371(c)(4)).

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

RF:nr 3/26/04 290.1052USN

EXPRESS MAIL LABEL NO. ER625088509US
Date of Mailing: 26 March 2004

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

13. [X] A FIRST preliminary amendment.

14. [X] 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. [X] 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	10 - 20	= 0	x $18.00 = $0.00
Ind. Claims	1 - 3	= 0	x $86.00 = $0.00

19. [X] Reduction by 1/2 for filing by small entity, if applicable. Applicant qualifies as small entity.
TOTAL FILING FEE: **$540.00**

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. [X] A check in the amount of **$540.00** to cover the above fee is enclosed.

23. [X] 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

PCT / FI 02 / 00770

METHOD AND NETWORK FOR ENSURING SECURE FORWARDING OF MESSAGES

TECHNICAL FIELD

The method and network of the invention is intended to secure mobile connections in telecommunication networks. Especially, it is meant for IPSec connections.

The invention provides a method for ensuring secure forwarding of a message in a telecommunication network, comprising at least one mobile terminal and another terminal, when the mobile terminal moves from a first address to a second address and there is a secure connection established between the first address of the mobile terminal and the other terminal, which secure connection defines at least the addresses of the two terminals. The invention also provides a network for performing such a method.

TECHNICAL BACKGROUND

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

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

There is a need to protect data and resources from disclosure, to guarantee the authenticity of data, and to protect systems from network based attacks. More in detail, there is a need for confidentiality (protecting the contents of data from being read), integrity (protecting the data from being modified, which is a property that is independent of confidentiality), authentication (obtaining assurance about 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.)

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

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

Two protocols are used to provide security at the IP layer, an authentication protocol designated by the header of the protocol, Authentication Header (AH), and a combined

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

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

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

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

In each IPSec implementation, there is a nominal security association data base (SADB) that defines the parameters associated with each SA. A security association is normally defined by the following parameters. The Sequence Number Counter is a 32-bit value used to generate the sequence number field in AH or ESP headers. The Sequence Counter Overflow is a flag indicating whether overflow of the sequence number counter should generate an auditable event and prevent further transmission of packets on this SA. An Anti-Replay Window is used to determine whether an inbound AH or ESP packet is a replay. AH information involves information about the authentication algorithm, keys and related parameters being used with AH. ESP information involves information of encryption and authentication algorithms, keys, initialisation vectors, and related parameters being used with IPSec. The sixth parameter, Lifetime of this Security Association, is a time-interval and/or byte-count after which a 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. Path MTU, which is an optional feature, defines the maximum size of a packet that can be transmitted without fragmentation.

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 that IPSec tunnelling).

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

networks by tunnel mode SAs set up by the IPSec software in the firewall or secure router at boundary of the local network.

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

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

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

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

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

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

The problem with standard IPSec tunnel end points are that they are fixed. A SA is bound to a certain IP address, and if it is changed, the existing IPSec SA becomes useless because it has been established by using different endpoint addresses. The problem has been discussed in the IETF standardisation forum, www.IETF.org, wherein an idea to support mobility for IPSec ESP tunnels by means of signalling to

update the address of one end after a movement was mentioned by Francis Dupont. No solutions have however been presented until this date.

The standard Mobile IP protocol provides a mobile terminal with a mobile connection, and defines mechanisms for performing efficient handovers from one network to another. However, Mobile IP has several disadvantages. The security of Mobile IP is very limited. The mobility signalling messages are authenticated, but not encrypted, and user data traffic is completely unprotected. Also, there is no key exchange mechanism for establishing the cryptographic keys required for authenticating the mobility signalling. Such keys need to be typically distributed manually. Finally, the current Mobile IP protocol does not define a method for working through Network Address Translation (NAT) devices.

A way to solve this problem is to use e.g. Mobile IP to handle the mobility of the host, and use IPSec on top of the static IP address provided by the Mobile IP. Thus, the IPSec SAs are bound to static addresses, and the IPSec SAs can survive mobility of the host. However, this approach suffers from packet size overhead of both Mobile IP and IPSec tunnels, which can affect performance considerably when using links with small throughput.

The documents that define IP in general are the RFC standards RFC 768, RFC 791, RFC 793, RFC 826 and RFC 2460. RFC 2002, RFC 2003, RFC 2131, RFC 3115, MOBILE Ipv4 and IPv6, and DHCPV6 define Mobile IP, IP-IP and DHCP.

Prior art solutions in this technical area are presented in WO 01 39538, WO 00 41427, WO 01 24560, US 2001/009025 and EP 1 24 397.

In WO 01 39538, WO 00 41427, WO 01 24560 and EP 1 24 397, a secure connection, which in the two first emntioned ones is an IPSec SA connection, is transferred from one access point to another in a hand-over situation of a mobile terminal. US 2001/009025 generally presents a secure communication method by means of an IP Sec SA connection.

ART 34 AMDT

REFERENCES

The following is a list of useful references of standards mentioned.

IP in general, TCP and UDP:

[RFC768]

J. Postel, *User Datagram Protocol*, RFC 768, August 1980.
ftp://ftp.isi.edu/in-notes/rfc768.txt

[RFC791]

J. Postel, *Internet Protocol*, RFC 791, September 1981.
ftp://ftp.isi.edu/in-notes/rfc791.txt

[RFC792]

J. Postel, *Internet Control Message Protocol*, RFC 792, September 1981.
ftp://ftp.isi.edu/in-notes/rfc792.txt

[RFC793]

J. Postel, *Transmission Control Protocol*, RFC 793, September 1981.
ftp://ftp.isi.edu/in-notes/rfc793.txt

[RFC826]

D.C. Plummer, *An Ethernet Address Resolution Protocol*, RFC 826, November 1982.
ftp://ftp.isi.edu/in-notes/rfc826.txt

[RFC2460]

S. Deering, R. Hinden, *Internet Protocol, Version 6 (IPv6) Specification*, RFC 2460, December 1998.

Mobile IP; IP-IP; DHCP:

[RFC2002]

C. Perkins, *IP Mobility Support*, RFC 2002, October 1996.
ftp://ftp.isi.edu/in-notes/rfc2002.txt

[RFC2003]

C. Perkins, *IP Encapsulation Within IP*, RFC 2003, October 1996.
ftp://ftp.isi.edu/in-notes/rfc2003.txt

[RFC2131]

R. Droms, *Dynamic Host Configuration Protocol*, RFC 2131, March 1997.
ftp://ftp.isi.edu/in-notes/rfc2131.txt

[RFC3115]

G. Dommety, and K. Leung, *Mobile IP Vendor/Organization-specific Extensions*, RFC 3115, April 2001.
ftp://ftp.isi.edu/in-notes/rfc3115.txt

[MOBILEIPv6]

D. B. Johnson, C. Perkins, *Mobility Support in IPv6*, Work in progress (Internet-Draft is available), July 2000.

[DHCPV6]

J. Bound, M. Carney, C. Perking, R.Droms, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*, Work in progress (Internet-Draft is available), June 2001.

IPsec standards:

[RFC2401]

S. Kent, and R. Atkinson, *Security Architecture for the Internet Protocol*, RFC 2401, November 1998.
ftp://ftp.isi.edu/in-notes/rfc2401.txt

[RFC2402]
S. Kent, and R. Atkinson, *IP Authentication Header*, RFC 2402, November 1998.
ftp://ftp.isi.edu/in-notes/rfc2402.txt

[RFC2403]
C. Madson, R. Glenn, The Use of HMAC-MD5-96 within ESP and AH, RFC 2403, November 1998.

[RFC2404]
C. Madson, R. Glenn, The Use of HMAC-SHA-1-96 within ESP and AH, RFC 2404, November 1998.

[RFC2405]
C. Madson, N. Doraswamy, The ESP DES-CBC Cipher Algorithm With Explicit IV, RFC 2405, November 1998.

[RFC2406]
S. Kent, and R. Atkinson, *IP Encapsulating Security Payload (ESP)*, RFC 2406, November 1998.
ftp://ftp.isi.edu/in-notes/rfc2406.txt

[RFC2407]
D. Piper, *The internet IP Security Domain of Interpretation for ISAKMP*, RFC 2407, November 1998.
ftp://ftp.isi.edu/in-notes/rfc2407.txt

[RFC2408]

D. Maughan, M. Schneider, M. Schertler, and J. Turner, *Internet Security Association and Key Management Protocol (ISAKMP)*, RFC 2408, November 1998.
ftp://ftp.isi.edu/in-notes/rfc2408.txt

[RFC2409]
D. Harkins, and D. Carrel, *The Internet Key Exchange (IKE)*, RFC 2409, November 1998.
ftp://ftp.isi.edu/in-notes/rfc2409.txt

[RFC2410]
R. Glenn, S. Kent, *The NULL Encryption Algorithm and Its Use With IPsec*, RFC 2410, November 1998.

[RFC2411]
R. Thayer, N. Doraswamy, R. Glenn, *IP Security Document Roadmap*, RFC 2411, November 1998.

[RFC2412]
H. Orman, *The OAKLEY Key Determination Protocol*, RFC 2412, November 1998.

NAT:

[RFC2694]
P. Srisuresh, G. Tsirtsis, P. Akkiraju, and A. Heffernan, *DNS extensions to Network Address Translators (DNS_ALG)*, RFC 2694, September 1999.

[RFC3022]
P. Shisuresh, K. Egevang, *Traditional IP Network Address Translator (Traditional NAT)*, RFC 3022, January 2001.
ftp://ftp.isi.edu/in-notes/rfc3022.txt

THE OBJECT OF THE INVENTION

The object of the invention is to ensure secure forwarding of messages from and to mobile terminals by avoiding the problems of prior art.

SUMMARY OF THE INVENTION

The method and network of the invention is to ensure secure forwarding of a message in a telecommunication network, comprising at least one first terminal and another terminal. In the method, the first terminal moves from a first address to a second address. A secure connection between the first address of the first terminal and the other terminal defining at least the addresses of the two terminals is established. The first terminal moves from the first address to a second address. The connection is changed to be between the second address and the other terminal by means of a request from the first terminal and preferably, a reply back to the first terminal.

In the invention, the first terminal is movable from one network to another. Such a terminal can physically be a mobile terminal or a fixed terminal.

The secure connection is an IPSec connection established by forming one or more Security Associations (SAs) using the IPSec protocols. The request and/or the reply message can be protected e.g. by IPSec encryption and/or authentication, possibly using the same IPSec SA that is used for traffic protection purposes.

In general, registration request and registration reply are Mobile IP terms while the invention is not bound to Mobile IP. In the invention, the terms request and reply are used in the generic sense, and may or may not be related to Mobile IP.

The method of the invention can be used in different kinds of networks. If the first terminal and the other terminal form an end-to-end connection, the secure connection may be an IPSec tunnel mode or transport mode connection. Furthermore, one of or

both of the first terminal and the other terminal can be a security gateway protecting one or more computers, whereby IPSec tunnel mode, or IPSec transport mode together with a tunnelling protocol (such as Layer 2 Tunnelling Protocol, L2TP), is used for the secure connection between the first terminal and the other terminal.

If both terminals are mobile, a special solution is required for the situation when both terminals move simultaneously in case of a so called "double jump" situation. This solution can be implemented e.g. by using a centralised registry of current locations of hosts, although other solutions exist for the problem. However, the "changeable" IPSec tunnel or transport mode SAs of the invention could be used in that case, too.

The applicant has solved the above problems of prior art by defining a signalling mechanism that allows an existing IPSec security association, that is, the symmetric encryption and authentication algorithms used for packet processing, along with their keys and other parameters, to be moved from one network to another. To be more precise, an existing IPSec tunnel endpoint can be moved in the invention from one point of attachment to another. For instance, an IPSec tunnel established between addresses A and X tunnel can be changed by using the defined signalling to be between addresses B and X, using only a single round trip for signalling (2 messages), or half a round trip (1 message, if a reply message is not used) for signalling. The solution requires minimal computational overhead compared to Diffie-Hellman or strong authentication calculations.

The signalling mechanism is preferably similar to the one in Mobile IP, i.e. a registration request (RREQ) is sent to the other end of the SA followed by a registration reply (RREP) back to the sender of the RREQ message, both of which are extensible for future features and optional attributes. The RREQ/RREP message pair is sent from the new network, and once properly authenticated, the sender IPSec tunnel endpoint is updated from the old network to the new network.

In case the security association used for protecting user traffic is also used for signalling purposes, the reception of the RREQ message by the other end of the SA

requires a change in a normal IPSec implementation to accept a packet that appears to belong to a certain IPSec tunnel, but comes from a wrong address (i.e. the tunnel is currently between A and X, and the RREQ comes from address B). This is only necessary for the RREQ message. Such an implementation is provided by the invention; it is necessary to modify IPSec if IPSec is used for the RREQ/RREP signalling. In that case, it is required specifically for processing of the RREQ and RREP messages, if the reply message is to be used.

The request message may update a set of security associations, for instance, a single security association, a security association bundle, an IPSec connection, a group of IPSec connections, or any combinations of these. In practice, it is useful to update either a single IPSec connection or a group of IPSec connections. The latter may be important if separate IPSec connections are used for different kinds of traffic. A single request message can then update all (or a certain set) of such connections to a new address, instead of requiring separate requests for each IPSec connection. In the following, the case of updating a single IPSec connection is discussed, without limiting the invention to this behaviour.

Another method of performing the signalling is to use a separate protocol. The protocol should preferably provide encryption and/or authentication of the signalling messages. The IKE protocol already has messages defined for e.g. deleting IPSec SAs. One method of providing the necessary signalling would be by adding a new IKE notification message type that requests a change in an existing IPSec SA. Such a message should provide its own encryption and/or authentication to avoid requiring an IKE connection set up from the new address, which would require extra messaging.

IP version 4 (IPv4) is the currently widely deployed Internet Protocol version. Its major disadvantage is the small number of unique, public IP addresses. IP version 6 (IPv6) has a much larger address space, which fixes the most important IPv4 problem known today. IPv6 also changes some other things in the Internet Protocol, for example, how fragmentation of packets is done, but these changes are quite small. Most protocols have separate definitions on how they are used within the IPv4 and the IPv6 context.

For instance, there are separate versions of IPSec and Mobile IP for use with IPv4 and IPv6. However, such modifications to protocols are quite small, and do not usually change the essentials of the protocols significantly. The invention can be applied to both IPv4 and IPv6.

In the following, the invention is further described by means of figures and some examples. The intention is not to restrict the invention to the details of the following description or to the details of protocols such as the IPSec and IKE protocols which might be changed in the future.

FIGURES

Figure 1 illustrates an example of a telecommunication network to be used in the invention.

Figure 2 illustrates a second example of a telecommunication network to be used in the invention.

Figure 3 illustrates a third example of a telecommunication network to be used in the invention.

Figure 4 describes the prior art solution to enable mobility for IPSec connections.

Figure 5 describes the method of the invention to enable mobility for IPSec connections.

DETAILED DESCRIPTION

Figure 1 illustrates an example of a telecommunication network to be used in the invention. Thus, in figure 1, computer 1 may be a client computer and computer 2 a

destination computer, to which the secure messages are sent in the invention by means of an IPSec tunnel established between computer 1 and computer 2. Computer 2 might be a security gateway for a third computer 3. Then, the messages sent from computer 2 to computer 3 are sent in plaintext. The security gateway can be a common security gateway for e.g. a company LAN, whereby there are several computers in the LAN protected by computer 2. The other protected computers are not shown in figure 1, but naturally, the invention covers also such networks.

The network of figure 2 otherwise corresponds to that of figure 1, but in figure 2 also computer 1 is a security gateway, e.g. for computer 4. Also here, the security gateway 1 can be a common security gateway for e.g. a company LAN, whereby there are several computers in the LAN protected by computer 1. The other protected computers are not shown in figure 2. But naturally, the invention covers also such networks. The messages between security gateway 1 and the computers it protects are sent in plaintext as the IPSec tunnel only exist between computers 1 and 2.

The network of figure 3 is a network, wherein the IPSec messages are sent between an end-to-end connection between two computers 1, 2 only whereby IPSec transport mode can be used instead of tunnel mode.

Figure 4 describes the prior art solution to enable mobility for IPSec connections. As a diagram, this is the standard IPSec procedure when establishing a tunnel between addresses A and X, and then B and X.

The protocol begins with the IKE main mode requiring 6 messages in total, see steps 1a - 6a in figure 4. The protocol involves strong user authentication, policy negotiation and the use of the Diffie-Hellman algorithm. Any other IKE phase 1 mode might of course be used as an alternative. Another approach to minimise the number of message exchanges would be to avoid IKE phase 1 and perform only the IKE quick mode (3 messages). However, IKE phase 1 is associated with IP addresses (along with other identifying information). A modified implementation might ignore IP addresses when processing IKE messages, and thus be able to maintain IKE phase 1 state between connection points.

The protocol then continues with IKE quick mode requiring 3 messages in total (steps 7a - 9a in figure 4). Quick mode includes IPSec policy negotiation and optionally the use of the Diffie-Hellman algorithm. An alternative IKE phase 2 exchange could of course be used instead of quick mode.

At this point the tunnel has been established between addresses A and X. 9 messages have been used along with the computational expense (each Diffie-Hellman computation may take hundreds of milliseconds, for instance, depending on the host), also the roundtrip times being considerable (9/2 = 4.5 roundtrips, with a roundtrip time of 500 ms this is 2.25 seconds for latency alone).

The movement of the mobile terminal to address B causes full re-negotiation and again IKE main mode requires 6 messages in total (steps 1b -6b in figure 4), strong user authentication, policy negotiation, and optionally the use of the Diffie-Hellman algorithm.

The use of the protocol continues with IKE quick mode requiring 3 messages total (steps 7b - 9b).
The tunnel between addresses B and X is now complete.

Figure 5 describes the method of the invention. To establish the tunnel between address A and host X, IKE main mode is again used requiring 6 messages in total (steps 1a - 6a in figure 5) as in figure 4 including strong user authentication, policy negotiation and the use of the Diffie-Hellman algorithm.

Then IKE quick mode is again used requiring 3 messages in total (steps 7a - 9a in figure 5). The quick mode includes IPSec policy negotiation, and optionally the use of the Diffie-Hellman algorithm.

Again, IKE main mode may be replaced by any other IKE phase 1 mode, and IKE quick mode by any other IKE phase 2 mode.

At this point the tunnel has been established between addresses A and X. 9 messages have been used along with the computational expense.

In the invention, movement to address B requires only a single round trip, when using registration request messages to be sent from the mobile terminal, when it moves from address A to address B. In signal 10a of figure 5, which is sent from the mobile terminal to the other end of the established IPSec tunnel when it has moved to address B, a request for registration (RREQ) of the new address is sent. Preferably, a reply message (RREP) is sent (step 11a) from the host to confirm the address change. Both signals 10a and 11a can be encrypted and/or authenticated. The encryption and/or authentication is preferably performed by using IPSec, in which case it is preferable to use the same IPSec SA for protecting both data and registration traffic.

11a is optional in the invention. The preferable encryption method is IPSec, preferably with the modified reception processing described previously. However, the exact method of signalling is not important, the essence is to carry over the IPSec SA to the new connection point.

The SA that existed between addresses A and X has now been changed to be between addresses B and X and is now complete. The next time the mobile terminal sends a message, host 2 in figure 1 - 3 is able to properly handle IPSec packets that come from address B and vice versa. Traffic can now flow inside the tunnel as normal with IPSec.

Any further movement from network to another can be accomplished with a similar exchange of signalling message(s). The IPSec SA does not need to be re-established until the lifetime of the SA has been exhausted.

The invention requires half a roundtrip if only a request message is used without a reply, and one roundtrip of the reply message is used.

The example describes the tunnel mode of IPSec, but transport mode can also be used. IPSec transport mode connections in examples can be replaced with IPSec tunnel mode connections and vice versa. IPSec transport mode combined with an external tunnelling protocol, such as the Layer 2 Tunnelling Protocol (L2TP), is a replacement for IPSec tunnel mode with regards to functionality.

The implementation may optimise the start of traffic flows with regard to message 10a (and optionally 11a); e.g. after sending 10a, the client may directly send IPSec-protected traffic. This essentially makes the handover latency zero, although it requires more complicated processing if the message 10a is lost while being delivered. However, the essential part of the invention is that it is possible to make the invention provide essentially zero-latency handover for client-to-server traffic, and half a roundtrip latency for server-to client traffic.

Different network topologies can, of course, be used in the invention. For instance in figure 1, the connection between hosts 2 and 3 may use IPSec transport or tunnel mode, instead of being plaintext, etc.

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.

CLAIMS

1. Method for ensuring secure forwarding of a message in a telecommunication network, comprising at least one mobile terminal and another terminal, the method comprising
   a) establishing a secure connection between a first address of the mobile terminal and the other terminal, the secure connection defined by at least the addresses of the two terminals,
   b) the mobile terminal moving from the first address to a second address,
   characterized by
   c) changing the connection to be defined between the second address and the other terminal by means of a request message from the mobile terminal to the other terminal to change the address in the definition of the secure connection to the second address.

2. Method of claim 1, characterized in that, the secure connection is established in step a) by forming a Security Association (SA) using the IPSec protocols.

3. Method of claim 1 or 2, characterized in that in step c) a reply back to the mobile terminal is sent from the other terminal after the request from the mobile terminal to change the address.

4. Method of any of claims 1 - 3, characterized in that the registration request and/or the reply message is encrypted and/or authenticated by using the same SA already established.

5. Method of any of claims 1 - 4, characterized in that the change of addresses in the secure connection as a result of the request message is performed by means of a central register of current address of the terminals belonging to the network.

6. Telecommunication network to perform the method of any of claims 1 - 5, comprising at least one mobile terminal and another terminal and a secure connection defined between a first address of the mobile terminal and the other terminal, c h a r a c t e r i z e d by means for changing the connection to be defined between a second address of the mobile terminal and the other terminal.

7. Network of claim 6, c h a r a c t e r i z e d in that the mobile terminal and the other terminal forms an end-to-end connection, whereby the secure connection is an IPSec transport connection or IPSec tunnel connection.

8. Network of claim 6, c h a r a c t e r i z e d in that one of or both of the mobile terminal and the other terminal is a security gateway protecting one or more computers, whereby IPSec tunnel mode or IPSec together with a tunnelling protocol is used for the secure connection between the mobile terminal and the other terminal.

9. Network of claim 6, c h a r a c t e r i z e d in that both terminals are mobile terminals.

10. Network of claim 9, c h a r a c t e r i z e d in that it further contains a central register of current locations of the terminals belonging to the network.

490,932

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 April 2003 (10.04.2003)

PCT

(10) International Publication Number
WO 03/030487 A1

(51) International Patent Classification[7]: H04L 29/06, H04Q 7/38

(21) International Application Number: PCT/FI02/00770

(22) International Filing Date:
27 September 2002 (27.09.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20011910 28 September 2001 (28.09.2001) FI

(71) Applicant *(for all designated States except US)*: **INTRASECURE NETWORKS OY** [FI/FI]; P.O. Box 38, FIN-02201 Espoo (FI).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **VAARALA, Sami** [FI/FI]; Neljäs Linja 22 A 24, FIN-00530 Helsinki (FI). **NUOPPONEN, Antti** [FI/FI]; Kaksoiskiventie 7-9 A 1, FIN-02760 Espoo (FI).

(74) Agent: **INNOPAT LTD**; P.O. Box 556, FIN-02151 Espoo (FI).

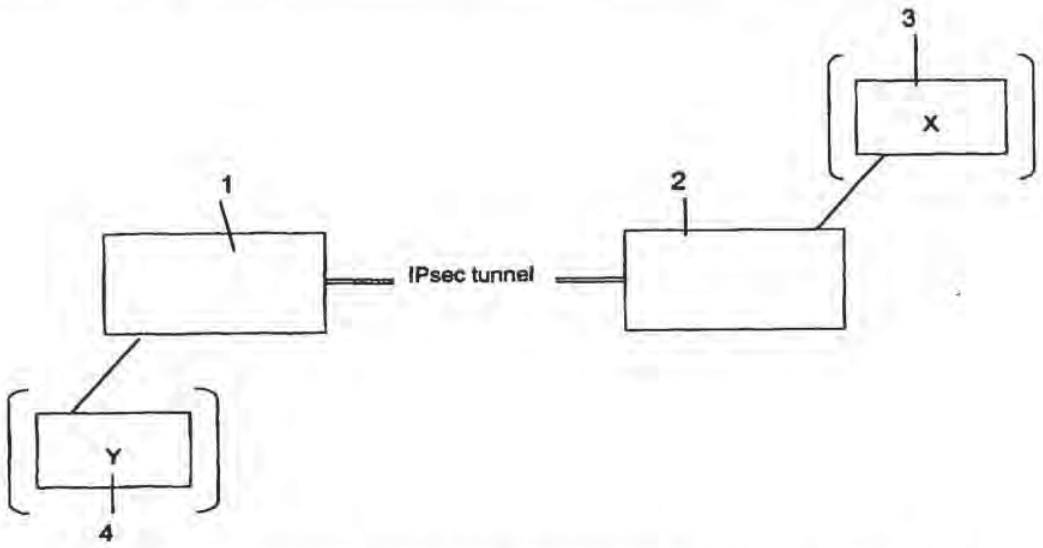
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: METHOD AND NETWORK FOR ENSURING SECURE FORWARDING OF MESSAGES



(57) Abstract: The invention is concerned with a method and a network to ensure secure forwarding of a message in a telecommunication network, comprising at least one first terminal and another terminal. In the method, the first terminal moves from a first address to a second address. A secure connection between the first address of the first terminal and the other terminal defining at least the addresses of the two terminals is established. When the first terminal mo ves from the first address to a second address, the connection is changed to be between the second address and the other terminal by means of a request from the first terminal and preferably, a reply back to the first terminal.

WO 03/030487 A1

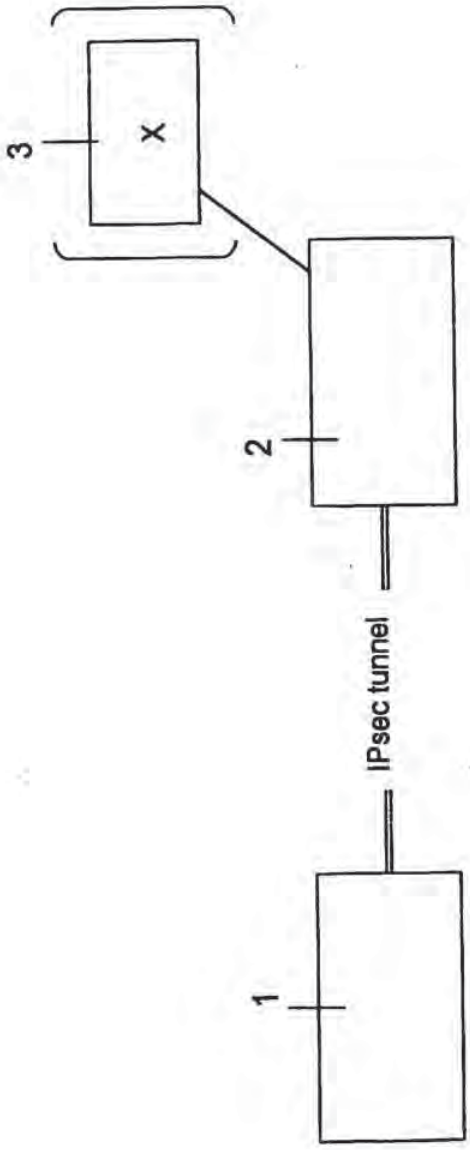


FIG. 1

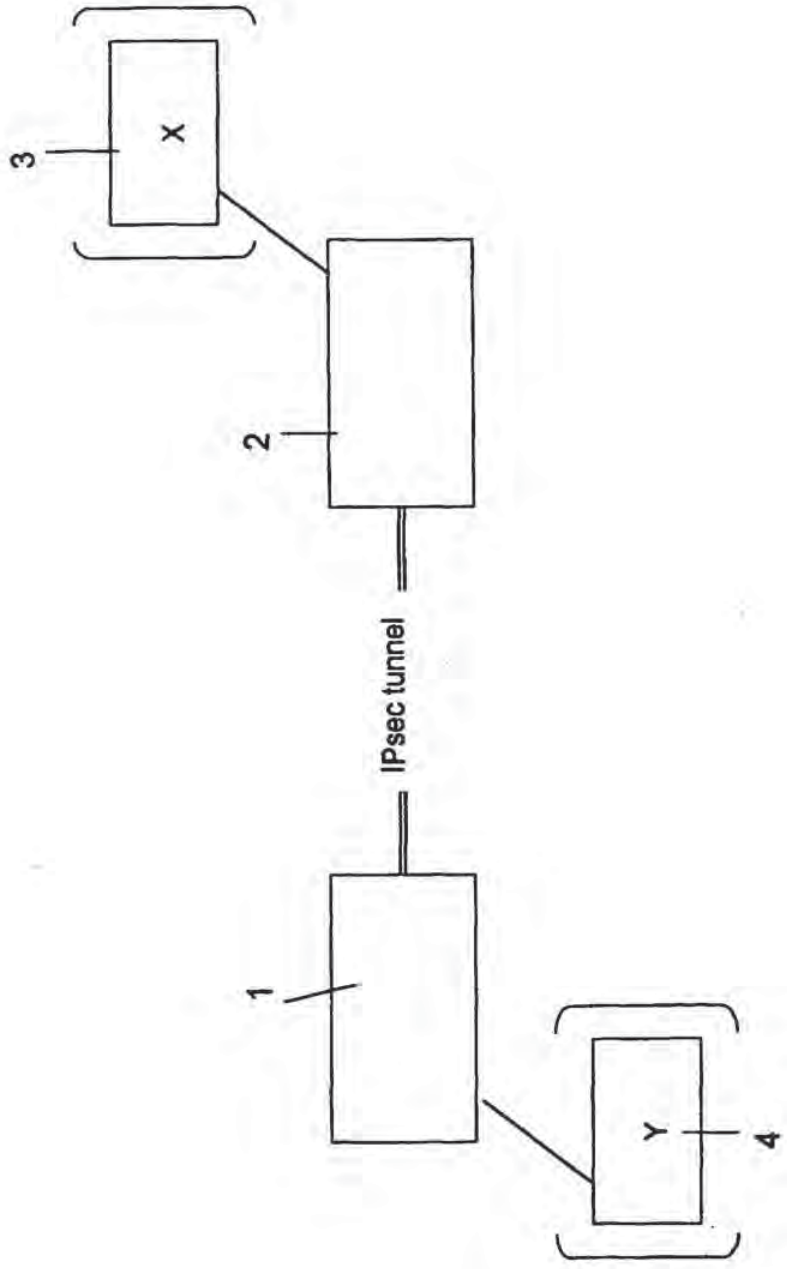
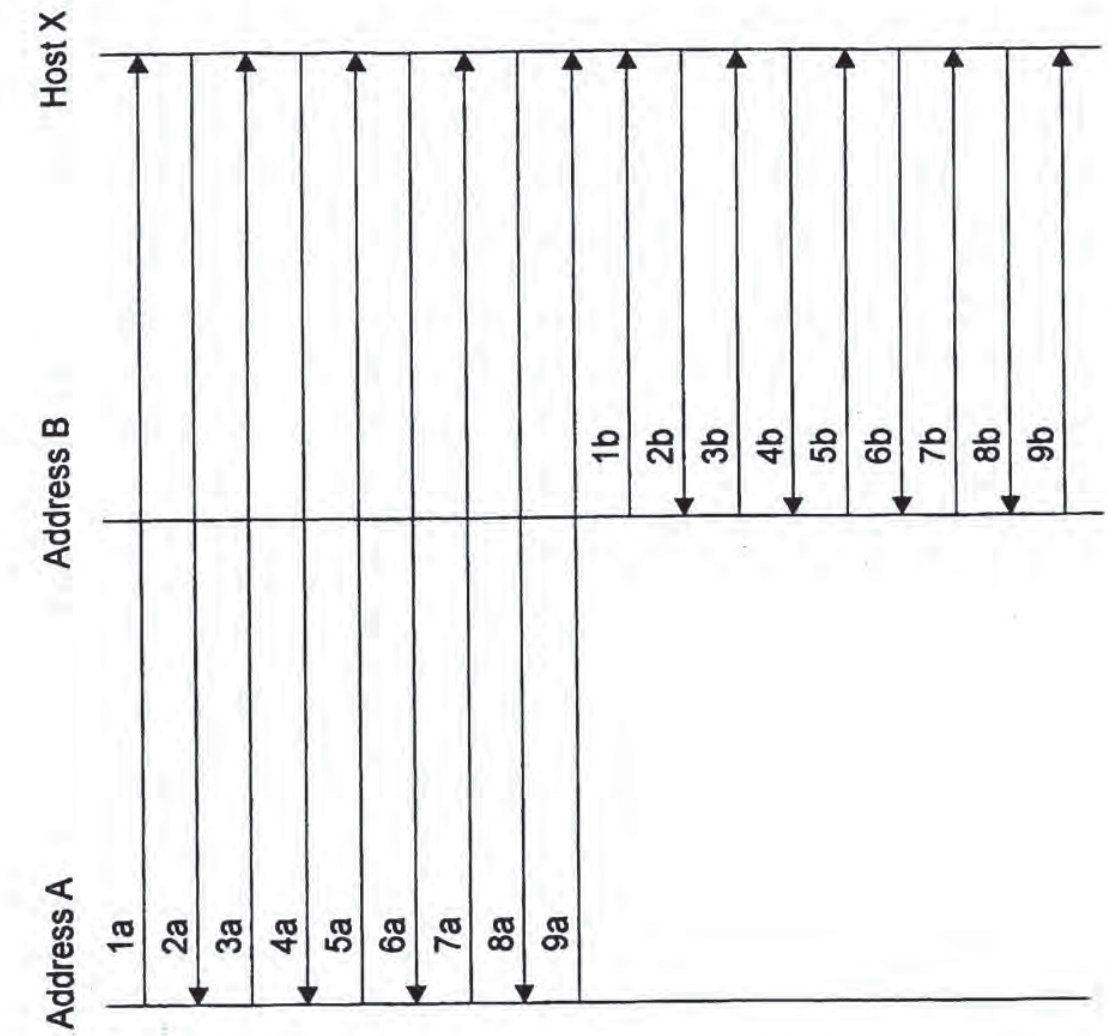


FIG. 2

FIG. 3



PRIOR ART

FIG. 4

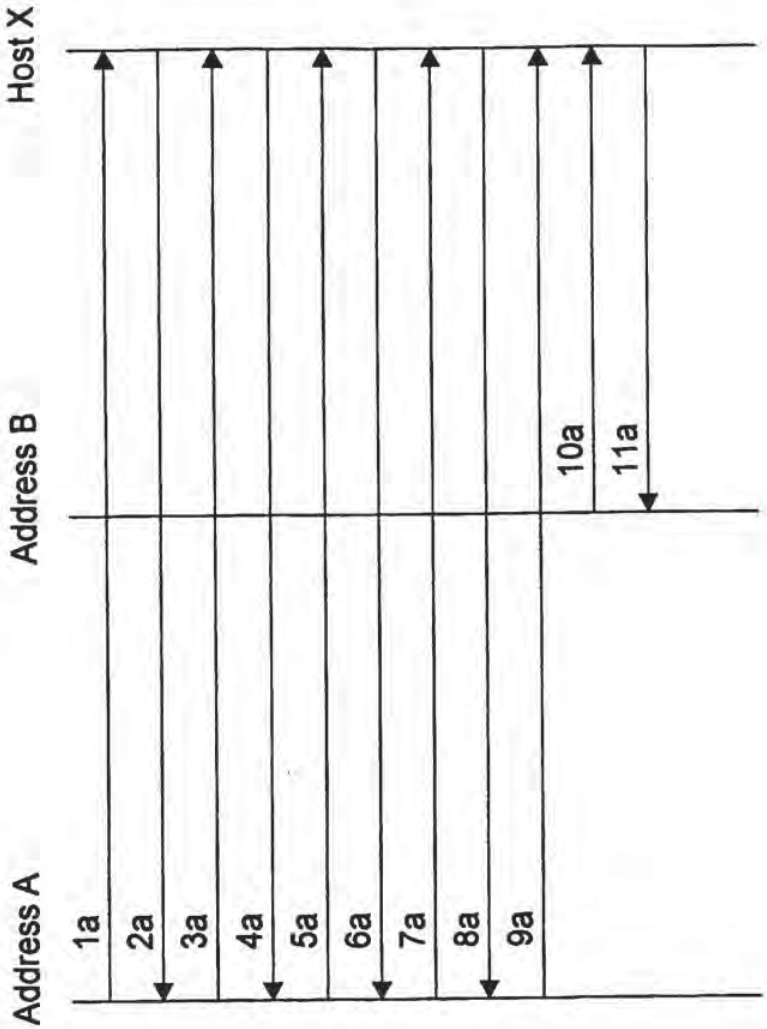


FIG. 5

RF 3/26/04 290.1052USN

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 NETWORK FOR ENSURING SECURE FORWARDING OF MESSAGES, the specification of which was filed as International Patent Application No. PCT/FI02/00770, on 27 September 2002.

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
20011910 (Number)	Finland (Country)	28 Sept. 2001 (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:

(not applicable)	(n/a)	(not applicable)
(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 22 A 24
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 A 1
FIN-02760 Espoo, Finland

PATENT APPLICATION FEE DETERMINATION RECORD
Effective October 1, 2003

Application or Docket Number: 10/490932

CLAIMS AS FILED - PART I

	(Column 1)	(Column 2)
TOTAL CLAIMS		
FOR	NUMBER FILED	NUMBER EXTRA
TOTAL CHARGEABLE CLAIMS	10 minus 20=	* —
INDEPENDENT CLAIMS	1 minus 3 =	* —
MULTIPLE DEPENDENT CLAIM PRESENT		☐

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

SMALL ENTITY TYPE ☐		OR	OTHER THAN SMALL ENTITY	
RATE	FEE		RATE	FEE
BASIC FEE		OR	BASIC FEE	920
XS 9=		OR	XS18=	
X43=		OR	X86=	
+145=		OR	-290=	
TOTAL		OR	TOTAL	920

CLAIMS AS AMENDED - PART II

AMENDMENT A

	(Column 1)		(Column 2)	(Column 3)
	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

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	

AMENDMENT B

	(Column 1)		(Column 2)	(Column 3)
	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
XS 9=		OR	X$18=	
X43=		OR	X86=	
+145=		OR	+290=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT C

	(Column 1)		(Column 2)	(Column 3)
	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X43=		OR	X86=	
+145=		OR	+290=	
TOTAL ADDIT. FEE		OR	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.

PATENT APPLICATION SERIAL NO. _____

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE
FEE RECORD SHEET

04/01/2004 GFREY1 00000077 10490932
01 FC:2611 540.00 OP

PTO-1556
(5/87)

*U.S. Government Printing Office: 2002 — 489-267/69033

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Art Unit

Sami Vaarala, Antti Nuopponen

Serial No.

Filed: Herewith

For: METHOD AND NETWORK FOR ENSURING SECURE FORWARDING OF MESSAGES

Examiner:

Date: 26 March 2004

PRELIMINARY AMENDMENT

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

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

In the specification:

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

--Prior Applications

This is a US national phase patent application that claims priority from PCT/FI02/00770, filed 27 September 2002, that claims priority from Finnish Patent Application No. 20011910, filed 28 September 2001.–

In the Claims:

Amend the claims as follows:

1. (Currently amended) A method ~~Method~~ for ensuring secure forwarding of a message in a telecommunication network, ~~comprising~~ having at least one mobile terminal and another terminal, the method comprising:
a) establishing a secure connection between a first address of the mobile terminal and the other terminal, the secure connection defined by at least the addresses of the two terminals,
b) the mobile terminal moving from the first address to a second address, and ~~characterized by~~
c) changing the connection to be defined between the second address and the other terminal by means of a request message from the mobile terminal to the other terminal to change the address in the definition of the secure connection to the second address.

2. (Currently amended) The method ~~Method~~ of claim 1, characterized in that, the secure connection is established in step a) by forming a Security Association (SA) using ~~the~~ IPSec protocols.

3. (Currently amended) The method ~~Method~~ of claim 1 ~~or 2~~, characterized in that in step c) a reply back to the mobile terminal is sent from the other terminal after the request from the mobile terminal to change the address.

4. (Currently amended) The method ~~Method~~ of claim 1 ~~any of claims 1-3~~, characterized in that the registration request and/or the reply message is encrypted and/or authenticated by using the same SA already established.

5. (Currently amended) The method ~~Method~~ of claim 1 ~~any of claims 1-4~~, characterized in that the change of addresses in the secure connection as a result of the request message is performed by means of a central register of current address of the terminals belonging to the network.

6. (Currently amended) ~~Telecommunication network to perform the method of~~ The method of claim 1 wherein the method further comprises providing a telecommunication network that has ~~any of claims 1-5, comprising~~ at least one mobile terminal and another terminal and a secure connection defined between a first address of the mobile terminal and the other terminal, characterized by means for changing the connection to be defined between a second address of the mobile terminal and the other terminal.

7. (Currently amended) ~~Network~~ The method of claim 6, characterized in that the mobile terminal and the other terminal forms an end-to-end connection whereby the secure connection is an IPSec transport connection or IPSec tunnel connection.

8. (Currently amended) ~~Network~~ The method of claim 6, characterized in that one of or both of the mobile terminal and the other terminal is a security gateway protecting one or more computers, whereby IPSec tunnel mode or IPSec together with a tunneling protocol is used for the secure connection between the mobile terminal and the other terminal.

9. (Currently amended) ~~Network~~ The method of claim 6, characterized in that both terminals are mobile terminals.

10. (Currently amended) ~~Network~~ The method of claim 9,

~~characterized in that it further contains~~ wherein the method further comprises providing a central register of current locations of the terminals belonging to the network.

In the Abstract:

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

--Abstract

The method and network ensure secure forwarding of a message in a telecommunication network that has at least one first terminal and another terminal. The first terminal moves from a first address to a second address. A secure connection between the first address of the first terminal and the other terminal defining at least the addresses of the two terminals is established. When the first terminal moves from the first address to a second address, the connection is changed to be between the second address and to the other terminal by means of a request from the first terminal and preferably a reply back to the first terminal.--

REMARKS

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

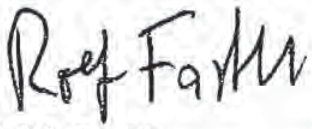
The claims have been amended to better conform to US patent practice. The claims contain no new matter.

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

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

Respectfully submitted,

FASTH LAW OFFICES



Rolf Fasth
Registration No. 36,999

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

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

cc: Paivi Soderman
(Your ref: S00051US)

PATENTTI- JA REKISTERIHALLITUS
NATIONAL BOARD OF PATENTS AND REGISTRATION

Helsinki 12.11.2002

ETUOIKEUSTODISTUS
PRIORITY DOCUMENT

Hakija Applicant	IntraSecure Networks Oy Espoo
Patenttihakemus nro Patent application no	20011910
Tekemispäivä Filing date	28.09.2001
Kansainvälinen luokka International class	H04Q

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

Keksinnön nimitys
Title of invention

"Method and network for ensuring secure forwarding of messages"
(Menetelmä ja verkko viestien turvallisen lähettämisen varmistamiseksi)

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

METHOD AND NETWORK FOR ENSURING SECURE FORWARDING OF MESSAGES

TECHNICAL FIELD

The method and network of the invention is intended to secure mobile connections in telecommunication networks. Especially, it is meant for IPSec connections.

TECHNICAL BACKGROUND

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

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

There is a need to protect data and resources from disclosure, to guarantee the authenticity of data, and to protect systems from network based attacks. More in detail, there is a need for confidentiality (protecting the contents of data from being read), integrity (protecting the data from being modified, which is a property that is independent of confidentiality), authentication (obtaining assurance about 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.)

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

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

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

Security association (SA) is a key concept in the authentication and the confidentiality mechanisms for IP. A security association is a one-way relationship between a sender and a receiver that offers security services to the traffic carried on it. If a secure two-

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

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

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

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

initialisation vectors, and related parameters being used with IPSec. The sixth parameter, Lifetime of this Security Association, is a time-interval and/or byte-count after which a 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. Path MTU, which is an optional feature, defines the maximum size of a packet that can be transmitted without fragmentation.

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 that IPSec tunnelling).

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

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

"IP | IP | payload". The next step is to secure the packet using ESP and/or AH. In case of ESP, the resulting packet is "IP | ESP | IP | payload". The whole inner packet is covered by the ESP and/or AH protection. AH also protects parts of the outer header, in addition to the whole inner packet.

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

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

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

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

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

The problem with standard IPSec tunnel end points are that they are fixed. A SA is bound to a certain IP address, and if it is changed, the existing IPSec SA becomes useless because it has been established by using different endpoint addresses. The problem has been discussed in the IETF standardisation forum, www.IETF.org, wherein an idea to support mobility for IPSec ESP tunnels by means of signalling to update the address of one end after a movement was mentioned by Francis Dupont. No solutions have however been presented until this date.

The standard Mobile IP protocol provides a mobile terminal with a mobile connection, and defines mechanisms for performing efficient handovers from one network to another. However, Mobile IP has several disadvantages. The security of Mobile IP is very limited. The mobility signalling messages are authenticated, but not encrypted, and user data traffic is completely unprotected. Also, there is no key exchange mechanism for establishing the cryptographic keys required for authenticating the mobility signalling. Such keys need to be typically distributed manually. Finally, the

current Mobile IP protocol does not define a method for working through Network Address Translation (NAT) devices.

A way to solve this problem is to use e.g. Mobile IP to handle the mobility of the host, and use IPSec on top of the static IP address provided by the Mobile IP. Thus, the IPSec SAs are bound to static addresses, and the IPSec SAs can survive mobility of the host. However, this approach suffers from packet size overhead of both Mobile IP and IPSec tunnels, which can affect performance considerably when using links with small throughput.

The documents that define IP in general are the RFC standards RFC 768, RFC 791, RFC 793, RFC 826 and RFC 2460. RFC 2002, RFC 2003, RFC 2131, RFC 3115, MOBILE Ipv4 and IPv6, and DHCPV6 define Mobile IP, IP-IP and DHCP.

REFERENCES

The following is a list of useful references of standards mentioned.

IP in general, TCP and UDP:

[RFC768]

J. Postel, *User Datagram Protocol*, RFC 768, August 1980.
ftp://ftp.isi.edu/in-notes/rfc768.txt

[RFC791]

J. Postel, *Internet Protocol*, RFC 791, September 1981.
ftp://ftp.isi.edu/in-notes/rfc791.txt

[RFC792]

J. Postel, *Internet Control Message Protocol*, RFC 792, September 1981.
ftp://ftp.isi.edu/in-notes/rfc792.txt

[RFC793]

J. Postel, *Transmission Control Protocol*, RFC 793, September 1981.
ftp://ftp.isi.edu/in-notes/rfc793.txt

[RFC826]

D.C. Plummer, *An Ethernet Address Resolution Protocol*, RFC 826, November 1982.
ftp://ftp.isi.edu/in-notes/rfc826.txt

[RFC2460]

S. Deering, R. Hinden, *Internet Protocol, Version 6 (IPv6) Specification*, RFC 2460, December 1998.

Mobile IP; IP-IP; DHCP:

[RFC2002]

C. Perkins, *IP Mobility Support*, RFC 2002, October 1996.
ftp://ftp.isi.edu/in-notes/rfc2002.txt

[RFC2003]

C. Perkins, *IP Encapsulation Within IP*, RFC 2003, October 1996.
ftp://ftp.isi.edu/in-notes/rfc2003.txt

[RFC2131]

R. Droms, *Dynamic Host Configuration Protocol*, RFC 2131, March 1997.
ftp://ftp.isi.edu/in-notes/rfc2131.txt

[RFC3115]

G. Dommety, and K. Leung, *Mobile IP Vendor/Organization-specific Extensions*, RFC 3115, April 2001.
ftp://ftp.isi.edu/in-notes/rfc3115.txt

[MOBILEIPv6]

D. B. Johnson, C. Perkins, *Mobility Support in IPv6*, Work in progress (Internet-Draft is available), July 2000.

[DHCPV6]

J. Bound, M. Carney, C. Perking, R.Droms, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*, Work in progress (Internet-Draft is available), June 2001.

IPsec standards:

[RFC2401]

S. Kent, and R. Atkinson, *Security Architecture for the Internet Protocol*, RFC 2401, November 1998.

ftp://ftp.isi.edu/in-notes/rfc2401.txt

[RFC2402]

S. Kent, and R. Atkinson, *IP Authentication Header*, RFC 2402, November 1998.

ftp://ftp.isi.edu/in-notes/rfc2402.txt

[RFC2403]

C. Madson, R. Glenn, The Use of HMAC-MD5-96 within ESP and AH, RFC 2403, November 1998.

[RFC2404]

C. Madson, R. Glenn, The Use of HMAC-SHA-1-96 within ESP and AH, RFC 2404, November 1998.

[RFC2405]

C. Madson, N. Doraswamy, The ESP DES-CBC Cipher Algorithm With Explicit IV, RFC 2405, November 1998.

[RFC2406]

S. Kent, and R. Atkinson, *IP Encapsulating Security Payload (ESP)*, RFC 2406, November 1998.

ftp://ftp.isi.edu/in-notes/rfc2406.txt

[RFC2407]

D. Piper, *The internet IP Security Domain of Interpretation for ISAKMP*, RFC 2407, November 1998.

ftp://ftp.isi.edu/in-notes/rfc2407.txt

[RFC2408]

D. Maughan, M. Schneider, M. Schertler, and J. Turner, *Internet Security Association and Key Management Protocol (ISAKMP)*, RFC 2408, November 1998.

ftp://ftp.isi.edu/in-notes/rfc2408.txt

[RFC2409]

D. Harkins, and D. Carrel, *The Internet Key Exchange (IKE)*, RFC 2409, November 1998.

ftp://ftp.isi.edu/in-notes/rfc2409.txt

[RFC2410]

R. Glenn, S. Kent, *The NULL Encryption Algorithm and Its Use With IPsec*, RFC 2410, November 1998.

[RFC2411]

R. Thayer, N. Doraswamy, R. Glenn, *IP Security Document Roadmap*, RFC 2411, November 1998.

[RFC2412]

H. Orman, *The OAKLEY Key Determination Protocol*, RFC 2412, November 1998.

NAT:

[RFC2694]

P. Srisuresh, G. Tsirtsis, P. Akkiraju, and A. Heffernan, *DNS extensions to Network Address Translators (DNS_ALG)*, RFC 2694, September 1999.

[RFC3022]

P. Shisuresh, K. Egevang, *Traditional IP Network Address Translator (Traditional NAT)*, RFC 3022, January 2001.
ftp://ftp.isi.edu/in-notes/rfc3022.txt

THE OBJECT OF THE INVENTION

The object of the invention is to ensure secure forwarding of messages from and to mobile terminals by avoiding the problems of prior art.

SUMMARY OF THE INVENTION

The method and network of the invention is to ensure secure forwarding of a message in a telecommunication network, comprising at least one first terminal and another terminal. In the method, the first terminal moves from a first address to a second address. A secure connection between the first address of the first terminal and the other terminal defining at least the addresses of the two terminals is established. The first terminal moves from the first address to a second address. The connection is changed to be between the second address and the other terminal by means of a request from the first terminal and preferably, a reply back to the first terminal.

In the invention, the first terminal is movable from one network to another. Such a terminal can physically be a mobile terminal or a fixed terminal.

The secure connection is an IPSec connection established by forming one or more Security Associations (SAs) using the IPSec protocols. The request and/or the reply message can be protected e.g. by IPSec encryption and/or authentication, possibly using the same IPSec SA that is used for traffic protection purposes.

In general, registration request and registration reply are Mobile IP terms while the invention is not bound to Mobile IP. In the invention, the terms request and reply are used in the generic sense, and may or may not be related to Mobile IP.

The method of the invention can be used in different kinds of networks. If the first terminal and the other terminal form an end-to-end connection, the secure connection may be an IPSec tunnel mode or transport mode connection. Furthermore, one of or both of the first terminal and the other terminal can be a security gateway protecting one or more computers, whereby IPSec tunnel mode, or IPSec transport mode together with a tunnelling protocol (such as Layer 2 Tunnelling Protocol, L2TP), is used for the secure connection between the first terminal and the other terminal.

If both terminals are mobile, a special solution is required for the situation when both terminals move simultaneously in case of a so called "double jump" situation. This solution can be implemented e.g. by using a centralised registry of current locations of hosts, although other solutions exist for the problem. However, the "changeable" IPSec tunnel or transport mode SAs of the invention could be used in that case, too.

The applicant has solved the above problems of prior art by defining a signalling mechanism that allows an existing IPSec security association, that is, the symmetric encryption and authentication algorithms used for packet processing, along with their keys and other parameters, to be moved from one network to another. To be more precise, an existing IPSec tunnel endpoint can be moved in the invention from one point of attachment to another. For instance, an IPSec tunnel established between addresses A and X tunnel can be changed by using the defined signalling to be between addresses B and X, using only a single round trip for signalling (2 messages), or half a round trip (1 message, if a reply message is not used) for signalling. The

solution requires minimal computational overhead compared to Diffie-Hellman or strong authentication calculations.

The signalling mechanism is preferably similar to the one in Mobile IP, i.e. a registration request (RREQ) is sent to the other end of the SA followed by a registration reply (RREP) back to the sender of the RREQ message, both of which are extensible for future features and optional attributes. The RREQ/RREP message pair is sent from the new network, and once properly authenticated, the sender IPSec tunnel endpoint is updated from the old network to the new network.

In case the security association used for protecting user traffic is also used for signalling purposes, the reception of the RREQ message by the other end of the SA requires a change in a normal IPSec implementation to accept a packet that appears to belong to a certain IPSec tunnel, but comes from a wrong address (i.e. the tunnel is currently between A and X, and the RREQ comes from address B). This is only necessary for the RREQ message. Such an implementation is provided by the invention; it is necessary to modify IPSec if IPSec is used for the RREQ/RREP signalling. In that case, it is required specifically for processing of the RREQ and RREP messages, if the reply message is to be used.

The request message may update a set of security associations, for instance, a single security association, a security association bundle, an IPSec connection, a group of IPSec connections, or any combinations of these. In practice, it is useful to update either a single IPSec connection or a group of IPSec connections. The latter may be important if separate IPSec connections are used for different kinds of traffic. A single request message can then update all (or a certain set) of such connections to a new address, instead of requiring separate requests for each IPSec connection. In the following, the case of updating a single IPSec connection is discussed, without limiting the invention to this behaviour.

Another method of performing the signalling is to use a separate protocol. The protocol should preferably provide encryption and/or authentication of the signalling messages.

The IKE protocol already has messages defined for e.g. deleting IPSec SAs. One method of providing the necessary signalling would be by adding a new IKE notification message type that requests a change in an existing IPSec SA. Such a message should provide its own encryption and/or authentication to avoid requiring an IKE connection set up from the new address, which would require extra messaging.

IP version 4 (IPv4) is the currently widely deployed Internet Protocol version. Its major disadvantage is the small number of unique, public IP addresses. IP version 6 (IPv6) has a much larger address space, which fixes the most important IPv4 problem known today. IPv6 also changes some other things in the Internet Protocol, for example, how fragmentation of packets is done, but these changes are quite small. Most protocols have separate definitions on how they are used within the IPv4 and the IPv6 context. For instance, there are separate versions of IPSec and Mobile IP for use with IPv4 and IPv6. However, such modifications to protocols are quite small, and do not usually change the essentials of the protocols significantly. The invention can be applied to both IPv4 and IPv6.

In the following, the invention is further described by means of figures and some examples. The intention is not to restrict the invention to the details of the following description or to the details of protocols such as the IPSec and IKE protocols which might be changed in the future.

FIGURES

Figure 1 illustrates an example of a telecommunication network to be used in the invention.

Figure 2 illustrates a second example of a telecommunication network to be used in the invention.

Figure 3 illustrates a third example of a telecommunication network to be used in the invention.

Figure 4 describes the prior art solution to enable mobility for IPSec connections.

Figure 5 describes the method of the invention to enable mobility for IPSec connections.

DETAILED DESCRIPTION

Figure 1 illustrates an example of a telecommunication network to be used in the invention. Thus, in figure 1, computer 1 may be a client computer and computer 2 a destination computer, to which the secure messages are sent in the invention by means of an IPSec tunnel established between computer 1 and computer 2. Computer 2 might be a security gateway for a third computer 3. Then, the messages sent from computer 2 to computer 3 are sent in plaintext. The security gateway can be a common security gateway for e.g. a company LAN, whereby there are several computers in the LAN protected by computer 2. The other protected computers are not shown in figure 1, but naturally, the invention covers also such networks.

The network of figure 2 otherwise corresponds to that of figure 1, but in figure 2 also computer 1 is a security gateway, e.g. for computer 4. Also here, the security gateway 1 can be a common security gateway for e.g. a company LAN, whereby there are several computers in the LAN protected by computer 1. The other protected computers are not shown in figure 2. But naturally, the invention covers also such networks. The messages between security gateway 1 and the computers it protects are sent in plaintext as the IPSec tunnel only exist between computers 1 and 2.

The network of figure 3 is a network, wherein the IPSec messages are sent between an end-to-end connection between two computers 1, 2 only whereby IPSec transport mode can be used instead of tunnel mode.

Figure 4 describes the prior art solution to enable mobility for IPSec connections. As a diagram, this is the standard IPSec procedure when establishing a tunnel between addresses A and X, and then B and X.

The protocol begins with the IKE main mode requiring 6 messages in total, see steps 1a - 6a in figure 4. The protocol involves strong user authentication, policy negotiation and the use of the Diffie-Hellman algorithm. Any other IKE phase 1 mode might of course be used as an alternative. Another approach to minimise the number of message exchanges would be to avoid IKE phase 1 and perform only the IKE quick mode (3 messages). However, IKE phase 1 is associated with IP addresses (along with other identifying information). A modified implementation might ignore IP addresses when processing IKE messages, and thus be able to maintain IKE phase 1 state between connection points.

The protocol then continues with IKE quick mode requiring 3 messages in total (steps 7a - 9a in figure 4). Quick mode includes IPSec policy negotiation and optionally the use of the Diffie-Hellman algorithm. An alternative IKE phase 2 exchange could of course be used instead of quick mode.

At this point the tunnel has been established between addresses A and X. 9 messages have been used along with the computational expense (each Diffie-Hellman computation may take hundreds of milliseconds, for instance, depending on the host), also the roundtrip times being considerable (9/2 = 4.5 roundtrips, with a roundtrip time of 500 ms this is 2.25 seconds for latency alone).

The movement of the mobile terminal to address B causes full re-negotiation and again IKE main mode requires 6 messages in total (steps 1b -6b in figure 4), strong user authentication, policy negotiation, and optionally the use of the Diffie-Hellman algorithm.

The use of the protocol continues with IKE quick mode requiring 3 messages total (steps 7b - 9b).

The tunnel between addresses B and X is now complete.

Figure 5 describes the method of the invention. To establish the tunnel between address A and host X, IKE main mode is again used requiring 6 messages in total (steps 1a - 6a in figure 5) as in figure 4 including strong user authentication, policy negotiation and the use of the Diffie-Hellman algorithm.

Then IKE quick mode is again used requiring 3 messages in total (steps 7a - 9a in figure 5). The quick mode includes IPSec policy negotiation, and optionally the use of the Diffie-Hellman algorithm.

Again, IKE main mode may be replaced by any other IKE phase 1 mode, and IKE quick mode by any other IKE phase 2 mode.

At this point the tunnel has been established between addresses A and X. 9 messages have been used along with the computational expense.

In the invention, movement to address B requires only a single round trip, when using registration request messages to be sent from the mobile terminal, when it moves from address A to address B. In signal 10a of figure 5, which is sent from the mobile terminal to the other end of the established IPSec tunnel when it has moved to address B, a request for registration (RREQ) of the new address is sent. Preferably, a reply message (RREP) is sent (step 11a) from the host to confirm the address change. Both signals 10a and 11a can be encrypted and/or authenticated. The encryption and/or authentication is preferably performed by using IPSec, in which case it is preferable to use the same IPSec SA for protecting both data and registration traffic.

11a is optional in the invention. The preferable encryption method is IPSec, preferably with the modified reception processing described previously. However, the exact method of signalling is not important, the essence is to carry over the IPSec SA to the new connection point.

The SA that existed between addresses A and X has now been changed to be between addresses B and X and is now complete. The next time the mobile terminal sends a message, host 2 in figure 1 - 3 is able to properly handle IPSec packets that come from address B and vice versa. Traffic can now flow inside the tunnel as normal with IPSec.

Any further movement from network to another can be accomplished with a similar exchange of signalling message(s). The IPSec SA does not need to be re-established until the lifetime of the SA has been exhausted.

The invention requires half a roundtrip if only a request message is used without a reply, and one roundtrip of the reply message is used.

The example describes the tunnel mode of IPSec, but transport mode can also be used. IPSec transport mode connections in examples can be replaced with IPSec tunnel mode connections and vice versa. IPSec transport mode combined with an external tunnelling protocol, such as the Layer 2 Tunnelling Protocol (L2TP), is a replacement for IPSec tunnel mode with regards to functionality.

The implementation may optimise the start of traffic flows with regard to message 10a (and optionally 11a); e.g. after sending 10a, the client may directly send IPSec-protected traffic. This essentially makes the handover latency zero, although it requires more complicated processing if the message 10a is lost while being delivered. However, the essential part of the invention is that it is possible to make the invention provide essentially zero-latency handover for client-to-server traffic, and half a roundtrip latency for server-to client traffic.

Different network topologies can, of course, be used in the invention. For instance in figure 1, the connection between hosts 2 and 3 may use IPSec transport or tunnel mode, instead of being plaintext, etc.

CLAIMS

1. Method for ensuring secure forwarding of a message in a telecommunication network, comprising at least one mobile terminal and another terminal, in which method the mobile terminal moves from a first address to a second address, characterized by
   a) establishing a secure connection between the first address of the mobile terminal and the other terminal defining at least the addresses of the two terminals,
   b) the mobile terminal moving from the first address to a second address.
   c) changing the connection to be between the second address and the other terminal by means of a request message from the mobile terminal to the other terminal to change the address of the secure connection to the second address.

2. Method of claim 1, characterized in that, the secure connection is established in step a) by forming a Security Association (SA) using the IPSec protocols.

3. Method of claim 1 or 2, characterized in that in step c) a reply back to the mobile terminal is sent from the other terminal after the request from the mobile terminal to change the address.

4. Method of any of claims 1 - 3, characterized in that the registration request and/or the reply message is encrypted and/or authenticated by using the same SA already established.

5. Method of any of claims 1 - 4, characterized in that the change of addresses in the secure connection as a result of the request message is performed by means of a central register of current address of the terminals belonging to the network.

6. Telecommunication network to perform the method of any of claims 1 - 5, comprising at least one mobile terminal and another terminal.

7. Network of claim 6, c h a r a c t e r i z e d in that the mobile terminal and the other terminal forms an end-to-end connection, whereby the secure connection is an IPSec transport connection or IPSec tunnel connection.

8. Network of claim 6, c h a r a c t e r i z e d in that one of or both of the mobile terminal and the other terminal is a security gateway protecting one or more computers, whereby IPSec tunnel mode or IPSec together with a tunnelling protocol is used for the secure connection between the mobile terminal and the other terminal.

9. Network of claim 6, c h a r a c t e r i z e d in that both terminals are mobile terminals.

10. Network of claim 9, c h a r a c t e r i z e d in that it further contains a central register of current locations of the terminals belonging to the network.

ABSTRACT

The invention is concerned with a method and a network to ensure secure forwarding of a message in a telecommunication network, comprising at least one first terminal and another terminal. In the method, the first terminal moves from a first address to a second address. A secure connection between the first address of the first terminal and the other terminal defining at least the addresses of the two terminals is established. When the first terminal moves from the first address to a second address, the connection is changed to be between the second address and the other terminal by means of a request from the first terminal and preferably, a reply back to the first terminal.

FIG. 2

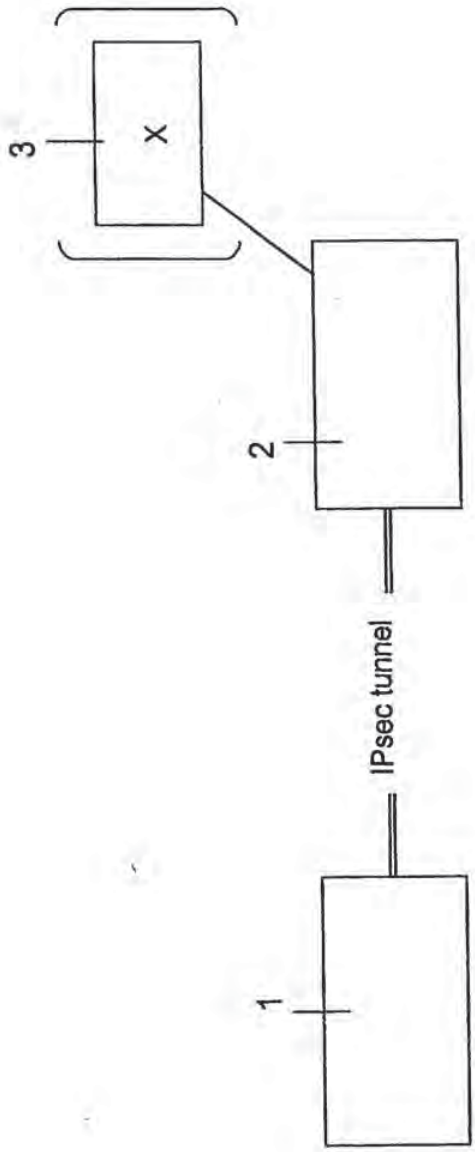


FIG. 1

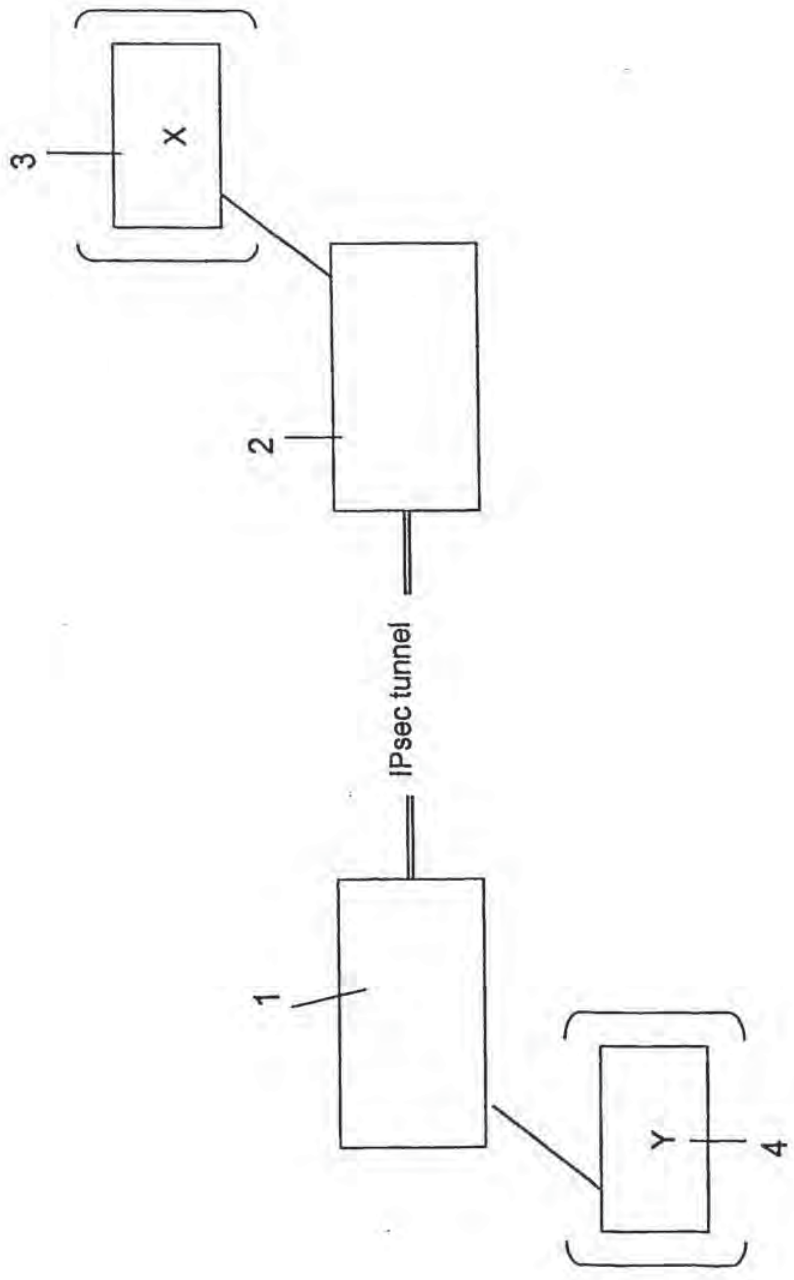


FIG. 2

FIG. 3

PRIOR ART

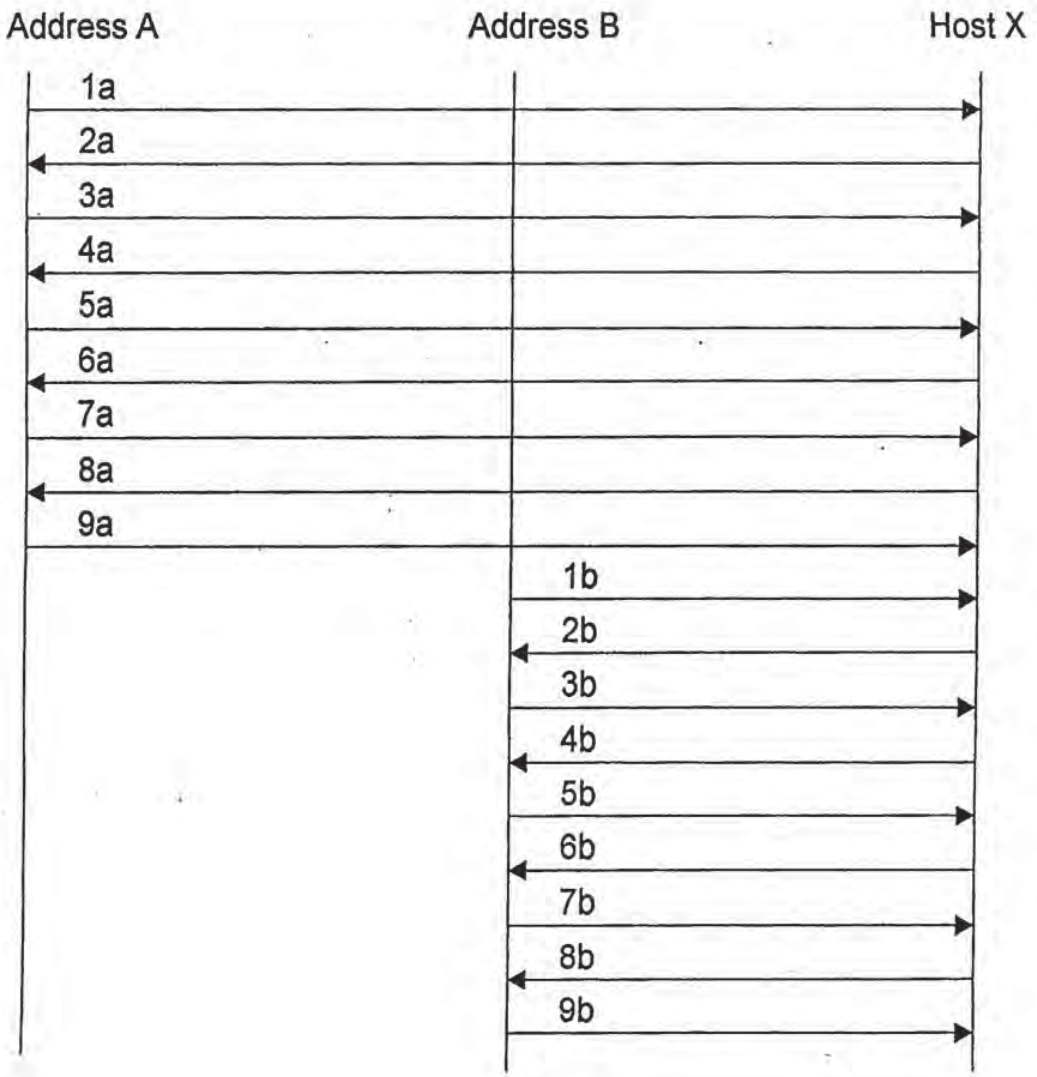


FIG. 4

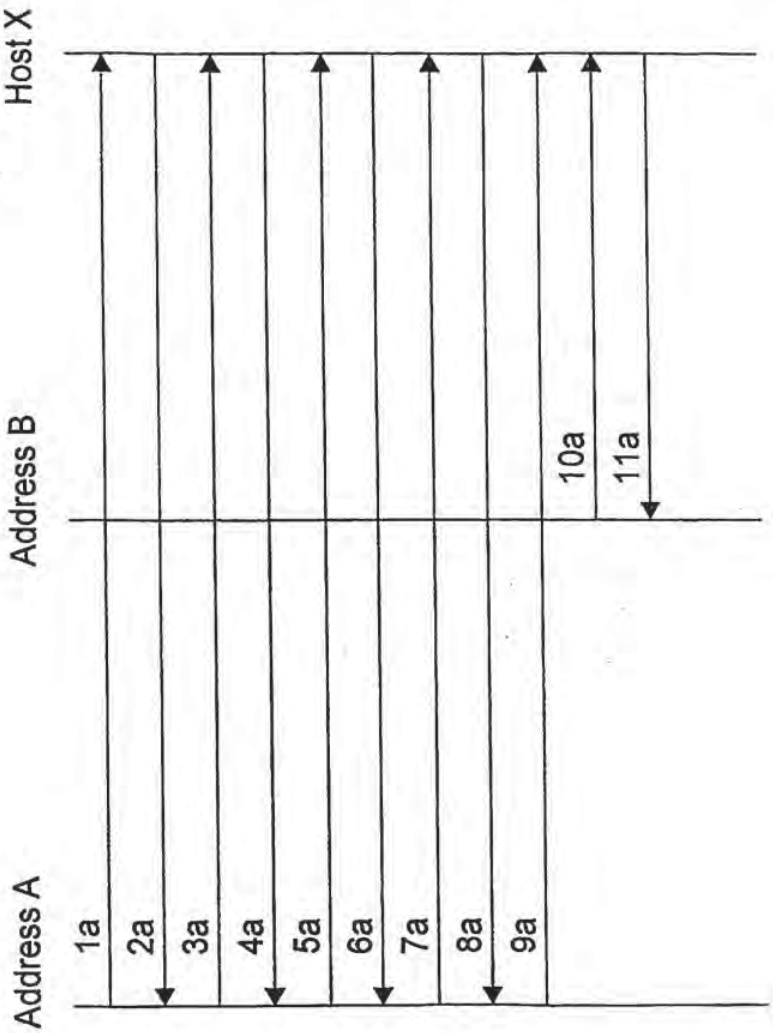


FIG. 5

DO/ EO WORKSHEET

Paralegal/ National Stage Division

U.S. Appl. No. 10/490932 International Appl. No. PI02/00770

Application filed by : ☑ 30 months

WIPO PUBLICATION INFORMATION :

Publication No.: WO /

Publication Language : ☑ English ☐ German ☐ French ☐ Japanese ☐ Russian ☐ Korean ☐ Other : _____

Publication Date : 10 Apr 03

Not Published : ☐ U.S. only designated ☐ EP request Published : ☐ EP

INTERNATIONAL APPLICATION PAPERS IN THE APPLICATION FILE :

- ☑ International Application
- ☐ Article 19 Amendments
- ☐ PCT/IB/331
- ☑ PCT/IPEA/409 IPER (PCT/IPEA/416 on front)
- ☑ Annexes to 409 (Article 34 Amendment)
- ☑ Priority Document (s) No. 1
- ☐ Request form PCT/RO/101
- ☑ PCT/ISA/210 - Search Report
- ☐ Search Report References
- ☐ PCT/IB/306 - Notification of a Change
- ☐ Other : _____

RECEIPTS FROM THE APPLICANT:

- ☑ Basic National Fee (*or authorization to charge*)
- ☑ Description
- ☑ Claims
- ☐ Drawing Figure(s) - (# of dwgs. 1) No Drawings
- ☐ Translation of Article 19 Amendments
  - ☐ entered ☐ not entered :
    - ☐ not a page for page substitution
    - ☐ replaced by Article 34 Amendment
- ☑ Translation of Annexes to 409
  - ☑ entered ☐ not entered :
    - ☐ not a page for page substitution
    - ☐ other : _____
- ☐ Application Data Sheet
- ☐ Power of Attorney ☐ Change of Address
- ☑ Preliminary Amendment(s) Filed on : 1. 26 Mar 04 2. _____ 3. _____
- ☐ Information Disclosure Statement(s) Filed on : 1. _____ 2. _____ 3. _____
- ☐ Assignment Document (forwarded to Assignment Branch)
- ☐ Assignee PG Publication Notice
- ☐ Substitute Specification Filed on : 1. _____ 2. _____
- ☐ Verified Small Status Statement (executed)
- ☐ Oath/ Declaration (executed)
  - ☐ surcharge was paid at the time of filing
- ☐ DNA Diskette ☐ Sequence Listing
- ☐ Other : 1. _____
- ☐ Other : 1. _____

NOTES : ☑ I.A. used as Specification ☐ Other :

35 U.S.C. 371 - Receipt of Request	26 Mar 04
Date Acceptable Oath/ Declaration Received	22 NOV 04
Date of Completion of requirements under 35 U.S.C. 371(c)(1), (c)(2) and (c)(4)	↓
Date of Completion of ALL requirements under 35 U.S.C. 371	↓
Date of Completion of DO/ EO 903 - Notification of Acceptance	13 DEC 04
Date of Completion of DO/ EO 905 - Notification of Missing Requirements	9 Sept 04
Date of Completion of DO/ EO 916 - Notification of Defective Response	
Date of Completion of DO/ EO 909 - Notification of Abandonment	

☐ EP ☐ JP ☐ SE ☐ AU ☐ US ☐ _

INTERNATIONAL SEARCH REPORT

Inter[illegible]plication No
PCT/F[illegible]2/00770

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, INSPEC, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 01 39538 A (NOKIA CORP ;NOKIA INC (US)) 31 May 2001 (2001-05-31) page 8, line 20 -page 10, line 19 page 14, line 19 -page 17, line 9 abstract; figure 2 ---	1-10
X	WO 00 41427 A (ERICSSON TELEFON AB L M) 13 July 2000 (2000-07-13) page 2, line 25 -page 4, line 21 page 6, line 38 -page 8, line 13 ---	1-10
A	WO 01 24560 A (SIMOCO INT LTD ;RAYNE MARK WENTWORTH (GB)) 5 April 2001 (2001-04-05) the whole document ---	1-10
A	US 2001/009025 A1 (AHONEN PASI MATTI KALEVI) 19 July 2001 (2001-07-19) the whole document ---	1-10

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 December 2002	20. 01. 2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	MARIANNE ENGDAHL/JA A

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter[illegible]pplication No
PCT/[illegible]2/00770

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 1 124 397 A (LUCENT TECHNOLOGIES INC) 16 August 2001 (2001-08-16) the whole document -----	1-10

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

[redacted] on patent family members

Inter[redacted]pplication No
PCT/[redacted]2/00770

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 0139538	A	31-05-2001	AU	1293301 A	04-06-2001
			BR	0015774 A	13-08-2002
			EP	1232662 A1	21-08-2002
			WO	0139538 A1	31-05-2001
WO 0041427	A	13-07-2000	US	6418130 B1	09-07-2002
			AU	2335300 A	24-07-2000
			CN	1337134 T	20-02-2002
			EP	1142400 A2	10-10-2001
			JP	2002534930 T	15-10-2002
			WO	0041427 A2	13-07-2000
WO 0124560	A	05-04-2001	AU	7534900 A	30-04-2001
			WO	0124560 A1	05-04-2001
			GB	2359464 A	22-08-2001
US 2001009025	A1	19-07-2001	GB	2364477 A	23-01-2002
			AU	2895801 A	31-07-2001
			WO	0154379 A1	26-07-2001
EP 1124397	A	16-08-2001	AU	1677001 A	16-08-2001
			BR	0100193 A	09-10-2001
			CN	1321049 A	07-11-2001
			EP	1124397 A2	16-08-2001
			JP	2001258059 A	21-09-2001

Form PCT/ISA/210 (patent family annex) (July 1992)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference S0051PCT	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/FI02/00770	International filing date *(day/month/year)* 27.09.2002	Priority date *(day/month/year)* 28.09.2001
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 6 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 21 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	Date of completion of this report
24.04.2003	04.12.2003
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 Bertini, S Telephone No. +49 89 2399-8985

Form PCT/IPEA/409 (Cover Sheet) (January 1994)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/FI02/00770

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

1-19 filed with telefax on 30.10.2003

Claims, Numbers

1-10 filed with telefax on 30.10.2003

Drawings, Sheets

1/5-5/5 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:

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	1-10
	No:	Claims	
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-10
Industrial applicability (IA)	Yes:	Claims	1-10
	No:	Claims	

2. Citations and explanations

   see separate sheet

V. REASONED STATEMENT UNDER RULE 66.2(A)(II) WITH REGARD TO NOVELTY, INVENTIVE STEP AND INDUSTRIAL APPLICABILITY

1. The documents cited in the International Search Report will be hereinafter referred to as D1-D5, taken in the order in which they appear in the Search Report.

2. Due to the broad formulation of its subject-matter, method claims 1 does not comply with the dispositions set out in Articles 33 (1), (3) PCT regarding inventive step.

3. Document D1, in fact, discloses (see passages cited in the Search Report), according to the main features of claim 1, a method for ensuring secure forwarding of a message (existing security association) in a telecommunication network whereby a mobile terminal, which already has a secure connection with another terminal, moving from a first address to a second address sends a request message to the other terminal to change the address of the already established secure connection to the second address (existing security association is re-established when a communication handover event occurs in a radio communications system ... by a challenge/response procedure).

   The wording of claim 1 is much too general, so that the subject-matter of the claim is already known, in all essential aspects, from document D1; therefore, a skilled person in telecommunications networks, being aware of the disclosure of D1 can apply common general knowledge of the art (step -c- of claim 1 which requires to make a request to change the address **when the address has to be changed because the connection is changed**, appears to be a simple and obvious step which the person skilled in the art would do without the exercise of any inventive activity) and arrive at the method of claim 1.

   The mobile terminal in the present application moves from a first address to a second address (claim 1, b)), i.e. "the first terminal is movable from one network to another" (see description page 12, line 18), whereas the mobile terminal in document D1 moves from an access point and another access point. The secure connection is in both cases between two terminals one of them is moving. The wording of the claim is so broad that the secure connection disclosed in D1 is also covered by the method for ensuring secure forwarding of a message

presently on file. Even if there were differences between the disclosure of the present application and that of D1, as argued by the Applicant, these differences are not included in claim 1 as amended.

3. A similar discussion concerning inventive step could also be started from prior art document D2, arriving at the same conclusion. Indeed, this document cited in the International Search Report also appears to be relevant for the subject-matter presently claimed.

4. The independent claim 6 cannot be accepted in the present amended form, because it does not contain **all the essential technical apparatus features** which in combination define the invention, Article 6 PCT.
The reference to the claimed method can only be interpreted as an arrangement suitable for carrying out the claimed method, without this reference itself defining the apparatus features necessary therefor. Claim 6 should therefore explicitly state all essential features of the invention (i.e. apparatus) without relying on a reference only to the method claims.
Such an amended apparatus claim corresponding, in terms of apparatus features, to method claim 1, would however the same problems related to the lack of inventive step already stated with regard to claim 1 presently on file.

5. Dependent claims 2 to 5 and 7 to 10 do not appear to contain any additional features which, in combination with the features of any claim to which they refer, involve an inventive step for the following reasons: the subject-matter of said claims is either directly derivable from prior art documents D1-D5 (and in particular from documents D1 and/or D2) or represent minor design details generally known in the field of secure mobile connections in telecommunications networks.

The subject-matter of dependent claims 2 to 5 and 7 to 10 therefore does not involve an inventive step so that these claims do not comply with the dispositions set out in Articles 33 (1) and (3) PCT.

6. a) The claims should have been properly drafted in the two part form recommended by Rule 6.3 (a) (b) PCT; reference signs in parentheses as

required by Rule 6.2 (b) PCT.

b) The prior art documents D1-D5 should have been correctly acknowledged in the description and the state of the art disclosed therein should have been briefly discussed in the opening part of the description, Rule 5.1 (a) (ii) PCT.

c) The abbreviation"SA" in claim 2 is not a reference sign and should not be included in the claim in parentheses but after a comma ("...Security Association, SA, using ...).

d) The abbreviation "IPSec" used in claims 7 and 8 should also be defined in the claims by "...IP security protocols, IPSec, ...".

WO 03/030487

PCT/FI02/00770

METHOD AND NETWORK FOR ENSURING SECURE FORWARDING OF MESSAGES

TECHNICAL FIELD

The method and network of the invention is intended to secure mobile connections in telecommunication networks. Especially, it is meant for IPSec connections.

TECHNICAL BACKGROUND

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

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

There is a need to protect data and resources from disclosure, to guarantee the authenticity of data, and to protect systems from network based attacks. More in detail, there is a need for confidentiality (protecting the contents of data from being read), integrity (protecting the data from being modified, which is a property that is independent of confidentiality), authentication (obtaining assurance about 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.)

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

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

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

Security association (SA) is a key concept in the authentication and the confidentiality mechanisms for IP. A security association is a one-way relationship between a sender and a receiver that offers security services to the traffic carried on it. If a secure two-

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

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

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

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

initialisation vectors, and related parameters being used with IPSec. The sixth parameter, Lifetime of this Security Association, is a time-interval and/or byte-count after which a 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. Path MTU, which is an optional feature, defines the maximum size of a packet that can be transmitted without fragmentation.

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 that IPSec tunnelling).

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

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

"IP | IP | payload". The next step is to secure the packet using ESP and/or AH. In case of ESP, the resulting packet is "IP | ESP | IP | payload". The whole inner packet is covered by the ESP and/or AH protection. AH also protects parts of the outer header, in addition to the whole inner packet.

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

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

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

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

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

The problem with standard IPSec tunnel end points are that they are fixed. A SA is bound to a certain IP address, and if it is changed, the existing IPSec SA becomes useless because it has been established by using different endpoint addresses. The problem has been discussed in the IETF standardisation forum, www.IETF.org, wherein an idea to support mobility for IPSec ESP tunnels by means of signalling to update the address of one end after a movement was mentioned by Francis Dupont. No solutions have however been presented until this date.

The standard Mobile IP protocol provides a mobile terminal with a mobile connection, and defines mechanisms for performing efficient handovers from one network to another. However, Mobile IP has several disadvantages. The security of Mobile IP is very limited. The mobility signalling messages are authenticated, but not encrypted, and user data traffic is completely unprotected. Also, there is no key exchange mechanism for establishing the cryptographic keys required for authenticating the mobility signalling. Such keys need to be typically distributed manually. Finally, the

current Mobile IP protocol does not define a method for working through Network Address Translation (NAT) devices.

A way to solve this problem is to use e.g. Mobile IP to handle the mobility of the host, and use IPSec on top of the static IP address provided by the Mobile IP. Thus, the IPSec SAs are bound to static addresses, and the IPSec SAs can survive mobility of the host. However, this approach suffers from packet size overhead of both Mobile IP and IPSec tunnels, which can affect performance considerably when using links with small throughput.

The documents that define IP in general are the RFC standards RFC 768, RFC 791, RFC 793, RFC 826 and RFC 2460. RFC 2002, RFC 2003, RFC 2131, RFC 3115, MOBILE Ipv4 and IPv6, and DHCPV6 define Mobile IP, IP-IP and DHCP.

REFERENCES

The following is a list of useful references of standards mentioned.

IP in general, TCP and UDP:

[RFC768]

J. Postel, *User Datagram Protocol*, RFC 768, August 1980.
ftp://ftp.isi.edu/in-notes/rfc768.txt

[RFC791]

J. Postel, *Internet Protocol*, RFC 791, September 1981.
ftp://ftp.isi.edu/in-notes/rfc791.txt

[RFC792]

J. Postel, *Internet Control Message Protocol*, RFC 792, September 1981.
ftp://ftp.isi.edu/in-notes/rfc792.txt

[RFC793]

J. Postel, *Transmission Control Protocol*, RFC 793, September 1981.
ftp://ftp.isi.edu/in-notes/rfc793.txt

[RFC826]

D.C. Plummer, *An Ethernet Address Resolution Protocol*, RFC 826, November 1982.
ftp://ftp.isi.edu/in-notes/rfc826.txt

[RFC2460]

S. Deering, R. Hinden, *Internet Protocol, Version 6 (IPv6) Specification*, RFC 2460, December 1998.

Mobile IP; IP-IP; DHCP:

[RFC2002]

C. Perkins, *IP Mobility Support*, RFC 2002, October 1996.
ftp://ftp.isi.edu/in-notes/rfc2002.txt

[RFC2003]

C. Perkins, *IP Encapsulation Within IP*, RFC 2003, October 1996.
ftp://ftp.isi.edu/in-notes/rfc2003.txt

[RFC2131]

R. Droms, *Dynamic Host Configuration Protocol*, RFC 2131, March 1997.
ftp://ftp.isi.edu/in-notes/rfc2131.txt

[RFC3115]

G. Dommety, and K. Leung, *Mobile IP Vendor/Organization-specific Extensions*, RFC 3115, April 2001.
ftp://ftp.isi.edu/in-notes/rfc3115.txt

[MOBILEIPv6]

D. B. Johnson, C. Perkins, *Mobility Support in IPv6*, Work in progress (Internet-Draft is available), July 2000.

[DHCPV6]

J. Bound, M. Carney, C. Perking, R.Droms, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*, Work in progress (Internet-Draft is available), June 2001.

IPsec standards:

[RFC2401]

S. Kent, and R. Atkinson, *Security Architecture for the Internet Protocol*, RFC 2401, November 1998.

ftp://ftp.isi.edu/in-notes/rfc2401.txt

[RFC2402]

S. Kent, and R. Atkinson, *IP Authentication Header*, RFC 2402, November 1998.

ftp://ftp.isi.edu/in-notes/rfc2402.txt

[RFC2403]

C. Madson, R. Glenn, The Use of HMAC-MD5-96 within ESP and AH, RFC 2403, November 1998.

[RFC2404]

C. Madson, R. Glenn, The Use of HMAC-SHA-1-96 within ESP and AH, RFC 2404, November 1998.

[RFC2405]

C. Madson, N. Doraswamy, The ESP DES-CBC Cipher Algorithm With Explicit IV, RFC 2405, November 1998.

[RFC2406]

S. Kent, and R. Atkinson, *IP Encapsulating Security Payload (ESP)*, RFC 2406, November 1998.

ftp://ftp.isi.edu/in-notes/rfc2406.txt

[RFC2407]

D. Piper, *The internet IP Security Domain of Interpretation for ISAKMP*, RFC 2407, November 1998.

ftp://ftp.isi.edu/in-notes/rfc2407.txt

[RFC2408]

D. Maughan, M. Schneider, M. Schertler, and J. Turner, *Internet Security Association and Key Management Protocol (ISAKMP)*, RFC 2408, November 1998.

ftp://ftp.isi.edu/in-notes/rfc2408.txt

[RFC2409]

D. Harkins, and D. Carrel, *The Internet Key Exchange (IKE)*, RFC 2409, November 1998.

ftp://ftp.isi.edu/in-notes/rfc2409.txt

[RFC2410]

R. Glenn, S. Kent, *The NULL Encryption Algorithm and Its Use With IPsec*, RFC 2410, November 1998.

[RFC2411]

R. Thayer, N. Doraswamy, R. Glenn, *IP Security Document Roadmap*, RFC 2411, November 1998.

[RFC2412]

H. Orman, *The OAKLEY Key Determination Protocol*, RFC 2412, November 1998.

NAT:

[RFC2694]

P. Srisuresh, G. Tsirtsis, P. Akkiraju, and A. Heffernan, *DNS extensions to Network Address Translators (DNS_ALG)*, RFC 2694, September 1999.

[RFC3022]

P. Shisuresh, K. Egevang, *Traditional IP Network Address Translator (Traditional NAT)*, RFC 3022, January 2001.

ftp://ftp.isi.edu/in-notes/rfc3022.txt

THE OBJECT OF THE INVENTION

The object of the invention is to ensure secure forwarding of messages from and to mobile terminals by avoiding the problems of prior art.

SUMMARY OF THE INVENTION

The method and network of the invention is to ensure secure forwarding of a message in a telecommunication network, comprising at least one first terminal and another terminal. In the method, the first terminal moves from a first address to a second address. A secure connection between the first address of the first terminal and the other terminal defining at least the addresses of the two terminals is established. The first terminal moves from the first address to a second address. The connection is changed to be between the second address and the other terminal by means of a request from the first terminal and preferably, a reply back to the first terminal.

In the invention, the first terminal is movable from one network to another. Such a terminal can physically be a mobile terminal or a fixed terminal.

The secure connection is an IPSec connection established by forming one or more Security Associations (SAs) using the IPSec protocols. The request and/or the reply message can be protected e.g. by IPSec encryption and/or authentication, possibly using the same IPSec SA that is used for traffic protection purposes.

In general, registration request and registration reply are Mobile IP terms while the invention is not bound to Mobile IP. In the invention, the terms request and reply are used in the generic sense, and may or may not be related to Mobile IP.

The method of the invention can be used in different kinds of networks. If the first terminal and the other terminal form an end-to-end connection, the secure connection may be an IPSec tunnel mode or transport mode connection. Furthermore, one of or both of the first terminal and the other terminal can be a security gateway protecting one or more computers, whereby IPSec tunnel mode, or IPSec transport mode together with a tunnelling protocol (such as Layer 2 Tunnelling Protocol, L2TP), is used for the secure connection between the first terminal and the other terminal.

If both terminals are mobile, a special solution is required for the situation when both terminals move simultaneously in case of a so called "double jump" situation. This solution can be implemented e.g. by using a centralised registry of current locations of hosts, although other solutions exist for the problem. However, the "changeable" IPSec tunnel or transport mode SAs of the invention could be used in that case, too.

The applicant has solved the above problems of prior art by defining a signalling mechanism that allows an existing IPSec security association, that is, the symmetric encryption and authentication algorithms used for packet processing, along with their keys and other parameters, to be moved from one network to another. To be more precise, an existing IPSec tunnel endpoint can be moved in the invention from one point of attachment to another. For instance, an IPSec tunnel established between addresses A and X tunnel can be changed by using the defined signalling to be between addresses B and X, using only a single round trip for signalling (2 messages), or half a round trip (1 message, if a reply message is not used) for signalling. The

solution requires minimal computational overhead compared to Diffie-Hellman or strong authentication calculations.

The signalling mechanism is preferably similar to the one in Mobile IP, i.e. a registration request (RREQ) is sent to the other end of the SA followed by a registration reply (RREP) back to the sender of the RREQ message, both of which are extensible for future features and optional attributes. The RREQ/RREP message pair is sent from the new network, and once properly authenticated, the sender IPSec tunnel endpoint is updated from the old network to the new network.

In case the security association used for protecting user traffic is also used for signalling purposes, the reception of the RREQ message by the other end of the SA requires a change in a normal IPSec implementation to accept a packet that appears to belong to a certain IPSec tunnel, but comes from a wrong address (i.e. the tunnel is currently between A and X, and the RREQ comes from address B). This is only necessary for the RREQ message. Such an implementation is provided by the invention; it is necessary to modify IPSec if IPSec is used for the RREQ/RREP signalling. In that case, it is required specifically for processing of the RREQ and RREP messages, if the reply message is to be used.

The request message may update a set of security associations, for instance, a single security association, a security association bundle, an IPSec connection, a group of IPSec connections, or any combinations of these. In practice, it is useful to update either a single IPSec connection or a group of IPSec connections. The latter may be important if separate IPSec connections are used for different kinds of traffic. A single request message can then update all (or a certain set) of such connections to a new address, instead of requiring separate requests for each IPSec connection. In the following, the case of updating a single IPSec connection is discussed, without limiting the invention to this behaviour.

Another method of performing the signalling is to use a separate protocol. The protocol should preferably provide encryption and/or authentication of the signalling messages.

The IKE protocol already has messages defined for e.g. deleting IPSec SAs. One method of providing the necessary signalling would be by adding a new IKE notification message type that requests a change in an existing IPSec SA. Such a message should provide its own encryption and/or authentication to avoid requiring an IKE connection set up from the new address, which would require extra messaging.

IP version 4 (IPv4) is the currently widely deployed Internet Protocol version. Its major disadvantage is the small number of unique, public IP addresses. IP version 6 (IPv6) has a much larger address space, which fixes the most important IPv4 problem known today. IPv6 also changes some other things in the Internet Protocol, for example, how fragmentation of packets is done, but these changes are quite small. Most protocols have separate definitions on how they are used within the IPv4 and the IPv6 context. For instance, there are separate versions of IPSec and Mobile IP for use with IPv4 and IPv6. However, such modifications to protocols are quite small, and do not usually change the essentials of the protocols significantly. The invention can be applied to both IPv4 and IPv6.

In the following, the invention is further described by means of figures and some examples. The intention is not to restrict the invention to the details of the following description or to the details of protocols such as the IPSec and IKE protocols which might be changed in the future.

FIGURES

Figure 1 illustrates an example of a telecommunication network to be used in the invention.

Figure 2 illustrates a second example of a telecommunication network to be used in the invention.

Figure 3 illustrates a third example of a telecommunication network to be used in the invention.

Figure 4 describes the prior art solution to enable mobility for IPSec connections.

Figure 5 describes the method of the invention to enable mobility for IPSec connections.

DETAILED DESCRIPTION

Figure 1 illustrates an example of a telecommunication network to be used in the invention. Thus, in figure 1, computer 1 may be a client computer and computer 2 a destination computer, to which the secure messages are sent in the invention by means of an IPSec tunnel established between computer 1 and computer 2. Computer 2 might be a security gateway for a third computer 3. Then, the messages sent from computer 2 to computer 3 are sent in plaintext. The security gateway can be a common security gateway for e.g. a company LAN, whereby there are several computers in the LAN protected by computer 2. The other protected computers are not shown in figure 1, but naturally, the invention covers also such networks.

The network of figure 2 otherwise corresponds to that of figure 1, but in figure 2 also computer 1 is a security gateway, e.g. for computer 4. Also here, the security gateway 1 can be a common security gateway for e.g. a company LAN, whereby there are several computers in the LAN protected by computer 1. The other protected computers are not shown in figure 2. But naturally, the invention covers also such networks. The messages between security gateway 1 and the computers it protects are sent in plaintext as the IPSec tunnel only exist between computers 1 and 2.

The network of figure 3 is a network, wherein the IPSec messages are sent between an end-to-end connection between two computers 1, 2 only whereby IPSec transport mode can be used instead of tunnel mode.

Figure 4 describes the prior art solution to enable mobility for IPSec connections. As a diagram, this is the standard IPSec procedure when establishing a tunnel between addresses A and X, and then B and X.

The protocol begins with the IKE main mode requiring 6 messages in total, see steps 1a - 6a in figure 4. The protocol involves strong user authentication, policy negotiation and the use of the Diffie-Hellman algorithm. Any other IKE phase 1 mode might of course be used as an alternative. Another approach to minimise the number of message exchanges would be to avoid IKE phase 1 and perform only the IKE quick mode (3 messages). However, IKE phase 1 is associated with IP addresses (along with other identifying information). A modified implementation might ignore IP addresses when processing IKE messages, and thus be able to maintain IKE phase 1 state between connection points.

The protocol then continues with IKE quick mode requiring 3 messages in total (steps 7a - 9a in figure 4). Quick mode includes IPSec policy negotiation and optionally the use of the Diffie-Hellman algorithm. An alternative IKE phase 2 exchange could of course be used instead of quick mode.

At this point the tunnel has been established between addresses A and X. 9 messages have been used along with the computational expense (each Diffie-Hellman computation may take hundreds of milliseconds, for instance, depending on the host), also the roundtrip times being considerable (9/2 = 4.5 roundtrips, with a roundtrip time of 500 ms this is 2.25 seconds for latency alone).

The movement of the mobile terminal to address B causes full re-negotiation and again IKE main mode requires 6 messages in total (steps 1b -6b in figure 4), strong user authentication, policy negotiation, and optionally the use of the Diffie-Hellman algorithm.

The use of the protocol continues with IKE quick mode requiring 3 messages total (steps 7b - 9b).

The tunnel between addresses B and X is now complete.

Figure 5 describes the method of the invention. To establish the tunnel between address A and host X, IKE main mode is again used requiring 6 messages in total (steps 1a - 6a in figure 5) as in figure 4 including strong user authentication, policy negotiation and the use of the Diffie-Hellman algorithm.

Then IKE quick mode is again used requiring 3 messages in total (steps 7a - 9a in figure 5). The quick mode includes IPSec policy negotiation, and optionally the use of the Diffie-Hellman algorithm.

Again, IKE main mode may be replaced by any other IKE phase 1 mode, and IKE quick mode by any other IKE phase 2 mode.

At this point the tunnel has been established between addresses A and X. 9 messages have been used along with the computational expense.

In the invention, movement to address B requires only a single round trip, when using registration request messages to be sent from the mobile terminal, when it moves from address A to address B. In signal 10a of figure 5, which is sent from the mobile terminal to the other end of the established IPSec tunnel when it has moved to address B, a request for registration (RREQ) of the new address is sent. Preferably, a reply message (RREP) is sent (step 11a) from the host to confirm the address change. Both signals 10a and 11a can be encrypted and/or authenticated. The encryption and/or authentication is preferably performed by using IPSec, in which case it is preferable to use the same IPSec SA for protecting both data and registration traffic.

11a is optional in the invention. The preferable encryption method is IPSec, preferably with the modified reception processing described previously. However, the exact method of signalling is not important, the essence is to carry over the IPSec SA to the new connection point.

The SA that existed between addresses A and X has now been changed to be between addresses B and X and is now complete. The next time the mobile terminal sends a message, host 2 in figure 1 - 3 is able to properly handle IPSec packets that come from address B and vice versa. Traffic can now flow inside the tunnel as normal with IPSec.

Any further movement from network to another can be accomplished with a similar exchange of signalling message(s). The IPSec SA does not need to be re-established until the lifetime of the SA has been exhausted.

The invention requires half a roundtrip if only a request message is used without a reply, and one roundtrip of the reply message is used.

The example describes the tunnel mode of IPSec, but transport mode can also be used. IPSec transport mode connections in examples can be replaced with IPSec tunnel mode connections and vice versa. IPSec transport mode combined with an external tunnelling protocol, such as the Layer 2 Tunnelling Protocol (L2TP), is a replacement for IPSec tunnel mode with regards to functionality.

The implementation may optimise the start of traffic flows with regard to message 10a (and optionally 11a); e.g. after sending 10a, the client may directly send IPSec-protected traffic. This essentially makes the handover latency zero, although it requires more complicated processing if the message 10a is lost while being delivered. However, the essential part of the invention is that it is possible to make the invention provide essentially zero-latency handover for client-to-server traffic, and half a roundtrip latency for server-to client traffic.

Different network topologies can, of course, be used in the invention. For instance in figure 1, the connection between hosts 2 and 3 may use IPSec transport or tunnel mode, instead of being plaintext, etc.

CLAIMS

1. Method for ensuring secure forwarding of a message in a telecommunication network, comprising at least one mobile terminal and another terminal, in which method the mobile terminal moves from a first address to a second address, characterized by
   a) establishing a secure connection between the first address of the mobile terminal and the other terminal defining at least the addresses of the two terminals,
   b) the mobile terminal moving from the first address to a second address.
   c) changing the connection to be between the second address and the other terminal by means of a request message from the mobile terminal to the other terminal to change the address of the secure connection to the second address.

2. Method of claim 1, characterized in that, the secure connection is established in step a) by forming a Security Association (SA) using the IPSec protocols.

3. Method of claim 1 or 2, characterized in that in step c) a reply back to the mobile terminal is sent from the other terminal after the request from the mobile terminal to change the address.

4. Method of any of claims 1 - 3, characterized in that the registration request and/or the reply message is encrypted and/or authenticated by using the same SA already established.

5. Method of any of claims 1 - 4, characterized in that the change of addresses in the secure connection as a result of the request message is performed by means of a central register of current address of the terminals belonging to the network.

6. Telecommunication network to perform the method of any of claims 1 - 5, comprising at least one mobile terminal and another terminal.

7. Network of claim 6, c h a r a c t e r i z e d in that the mobile terminal and the other terminal forms an end-to-end connection, whereby the secure connection is an IPSec transport connection or IPSec tunnel connection.

8. Network of claim 6, c h a r a c t e r i z e d in that one of or both of the mobile terminal and the other terminal is a security gateway protecting one or more computers, whereby IPSec tunnel mode or IPSec together with a tunnelling protocol is used for the secure connection between the mobile terminal and the other terminal.

9. Network of claim 6, c h a r a c t e r i z e d in that both terminals are mobile terminals.

10. Network of claim 9, c h a r a c t e r i z e d in that it further contains a central register of current locations of the terminals belonging to the network.

PATENT APPLICATION FEE DETERMINATION RECORD
Effective October 1, 2003

Application or Docket Number: 10/490932

CLAIMS AS FILED - PART I

	(Column 1)	(Column 2)
TOTAL CLAIMS		
FOR	NUMBER FILED	NUMBER EXTRA
TOTAL CHARGEABLE CLAIMS	10 minus 20=	* —
INDEPENDENT CLAIMS	1 minus 3 =	* —
MULTIPLE DEPENDENT CLAIM PRESENT		☐

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

SMALL ENTITY TYPE ☐		OR	OTHER THAN SMALL ENTITY	
RATE	FEE		RATE	FEE
BASIC FEE		OR	BASIC FEE	920
XS 9=		OR	XS16=	
X43=		OR	X86=	
+145=		OR	+290=	
TOTAL		OR	TOTAL	920

CLAIMS AS AMENDED - PART II

03/26/04

AMENDMENT A	(Column 1)		(Column 2)	(Column 3)
	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
Total	* 10	Minus	** 20	=
Independent	* 1	Minus	*** 3	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
XS 9=		OR	XS16=	
X43=		OR	X86=	
+145=		OR	+290=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT B	(Column 1)		(Column 2)	(Column 3)
	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
Total	*	Minus	**	=
Inoependent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
XS 9=		OR	XS16=	
X43=		OR	X86=	
+145=		OR	+290=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT C	(Column 1)		(Column 2)	(Column 3)
	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
XS 9=		OR	XS16=	
X43=		OR	X86=	
+145=		OR	+290=	
TOTAL ADDIT. FEE		OR	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.

RF:ar 6/25/04 290.1052USN

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Sami Vaarala, Antti Nuopponen

Serial No. 10/490,932

Filed: 26 March 2004

For: METHOD AND NETWORK FOR ENSURING SECURE FORWARDING OF MESSAGES

Examiner:

Date: 25 June 2004

Art Unit

Batch No.

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 25, 2004 AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO: MAIL STOP DD, COMMISSIONER FOR PATENTS, P.O. BOX 1450, ALEXANDRIA, VA 22313-1450.

Rolf Fasth
Attorney for Applicant

TRANSMITTAL LETTER

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

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

(X) Information Disclosure Statement (No references)
(X) The Commissioner is hereby authorized to charge any additional fees which may be required in connection with the filing of this information disclosure statement, or credit over-payment, to Account No. 06-0243.

Respectfully submitted,

FASTH LAW OFFICES

Rolf Fasth
Registration No. 36,999

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

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

RF:nr 6/25/04 290.1052USN

PATENT

Attorney Matter No. 290.1052USN

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of
Sami Vaarala, Antti Nuopponen

Serial No. 10/490,932 Art Unit

Filed: 26 March 2004 Confirmation No.

For: METHOD AND NETWORK FOR ENSURING SECURE FORWARDING OF MESSAGES

Examiner:

Date: June 25, 2004

INFORMATION DISCLOSURE STATEMENT

TO: COMMISSIONER FOR PATENTS

This Information Disclosure Statement is being filed to comply with the Applicant's duty of disclosure. Applicant knows of no information in addition to the references cited in the International Search Report that would be material to the patentability of the claimed invention.

Respectfully submitted,

FASTH LAW OFFICES

Rolf Fasth
Registration No. 36,999

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

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

#3

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.	FIRST NAMED APPLICANT	ATTY. DOCKET NO.
10/490,932	Sami Vaarala	290.1052USN

INTERNATIONAL APPLICATION NO.	
PCT/FI02/00770	
I.A. FILING DATE	PRIORITY DATE
09/27/2002	09/28/2001

Rolf Fasth
Fasth Law Offices
629 E Boca Raton Road
Phoenix, AZ 85022

CONFIRMATION NO. 2427

371 FORMALITIES LETTER

OC000000013744998

Date Mailed: 09/09/2004

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 03/26/2004
- Copy of the International Search Report filed on 03/26/2004
- Copy of IPE Report filed on 03/26/2004
- Copy of Annexes to the IPER filed on 03/26/2004
- Preliminary Amendments filed on 03/26/2004
- Oath or Declaration filed on 03/26/2004
- Request for Immediate Examination filed on 03/26/2004
- U.S. Basic National Fees filed on 03/26/2004
- Priority Documents filed on 03/26/2004

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.*

TAMALA D HOLLAND

Telephone: (703) 305-5483

PART 2 - OFFICE COPY

U.S. APPLICATION NUMBER NO.	INTERNATIONAL APPLICATION NO.	ATTY. DOCKET NO.
10/490,932	PCT/FI02/00770	290.1052USN

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

PATENT #4

RF:nz 11/17/04 290.1052USN

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Sami Vaarala, Antti Nuopponen

Serial No. 10/490,932

Filed: 26 March 2004
I.A. filed: 27 September 2002

For: METHOD AND NETWORK FOR ENSURING SECURE FORWARDING OF MESSAGES

Examiner:

Date: 17 November 2004

Art Unit

Confirmation No. 2427

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 November 17, 2004 AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO: MAIL STOP MISSING PARTS, COMMISSIONER FOR PATENTS, P.O. BOX 1450, ALEXANDRIA, VA 22313-1450.

Rolf Fasth
Attorney for Applicant

TRANSMITTAL LETTER

MAIL STOP MISSING PARTS
COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

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

(X) Notification of Missing Requirements mailed 9 September 2004
(X) Signed Oath or Declaration of the inventor
(X) Check #4049 for $120.00 to cover surcharge for providing signed oath or declaration later than 30 months from priority date ($65.00) and ONE MONTH EXTENSION in replying to Missing Requirements Notification ($55.00)
(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.

11/29/2004 MKAYPAGH 00000082 10490932
01 FC:2251 55.00 DP

11/29/2004 MKAYPAGH 00000082 10490932
02 FC:2657 65.00 DP

Respectfully submitted,
FASTH LAW OFFICES

Rolf Fasth
Registration No. 36,999

FASTH LAW OFFICES
629 E. Boca Raton Road
Phoenix, AZ 85022
Telephone: 602-993-9099
Facsimile: 602-942-8364
cc: Paivi Soderman (Your ref: S0059US)

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.	FIRST NAMED APPLICANT	ATTY. DOCKET NO.
10/490,932	Sami Vaarala	290.1052USN

INTERNATIONAL APPLICATION NO.	
PCT/FI02/00770	
I.A. FILING DATE	PRIORITY DATE
09/27/2002	09/28/2001

Rolf Fasth
Fasth Law Offices
629 E Boca Raton Road
Phoenix, AZ 85022

CONFIRMATION NO. 2427

371 FORMALITIES LETTER

OC000000013744998

Date Mailed: 09/09/2004

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 03/26/2004
- Copy of the International Search Report filed on 03/26/2004
- Copy of IPE Report filed on 03/26/2004
- Copy of Annexes to the IPER filed on 03/26/2004
- Preliminary Amendments filed on 03/26/2004
- Oath or Declaration filed on 03/26/2004
- Request for Immediate Examination filed on 03/26/2004
- U.S. Basic National Fees filed on 03/26/2004
- Priority Documents filed on 03/26/2004

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.*

TAMALA D HOLLAND

Telephone: (703) 305-5483

PART 1 - ATTORNEY/APPLICANT COPY

U.S. APPLICATION NUMBER NO.	INTERNATIONAL APPLICATION NO.	ATTY. DOCKET NO.
10/490,932	PCT/FI02/00770	290.1052USN

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

RF 3/28/04 290.1052USN

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 NETWORK FOR ENSURING SECURE FORWARDING OF MESSAGES, the specification of which was filed as International Patent Application No. PCT/FI02/00770, on 27 September 2002.

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
20011910 (Number)	Finland (Country)	28 Sept. 2001 (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:

(not applicable)	(n/a)	(not applicable)
(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.

RF 3/29/04 290.1052USN

100

Full name of first joint inventor: Sami Vaarala

Inventor's signature Sami V 10.5.2004 Date

Residence: Helsinki, Finland FIX

Citizenship: Finland

Post Office address: ~~Neljas Linja 22 A 24~~ ~~FIN-00530 Helsinki, Finland~~ SÄTERINRINNE 8 B 37 02600 ESPOO

200

Full name of second joint inventor: Antti Nuopponen

Inventor's signature 10.5.2004 Date

Residence: Espoo, Finland FIX

Citizenship: Finland

Post Office address: Kaksoiskiventie 7-9 A 1
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. 2427

SERIAL NUMBER	FILING OR 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
10/490,932	11/22/2004 RULE	455	2681	290.1052USN

APPLICANTS

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

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

This application is a 371 of PCT/FI02/00770 09/27/2002

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

FINLAND 20011910 09/28/2001

** SMALL ENTITY **

Foreign Priority claimed	STATE OR COUNTRY	SHEETS DRAWING	TOTAL CLAIMS	INDEPENDENT CLAIMS
☐ yes ☐ no	FINLAND		10	1

35 USC 119 (a-d) conditions met ☐ yes ☐ no ☐ Met after Allowance

Verified and Acknowledged _____ Examiner's Signature Initials

ADDRESS

Rolf Fasth

Fasth Law Offices

629 E Boca Raton

Phoenix ,AZ 85022

TITLE

Method and nework for ensuring secure forwarding of messages

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

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.	FIRST NAMED APPLICANT	ATTY. DOCKET NO.
10/490,932	Sami Vaarala	290.1052USN

INTERNATIONAL APPLICATION NO.	
PCT/FI02/00770	
I.A. FILING DATE	PRIORITY DATE
09/27/2002	09/28/2001

Rolf Fasth
Fasth Law Offices
629 E Boca Raton
Phoenix, AZ 85022

CONFIRMATION NO. 2427

371 ACCEPTANCE LETTER

OC000000014787165

Date Mailed: 12/27/2004

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:

11/22/2004	11/22/2004
DATE OF RECEIPT OF 35 U.S.C. 371(c)(1), (c)(2) and (c)(4) REQUIREMENTS	DATE OF COMPLETION OF ALL 35 U.S.C. 371 REQUIREMENTS

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 03/26/2004
- Copy of the International Search Report filed on 03/26/2004
- Copy of IPE Report filed on 03/26/2004
- Copy of Annexes to the IPER filed on 03/26/2004
- Preliminary Amendments filed on 03/26/2004
- Oath or Declaration filed on 11/22/2004

- Request for Immediate Examination filed on 03/26/2004
- U.S. Basic National Fees filed on 03/26/2004
- Priority Documents filed on 03/26/2004

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)

TAMALA D HOLLAND

Telephone: (703) 305-5483

PART 3 - OFFICE COPY

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

TFW 2681

PTO/SB/122 (04-05)
Approved for use through 07/31/2006. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

CHANGE OF CORRESPONDENCE ADDRESS
Application

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

Application Number	10/480,932
Filing Date	22 NOVEMBER 2004
First Named Inventor	SAMI VAARALLA
Art Unit	2681
Examiner Name	
Attorney Docket Number	290.1052USN

Please change the Correspondence Address for the above-identified patent application to:

☑ The address associated with Customer Number: 33369

OR

☐ Firm or Individual Name

33369
PATENT TRADEMARK OFFICE

Address

City | State | Zip

Country

Telephone | Email

This form cannot be used to change the data associated with a Customer Number. To change the data associated with an existing Customer Number use "Request for Customer Number Data Change" (PTO/SB/124).

I am the:

☐ Applicant/Inventor

☐ Assignee of record of the entire interest. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96).

☑ Attorney or agent of record. Registration Number 36,999

☐ Registered practitioner named in the application transmittal letter in an application without an executed oath or declaration. See 37 CFR 1.33(a)(1). Registration Number _____

Signature Rolf Fasth

Typed or Printed Name ROLF FASTH

Date ~~13 Oct 2005~~ 16JAN.2006 Telephone 910-687-0001

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

☑ *Total of 1 forms are submitted.

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

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

33369
PATENT TRADEMARK OFFICE

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	17	(mobile or terminal)adj2 IPsec with tunnel$4	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/29 19:30
L2	12	(mobile or terminal)near IPsec with tunnel$4	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/29 19:30
L3	1	L1 and "380"/$.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/29 19:31
L4	1	L2 and "380"/$.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/29 19:31
L5	345	713/161.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/29 19:32
L6	38	L5 and IPsec	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/29 19:32
L7	20	L6 and (moblie or telephone or terminal)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/29 19:33
S2	11807	secur$3 with connect$4 near terminal	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/29 14:30

EAST Search History

S4	36	S2 and ipsec with protocol	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/29 14:50
S5	9	VAARALA near SAMI	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/29 14:51
S6	9	NUOPPONEN near ANTTI	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/29 14:51
S7	5	S5 and ipsec	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/29 15:03
S8	5	S6 and ipsec	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/29 15:48
S9	9	signal$4 near IPsec	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/29 16:56
S10	0	wo-0139538-$.did.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/29 16:58
S11	1	wo-200139538-$.did.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/29 16:59

EAST Search History

S12	1	wo-200041427-$.did.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/29 17:00
S13	6	IPsec with telecommunicat$3 with terminal	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/29 17:45
S14	2	"6587680".pn.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/29 19:28

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.
10/490,932	11/22/2004	Sami Vaarala	290.1052USN	2427

33369 7590 07/06/2007
FASTH LAW OFFICES (ROLF FASTH)
26 PINECREST PLAZA, SUITE 2
SOUTHERN PINES, NC 28387-4301

EXAMINER	
YALEW, FIKREMARIAM A	
ART UNIT	**PAPER NUMBER**
2136	
MAIL DATE	**DELIVERY MODE**
07/06/2007	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.	Applicant(s)	
	10/490,932	VAARALA ET AL.	
	Examiner	Art Unit	
	Fikremariam Yalew	2136	

-- 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 *10 January 2007*.

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) *1-10* 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) *1-10* is/are rejected.

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

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

Application Papers

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

10)☒ The drawing(s) filed on *26 June 2004* 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 *06/29/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-10 have been examined.

Claim Objections

2. Claim 6 is objected to because of the following informalities: Claim 6 has similar claim limitation with claim 1 and it doesn't further limit. Appropriate correction is required.

Claim Rejections - 35 USC § 102

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

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-10 are rejected under 35 U.S.C. 102(b) as being anticipated by Ala-Laurila et al (hereinafter referred as Ala) US Patent No 6,587,680 B1.

5. As per claim 1: Ala discloses a method for ensuring secure forwarding of a message in a telecommunication network, having at least one mobile terminal and another terminal, the method comprising:

a) establishing a secure connection between a first address of the mobile terminal and the other terminal, the secure connection defined by at least the addresses of the two terminals(col 8 lines 1-3(i.e., security association exists) and Fig 2),

b) the mobile terminal moving from the first address to a second address(See col 8 lines 6-9(i.e., mobile terminal moves from cell to cell) and Fig 2), and

c) changing the connection to be defined between the second address and the other terminal by means of a request message from the mobile terminal to the other terminal to change the address in the definition of the secure connection to the second address(i.e., abstract and Fig 2 (i.e., existing security association is re-established when communication handover event occurs in a radio communications system.....by a challenge/response procedure)).

6. As per claim 2: Ala discloses the method characterized in that, the secure connection is established in step a) by forming a Security Association (SA) using the IPSec protocols (See col 5 lines 27-36 and Fig 2 IPsec tunneling, SA Parameter).

7. As per claim 3: Ala discloses the method characterized in that in step c) a reply back to the mobile terminal is sent from the other terminal after the request from the mobile terminal to change the address (See Fig 2 and col 5 lines 43-50).

8. As per claim 4: Ala discloses the method characterized in that the registration request and/or the reply message is encrypted and/or authenticated by using the same SA already established (See col 8 lines 1-22 and Fig 2).

9. As per claim 5: Ala discloses the method characterized in that the change of addresses in the secure connection as a result of the request message is performed by

means of a central register of current address of the terminals belonging to the network (See col 8 lines 17-22).

10. As per claim 6: Ala discloses the method wherein the method further comprises providing a telecommunication network that has at least one mobile terminal and another terminal and a secure connection defined between a first address of the mobile terminal and the other terminal, characterized by means for changing the connection to be defined between a second address of the mobile terminal and the other terminal (See abstract and Fig 2).

11. As per claim 7: Ala discloses the method characterized in that the mobile terminal and the other terminal forms an end-to-end connection whereby the secure connection is an IPSec transport connection or IPSec tunnel connection (See Fig 2 IPsec tunneling, SA Parameter).

12. As per claim 8: Ala discloses the method characterized in that one of or both of the mobile terminal and the other terminal is a security gateway protecting one or more computers, whereby IPSec tunnel mode or IPSec together with a tunneling protocol is used for the secure connection between the mobile terminal and the other terminal IPsec tunneling, SA Parameter).

13. As per claim 9: Ala discloses the method characterized in that both terminals are mobile terminals (See col 8 lines 17-22 and Fig 2).

14. As per claim 10: Ala discloses the method further comprises providing a central register of current locations of the terminals belonging to the network (See col 7 lines 46-67).

Conclusion

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO 892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fikremariam Yalew whose telephone number is 5712723852. The examiner can normally be reached on 9-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Fikremariam Yalew
06/29/2006
FA

Art Unit 2136
NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

7,2,07

Notice of References Cited	Application/Control No. 10/490,932	Applicant(s)/Patent Under Reexamination VAARALA ET AL.	
	Examiner Fikremariam Yalew	Art Unit 2136	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,587,680	07-2003	Ala-Laurila et al.	455/411
*	B	US-6,418,130	07-2002	Cheng et al.	370/331
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	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. 2427

SERIAL NUMBER	FILING OR 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
10/490,932	11/22/2004 RULE	713	2136	290.1052USN

APPLICANTS

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

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

This application is a 371 of PCT/FI02/00770 09/27/2002

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

FINLAND 20011910 09/28/2001

** SMALL ENTITY **

		STATE OR COUNTRY	SHEETS DRAWING	TOTAL CLAIMS	INDEPENDENT CLAIMS
Foreign Priority claimed	☒ yes ☐ no	FINLAND	0	10	1
35 USC 119 (a-d) conditions met	☒ yes ☐ no ☐ Met after Allowance				
Verified and Acknowledged	Examiner's Signature: [signature] Initials: FA				

ADDRESS
33369

TITLE
Method and nework for ensuring secure forwarding of messages

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

Search Notes	Application/Control No.	Applicant(s)/Patent under Reexamination
	10/490,932	VAARALA ET AL.
	Examiner	Art Unit
	Fikremariam Yalew	2136

SEARCHED			
Class	Subclass	Date	Examiner
713	161	6/29/2007	FA
380	247	6/29/2007	FA

INTERFERENCE SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES (INCLUDING SEARCH STRATEGY)		
	DATE	EXMR
East(text search and classification search)	6/29/2007	FA
IEEE	6/29/2007	FA
Google Patent	6/29/2007	FA

Index of Claims

Application/Control No.	Applicant(s)/Patent under Reexamination
10/490,932	VAARALA ET AL.
Examiner	**Art Unit**
Fikremariam Yalew	2136

√	Rejected	–	(Through numeral) Cancelled	N	Non-Elected	A	Appeal
=	Allowed	+	Restricted	I	Interference	O	Objected

Claim		Date
Final	Original	
	1	05/29/07
	2	~
	3	~
	4	~
	5	~
	6	~
	7	~
	8	~
	9	~
	10	√
	11	
	12	
	13	
	14	
	15	
	16	
	17	
	18	
	19	
	20	
	21	
	22	
	23	
	24	
	25	
	26	
	27	
	28	
	29	
	30	
	31	
	32	
	33	
	34	
	35	
	36	
	37	
	38	
	39	
	40	
	41	
	42	
	43	
	44	
	45	
	46	
	47	
	48	
	49	
	50	

Claim		Date
Final	Original	
	51	
	52	
	53	
	54	
	55	
	56	
	57	
	58	
	59	
	60	
	61	
	62	
	63	
	64	
	65	
	66	
	67	
	68	
	69	
	70	
	71	
	72	
	73	
	74	
	75	
	76	
	77	
	78	
	79	
	80	
	81	
	82	
	83	
	84	
	85	
	86	
	87	
	88	
	89	
	90	
	91	
	92	
	93	
	94	
	95	
	96	
	97	
	98	
	99	
	100	

Claim		Date
Final	Original	
	101	
	102	
	103	
	104	
	105	
	106	
	107	
	108	
	109	
	110	
	111	
	112	
	113	
	114	
	115	
	116	
	117	
	118	
	119	
	120	
	121	
	122	
	123	
	124	
	125	
	126	
	127	
	128	
	129	
	130	
	131	
	132	
	133	
	134	
	135	
	136	
	137	
	138	
	139	
	140	
	141	
	142	
	143	
	144	
	145	
	146	
	147	
	148	
	149	
	150	

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of Art Unit 2136

Sami Vaarala, Antti Nuopponen

Serial No. 10/490,932

Filed: 22 November 2004

For: METHOD AND NETWORK FOR ENSURING SECURE FORWARDING OF MESSAGES

Examiner: Yalew, Fikremariam A

Date: 30 August 2007

ATTORNEY DOCKET NO. 290.1052USN

AMENDMENT

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

This is in response to the Office action of 6 July, 2007. Please amend the above-identified patent application as follows:

In the Claims:

Amend the claims as follows:

1. (Currently amended) A method for ensuring secure forwarding of a message in a telecommunication network, having at least one mobile terminal and another terminal, the method comprising:
a) establishing a secure connection between a first address of the mobile terminal and a first address of the other terminal, the secure connection defined by at least the addresses of the two terminals,
b) the mobile terminal moving from the first address of the mobile terminal to a second address, and
c) while at the second address, the mobile terminal sending a request message to the first address of the other terminal to request the other terminal to change the secure connection ~~changing the connection~~ to be defined between the second address and the first address of the other terminal, and the other terminal, while at the first address of the other terminal, changing an address definition of the secure connection from the first address to the second address ~~by means of a request message from the mobile terminal to the other terminal to change the address in the definition of the secure connection to the second address~~.

2. (Currently amended) The method of claim 1, ~~characterized in that,~~ wherein the secure connection is established in step a) by forming a Security Association (SA) using IPSec protocols.

3. (Currently amended) The method of claim 1, ~~characterized in that~~ wherein in step c) a reply back to the mobile terminal is sent from the other terminal after the request from the mobile terminal to change the address.

4. (Currently amended) The method of claim 1, ~~characterized in that~~ wherein the registration request and/or the reply message is encrypted and/or authenticated by using the same SA already established.

5. (Currently amended) The method of claim 1, ~~characterized in that~~ wherein the change of addresses in the secure connection as a result of the request message is performed by means of a central register of current address of the terminals belonging to the network.

6. (Currently amended) The method of claim 1 wherein the method further comprises the other terminal sending back a reply message to the mobile terminal at the second address to confirm the address change. ~~providing a telecommunication network that has at least one mobile terminal and another terminal and a secure connection defined between a first address of the mobile terminal and the other terminal, characterized by means for changing the connection to be defined between a second address of the mobile terminal and the other terminal.~~

7. (Currently amended) The method of claim 6, ~~characterized in that~~ wherein the mobile terminal and the other terminal forms an end-to-end connection whereby the secure connection is an IPSec transport connection or IPSec tunnel connection.

8. (Currently amended) The method of claim 6, ~~characterized in that~~ wherein one of or both of the mobile terminal and the other terminal is a security gateway protecting one or more computers, whereby IPSec tunnel mode or IPSec together with a tunneling protocol is used for the secure connection between the mobile terminal and the other terminal.

9. (Currently amended) The method of claim 6, ~~characterized in that~~ wherein both terminals are mobile terminals.

10. (Previously presented) The method of claim 9, wherein the method further comprises providing a central register of current locations of the terminals belonging to the network.

REMARKS

Reconsideration of the application is respectfully requested. Applicants notice that the Office action states that it is in response to communication filed 10 January 2007. This must be a mistake. There is no record of sending in anything on 10 January 2007. The current application was filed 22 November 2004 and applicants believe the current Office action is responsive to communication filed on 22 November 2004.

Claim 6 was objected to since the claim did not further limit claim 1. Claim 6 has been amended to provide the required limitation. Claim 6 should now be in full conformance.

Claims 1-10 were rejected under Section 102 as being anticipated by Ala-Laurila (US Patent No. 6,587,680). This rejection is respectfully traversed.

To summarize the method of the present invention, it is an effective method and network for ensuring secure forwarding of a message as a first terminal moves from a first address to a second address. The secure connection is changed to be between the second address and another terminal as a result of an address change request from the first terminal. This is done without the need for cumbersome and time consuming exchange of security keys required to set up a new security association.

Ala merely discloses a conventional system for transferring a security association during a mobile terminal handover. This means the mobile terminal is moved from a first address to a second adress and a new access point is established between the mobile-terminal at the second address that belongs to a new coverage area of the new access point. Ala's system requires a change of the location of both the mobile terminal and the access points. The original access point is not really used by the mobile terminal while at the

second address.

In col. 5, lines 37-42, Ala explains that a challenge/response procedure is used to authenticate a mobile terminal during a handover event. The new AP (access point), not the mobile terminal, sends a challenge to the mobile terminal and the mobile terminal responds by sending a response. In col. 5, lines 51-58, Ala explains that the new AP requests the keys and other information that is transferred from the old AP to the new AP (so that all such communication is between the two APs and not between the old AP and the mobile terminal). More importantly, the mobile terminal in Ala's system does not send a request to the old AP to request the old AP to change the address from the first address to the second address in the security association.

In col. 8, lines 49-61, Ala describes the procedure for a backward handover where the handover is requested by the mobile terminal in communication with the old AP. A radio interface message 31 carries the authentication challenge from old AP to the mobile terminal to trigger the backward handover. The authentication challenge is used to indicate to the mobile terminal to disconnect from the old AP and connect to the new AP whereat a security association has already been prepared for the mobile terminal.

This means the mobile terminal never sends a request to the old AP to change the security association to be defined the second address and the original address of the old AP, as required by the amended claim 1.

It is submitted that it would not make sense for the mobile terminal to send such a request to the old AP since the mobile terminal has been instructed to disconnect from the old AP since the new security association has been set up between the new AP and the mobile terminal at the second address without any real participation by the mobile terminal. When the mobile terminal connects to the new AP, the security association has already been set up for the mobile terminal.

In col. 10, lines 32 to col. 11, line 8, Ala explains that when the handover request is sent from the mobile terminal to the old AP, the message is received by the old AP. The old AP then retrieves the security association from its database and sends a handover request that contains the SA parameters to the new AP (lines 47-49). In other words, there is no communication between the mobile terminal and the old AP. More importantly, the old AP does not change the definition of the secure connection to be between the second address of the mobile terminal and the original address of the old AP. In contrast, the new AP in Ala's system then creates the new security association and generates a challenge to authenticate the mobile terminal and the handover request is sent to the old AP. The old AP then sends a disassociate message to the mobile terminal (lines 59-60). The mobile terminal updates its security association parameters to include the new AP and sends a challenge to authenticate the new AP. It is important to note that Ala's mobile terminal never requests the old AP to change the addresses in the security association.

It is submitted that it would not be obvious to modify Ala to include the steps required of the amended claim 1. For example, the first terminal in Ala's system could not send the request to the first address of the second terminal i.e. the old AP, since the mobile terminal has been disassociated from the old AP when the mobile terminal is at the second address. It is submitted that Ala's system would not be operational if the mobile terminal tried to send the request to the original address of the old AP while the mobile terminal is at the second address.

Applicants fails to see why a person of ordinary skill in the art would look to Ala and the other cited references to learn about the features of the amended claim 1 when such features are completely missing in the cited references. All the cited references fail to teach or suggest

the step of the mobile terminal, while at the second address, sending a request message to the first address of the other terminal to request the other terminal to change the secure connection to be defined between the second address of the mobile terminal and the first address of the other terminal.

On page 3, paragraph 5c, of the Office action, the Examiner refers to the challenge/response procedure. It is correct that Ala teaches the challenge/response procedure but this procedure in Ala's system is different from the steps of the amended claim 1 of the present invention. In Ala's system the new AP, at the new second address, sends a challenge to the mobile terminal and the mobile terminal responds to this message (col. 5, lines 27-36 referred to by the Examiner). Ala fails to teach or suggest:

1) While at the second address, the mobile terminal sending a request message to the first address of the other terminal to change the secure connection to be defined between the second address of the mobile terminal and the first address of the other terminal, and

2) The other terminal, at the first address of the other terminal, changing an address definition of the secure connection from the first address of the mobile terminal to the second address of the mobile terminal.

In summary, Ala's mobile terminal never sends a request message to the old AP to change the secure connection to be defined between the second address of the mobile terminal and the original first address of the old AP. In contrast, in Ala's system the old AP sends this request to the new AP, as described in col. 10, lines 43-49. Also, Ala's old AP never changes any address definition in the secure connection. In contrast, the new AP (not the old AP), at the new second address, creates the new security association between the new AP and the second address of the mobile terminal, as explained in col. 10, lines 50-52.

It is submitted that Ala and the other cited

references would require extensive modifications that are not taught or suggested, to meet the requirements of the amended claim 1. It is also submitted that those modifications are not obvious since Ala completely fails to teach or suggest the required modifications.

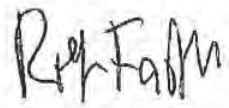
In view of the above, it is submitted that the amended claim 1 is allowable.

Claims 2-10 are submitted to be allowable because the claims depend upon the allowable base claim 1 and because each claim includes limitations that are not taught or suggested in the cited references.

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

Respectfully submitted,

FASTH LAW OFFICES



Rolf Fasth
Registration No. 36,999

ATTORNEY DOCKET NO. 290.1052USN

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

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

cc: Lisbeth Soderman, IprBox
(Your ref: S00051US)

Attorney Docket No. 290.1052USN PATENT
RF:ss 8/30/07

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Sami Vaarala,
Antti Nuopponen

Art Unit 2136
Confirmation No. 2427

Serial No. 10/490,932

Filed: 22 November 2004

For: METHOD AND NETWORK FOR ENSURING SECURE FORWARDING OF MESSAGES

Examiner: Fikremariam A. Yalew

Date: 30 August 2007

CERTIFICATE OF MAILING

I HEREBY CERTIFY THAT THIS PAPER AND THE DOCUMENTS REFERRED TO AS BEING ATTACHED OR ENCLOSED HEREWITH ARE BEING SUBMITTED ELECTRONICALLY TO THE UNITED STATES PATENT AND TRADEMARK OFFICE ON **30 August 2007.**

/rfasth/

Rolf Fasth
Attorney for Applicant

TRANSMITTAL LETTER

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

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

(X) Response to Office Action dated 6 July 2007.
(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. 290.1052USN

Electronic Acknowledgement Receipt

EFS ID:	2141210
Application Number:	10490932
International Application Number:	
Confirmation Number:	2427
Title of Invention:	Method and nework for ensuring secure forwarding of messages
First Named Inventor/Applicant Name:	Sami Vaarala
Customer Number:	33369
Filer:	Rolf Fasth/Sloan Smith
Filer Authorized By:	Rolf Fasth
Attorney Docket Number:	290.1052USN
Receipt Date:	30-AUG-2007
Filing Date:	22-NOV-2004
Time Stamp:	12:02:44
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	269740 4ff381973b9ae97c78a0fdb35ad1713a0e8414fd	yes	9

	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Amendment - After Non-Final Rejection		1	1	
	Claims		2	4	
	Applicant Arguments/Remarks Made in an Amendment		5	9	
Warnings:					
Information:					
2	Miscellaneous Incoming Letter	TRX.PDF	34362 6e180bcf14513371822b7c776a42f14c1bd2e28	no	1
Warnings:					
Information:					
		Total Files Size (in bytes):	304102		

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
10/490,932	11/22/2004	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☒ RATE ($)	SMALL ENTITY ☒ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	08/30/2007	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 10	Minus	** 20	= 0	X $25 =	0	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 1	Minus	***3	= 0	X $100 =	0	OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

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

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

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

Legal Instrument Examiner:
Juliet McMillan

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.

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	2	"6587680".pn.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/11/05 16:18
L2	385	713/161.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/11/05 17:39
L3	1	L2 and (mobile with terminal)(address with change)(IPSEC)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/11/05 17:42
L5	344	380/247.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/11/05 17:44
L6	1	L5 and (mobile with terminal)(IPSEC)(address with change)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/11/05 17:44
L7	1	(modify$3 or upgrad$3 or refresh$3 or chang$3) near IPsec with signal$4	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/11/05 17:45
L8	16	(modify$3 or upgrad$3 or refresh$3 or chang$3) same IPsec with signal$4	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/11/05 17:52
L9	4	713/151.ccls. and (mobile with terminal)(IPSEC)((updat$3 or chang$3 or upgrad$3) with address)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/11/05 17:53

EAST Search History

S3	0	(((moblie with terminal)with request)(AP or Access with point))(chang$3 or upgrad$4 or refresh$3)with (SA or security with association)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/11/05 14:04
S5	1041	(mobile with terminal)(access with point or AP)(chang$3 or upgrad$3 or refesh$3)with address	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/11/05 14:06
S6	110	S5 and (security with association or SA)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/11/05 14:06
S7	8	S6 and "713"/$.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/11/05 17:39
S8	4	S6 and "380"/$.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/11/05 14:07
S9	8	S6 and "726"/$.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/11/05 14:18
S10	9	VAARALA near SAMI	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/11/05 14:56
S11	3	"20020066036"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/11/05 16:18

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.
10/490,932	11/22/2004	Sami Vaarala	290.1052USN	2427

33369 7590 11/07/2007
FASTH LAW OFFICES (ROLF FASTH)
26 PINECREST PLAZA, SUITE 2
SOUTHERN PINES, NC 28387-4301

EXAMINER	
YALEW, FIKREMARIAM A	
ART UNIT	PAPER NUMBER
2136	
MAIL DATE	DELIVERY MODE
11/07/2007	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.	Applicant(s)	
	10/490,932	VAARALA ET AL.	
	Examiner	Art Unit	
	Fikremariam Yalew	2136	

-- 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 *30 August 2007*.

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) *1-10* 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) *1-10* is/are rejected.

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

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

Application Papers

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

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

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

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

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

Priority under 35 U.S.C. § 119

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

a)☐ All b)☐ Some * c)☐ None of:

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

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

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

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

Attachment(s)

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

DETAILED ACTION

1. The office action is in replay to an amendment filed on 08/30/2007. Claims 1-10 have been amended. Claims 1-10 are pending.

2. The examiner withdraws the claim objection based on applicant amendment.

Response to Arguments

3. Applicant's arguments with respect to claim 1-10 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

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

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

5. Claims 1-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ala-Laurila et al (hereinafter referred as Ala) US Patent No 6,587,680 B1 in view of Makineni et al(hereinafter referred as Makineni) US Pub No 20020066036.

6. As per claim 1: Ala discloses a method for ensuring secure forwarding of a message in a telecommunication network, having at least one mobile terminal and another terminal, the method comprising:

a) establishing a secure connection between a first address of the mobile terminal and the other terminal and first address of the other terminal, the secure

connection defined by at least the addresses of the two terminals(col 8 lines 1-22 and Fig 2),

b) the mobile terminal moving from the first address of the mobile terminal to a second address(See col 8 lines 6-9 and Fig 2)

Ala does not explicitly teach c) while at the second address, the mobile terminal sending a request message to the first address of the other terminal to request the other terminal to change the secure connection to be defined between the second address and the first address of the other terminal, and the other terminal, while at the first address of the other terminal, changing and address definition of the other terminal, changing and address definition of the secure connection from the first address to the second address.

However Makineni discloses c) while at the second address, the mobile terminal sending a request message to the first address of the other terminal to request the other terminal to change the secure connection to be defined between the second address and the first address of the other terminal, and the other terminal, while at the first address of the other terminal, changing and address definition of the other terminal, changing and address definition of the secure connection from the first address to the second address(See 0026-0028).

Therefore it would have been obvious to one having ordinary skill in the art at that time the invention was made to modify the teaching method of Makineni within Ala method inorder to provide secure communication from any location and at anytime (See Makineni 0010).

7. As per claim 2: the combination of Ala and Makineni disclose the method wherein, the secure connection is established in step a) by forming a Security Association (SA) using the IPSec protocols (See Ala col 5 lines 27-36 and Fig 2).

8. As per claim 3: the combination of Ala and Makineni disclose the method wherein that in step c) a reply back to the mobile terminal is sent from the other terminal after the request from the mobile terminal to change the address (See Ala Fig 2 and col 5 lines 43-50).

9. As per claim 4: the combination of Ala and Makineni disclose the method wherein the registration request and/or the reply message is encrypted and/or authenticated by using the same SA already established (See Ala col 8 lines 1-22 and Fig 2).

10. As per claim 5: the combination of Ala and Makineni disclose the method wherein the change of addresses in the secure connection as a result of the request message is performed by means of a central register of current address of the terminals belonging to the network (See Ala col 8 lines 17-22).

11. As per claim 6: the combination of Ala and Makineni disclose the method wherein the method further comprises the other terminal sending back a replay message to the mobile terminal at the second address to confirm address change(See Makineni 0026-0028).

12. As per claim 7: the combination of Ala and Makineni disclose the method wherein the mobile terminal and the other terminal forms an end-to-end connection whereby the

secure connection is an IPSec transport connection or IPSec tunnel connection (See Ala Fig 2 IPsec tunneling, SA Parameter).

13. As per claim 8: the combination of Ala and Makineni disclose the method wherein one of or both of the mobile terminal and the other terminal is a security gateway protecting one or more computers, whereby IPSec tunnel mode or IPSec together with a tunneling protocol is used for the secure connection between the mobile terminal and the other terminal (See Ala Fig2 IPsec tunneling, SA Parameter).

14. As per claim 9: the combination of Ala and Makineni disclose the method wherein both terminals are mobile terminals (See Ala col 8 lines 17-22 and Fig 2).

15. As per claim 10: the combination of Ala and Makineni disclose the method further comprises providing a central register of current locations of the terminals belonging to the network (See Ala col 7 lines 46-67).

Conclusion

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

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fikremariam Yalew whose telephone number is 5712723852. The examiner can normally be reached on 9-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Fikremariam Yalew
11/05/2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Art Unit 2136

11/5/07

Notice of References Cited	Application/Control No. 10/490,932	Applicant(s)/Patent Under Reexamination VAARALA ET AL.	
	Examiner Fikremariam Yalew	Art Unit 2136	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,587,680	07-2003	Ala-Laurila et al.	455/411
*	B	US-6,418,130	07-2002	Cheng et al.	370/331
*	C	US-2002/0066036	05-2002	Makineni et al.	713/201
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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

Index of Claims

Application/Control No.	Applicant(s)/Patent under Reexamination
10/490,932	VAARALA ET AL.
Examiner	**Art Unit**
Fikremariam Yalew	2136

√	Rejected	–	(Through numeral) Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

Claim		Date
Final	Original	
	1	10/25/07
	2	
	3	
	4	
	5	
	6	
	7	
	8	
	9	
	10	
	11	
	12	
	13	
	14	
	15	
	16	
	17	
	18	
	19	
	20	
	21	
	22	
	23	
	24	
	25	
	26	
	27	
	28	
	29	
	30	
	31	
	32	
	33	
	34	
	35	
	36	
	37	
	38	
	39	
	40	
	41	
	42	
	43	
	44	
	45	
	46	
	47	
	48	
	49	
	50	

Claim		Date
Final	Original	
	51	
	52	
	53	
	54	
	55	
	56	
	57	
	58	
	59	
	60	
	61	
	62	
	63	
	64	
	65	
	66	
	67	
	68	
	69	
	70	
	71	
	72	
	73	
	74	
	75	
	76	
	77	
	78	
	79	
	80	
	81	
	82	
	83	
	84	
	85	
	86	
	87	
	88	
	89	
	90	
	91	
	92	
	93	
	94	
	95	
	96	
	97	
	98	
	99	
	100	

Claim		Date
Final	Original	
	101	
	102	
	103	
	104	
	105	
	106	
	107	
	108	
	109	
	110	
	111	
	112	
	113	
	114	
	115	
	116	
	117	
	118	
	119	
	120	
	121	
	122	
	123	
	124	
	125	
	126	
	127	
	128	
	129	
	130	
	131	
	132	
	133	
	134	
	135	
	136	
	137	
	138	
	139	
	140	
	141	
	142	
	143	
	144	
	145	
	146	
	147	
	148	
	149	
	150	

Search Notes

Application/Control No.	Applicant(s)/Patent under Reexamination	
10/490,932	VAARALA ET AL.	
Examiner	**Art Unit**	
Fikremariam Yalew	2136	

SEARCHED			
Class	Subclass	Date	Examiner
713	161	11/5/2007	FA
380	247	11/15/2007	FA

INTERFERENCE SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES (INCLUDING SEARCH STRATEGY)		
	DATE	EXMR
East(update text and classification search)	11/5/2007	FA
NPL(Google Patent,IEEE)	11/5/2007	FA
Inventor Search	11/5/2007	FA

PTO/SB/30EFS (05/07)
Approved for use through 11/30/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

Application Number	10/490,932	Filing Date	2004-11-22	Docket Number (if applicable)	20.1052USN	Art Unit	2136
First Named Inventor	Sami Vaarala			Examiner Name	Fikremariam A. Yalew		

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

Signature of Registered U.S. Patent Practitioner			
Signature	/rfasth/	Date (YYYY-MM-DD)	2008-01-03
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 record s.

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.

Attorney Docket No. 290.1052USN PATENT

RF:ss 1/3/08

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Sami Vaarala,
Antti Nuopponen

EXPEDITED PROCEDURE UNDER 37 CFR 1.114

Art Unit 2136
Confirmation No. 2427

Serial No. 10/490,932

Filed: 22 November 2004

For: METHOD AND NETWORK FOR ENSURING SECURE FORWARDING OF MESSAGES

Examiner: Fikremariam A. Yalew

Date: 3 January 2008

CERTIFICATE OF MAILING

I HEREBY CERTIFY THAT THIS PAPER AND THE DOCUMENTS REFERRED TO AS BEING ATTACHED OR ENCLOSED HEREWITH ARE BEING SUBMITTED ELECTRONICALLY TO THE UNITED STATES PATENT AND TRADEMARK OFFICE ON **3 January 2008**.

/rfasth/

Rolf Fasth
Attorney for Applicant

TRANSMITTAL LETTER

ELECTRONIC SUBMISSION

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

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

(X) Response to Final Office Action dated 7 November 2007.
(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. 290.1052USN

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:	10490932
Filing Date:	22-Nov-2004
Title of Invention:	Method and nework for ensuring secure forwarding of messages
First Named Inventor/Applicant Name:	Sami Vaarala
Filer:	Rolf Fasth/Sloan Smith
Attorney Docket Number:	290.1052USN
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:	2664322
Application Number:	10490932
International Application Number:	
Confirmation Number:	2427
Title of Invention:	Method and nework for ensuring secure forwarding of messages
First Named Inventor/Applicant Name:	Sami Vaarala
Customer Number:	33369
Filer:	Rolf Fasth/Sloan Smith
Filer Authorized By:	Rolf Fasth
Attorney Docket Number:	290.1052USN
Receipt Date:	03-JAN-2008
Filing Date:	22-NOV-2004
Time Stamp:	11:47:12
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	5851
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 CFR 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	38268 1cd4935c437a3698c82e58c5e14b65f4 03c7b36b	yes	14
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Amendment Submitted/Entered with Filing of CPA/RCE		1	1	
	Claims		2	3	
	Applicant Arguments/Remarks Made in an Amendment		4	14	
Warnings:					
Information:					
2	Request for Continued Examination (RCE)	RCE.PDF	718155 0643097ad07e9853c09b613c476791751469645i	no	3
Warnings:					
Information:					
3	Miscellaneous Incoming Letter	TRX.PDF	19210 23b19ebe9eb0518707038ba7583b365aac9a0819	no	1
Warnings:					
Information:					
4	Fee Worksheet (PTO-06)	fee-info.pdf	8190 3983a178d6575ebe2873a8c16c010eea5a7c9035	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	783823		

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 2136

Sami Vaarala, Antti Nuopponen

Serial No. 10/490,932

Filed: 22 November 2004

For: METHOD AND NETWORK FOR ENSURING SECURE FORWARDING OF MESSAGES

Examiner: Yalew, Fikremariam A

Date: 3 January 2008

ATTORNEY DOCKET NO. 290.1052USN

AMENDMENT

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

This is in response to the Office action of 7 November, 2007. Please amend the above-identified patent application as follows:

In the Claims:

Amend the claims as follows:

1. (Currently amended) A method for ensuring secure forwarding of a message in a telecommunication network, having at least one mobile terminal and another terminal, the method comprising:
a) establishing a secure connection between a first address of the mobile terminal and a first address of the other terminal, the secure connection defined by at least the addresses of the two terminals,
b) the mobile terminal moving from the first address of the mobile terminal to a second address, and
c) while at the second address, the mobile terminal sending a request message to the first address of the other terminal to request the other terminal to change the previously established secure connection to be defined between the second address and the first address of the other terminal, and
the other terminal, while at the first address of the other terminal, changing an address definition of the previously established secure connection from the first address to the second address.

2. (Previously presented) The method of claim 1, wherein the secure connection is established in step a) by forming a Security Association (SA) using IPSec protocols.

3. (Previously presented) The method of claim 1, wherein in step c) a reply back to the mobile terminal is sent from the other terminal after the request from the mobile terminal to change the address.

4. (Previously presented) The method of claim 1, wherein the

registration request and/or the reply message is encrypted and/or authenticated by using the same SA already established.

5. (Previously presented) The method of claim 1, wherein the change of addresses in the secure connection as a result of the request message is performed by means of a central register of current address of the terminals belonging to the network.

6. (Previously presented) The method of claim 1 wherein the method further comprises the other terminal sending back a reply message to the mobile terminal at the second address to confirm the address change.

7. (Previously presented) The method of claim 6, wherein the mobile terminal and the other terminal forms an end-to-end connection whereby the secure connection is an IPSec transport connection or IPSec tunnel connection.

8. (Previously presented) The method of claim 6, wherein one of or both of the mobile terminal and the other terminal is a security gateway protecting one or more computers, whereby IPSec tunnel mode or IPSec together with a tunneling protocol is used for the secure connection between the mobile terminal and the other terminal.

9. (Previously presented) The method of claim 6, wherein both terminals are mobile terminals.

10. (Previously presented) The method of claim 9, wherein the method further comprises providing a central register of current locations of the terminals belonging to the network.

REMARKS

Reconsideration of the application is respectfully requested. Claims 1-10 were rejected under Section 103 as being anticipated by Ala-Laurila (US Patent No. 6,587,680) in view of Makineni (US Patent Application No. 200020066036). This rejection is respectfully traversed.

To summarize the method of the present invention, it is an effective method and network for ensuring secure forwarding of a message as a mobile terminal moves from a first address to a second address in the same existing secure connection (without the need for setting up a new secure connection). Thus, the same already existing secure connection is merely changed to be between the second address of the mobile terminal and the address of the other terminal as a result of an address change request from the mobile terminal. Since the same secure connection is used, the address change may be done without the need for the cumbersome and time consuming exchange of security keys (IKE negotiations) typically required to set up a new security association.

Claim 1 has been amended to further clarify that the already existing or previously established secure connection is used even after the mobile terminal has moved from the first address to the second address. No new matter has been added to claim 1. For example, paragraphs [0091, 0120 and 0121] explain that the same existing secure connection is used

and there is no need to re-establish the secure connection after the mobile terminal has moved to the new second address.

Ala-Laurila merely discloses a conventional system for transferring a security association during a mobile terminal handover. This means the mobile terminal is moved from a first address to a second adress and a new access point is established between the mobile-terminal at the second address that belongs to a new coverage area of the new access point. Ala-Laurila's system requires a change of the location of both the mobile terminal and the access points. Additionally, the original access point is not really used by the mobile terminal while at the second address.

In col. 5, lines 37-42, Ala-Laurila explains that a challenge/response procedure is used to authenticate a mobile terminal during a handover event. The new AP (access point), not the mobile terminal, sends a challenge to the mobile terminal and the mobile terminal responds by sending a response. In col. 5, lines 51-58, Ala-Laurila explains that the new AP requests the keys and other information that is transferred from the old AP to the new AP (so that all such communication is between the two APs and not between the old AP and the mobile terminal). More importantly, the mobile terminal in Ala-Laurila's system does not send a request to the old AP to request the old AP to change the address from the first address to the second address in the security association.

In col. 8, lines 49-61, Ala-Laurila describes the procedure for a backward handover where the handover is requested by the mobile terminal in communication with the old AP. A radio interface message 31 carries the authentication challenge from old AP to the mobile terminal to trigger the backward handover. The authentication challenge is used to indicate to the mobile terminal to disconnect from the old AP and connect to the new AP whereat a security association has already been prepared for the mobile terminal.

This means the mobile terminal never sends a request to the old AP to change the security association to be defined the second address and the original address of the old AP, as required by the amended claim 1.

It is submitted that it would not make sense for the mobile terminal to send such a request to the old AP since the mobile terminal has been instructed to disconnect from the old AP and since the new security association has been set up between the new AP and the mobile terminal at the second address without any real participation by the mobile terminal. When the mobile terminal connects to the new AP, the security association has already been set up for the mobile terminal.

In col. 10, lines 32 to col. 11, line 8, Ala-Laurila explains that when the handover request is sent from the mobile terminal to the old AP, the message is received by the old AP. (It is here question about a backward handover, wherein the mobile terminal changes back from a "new" AP to an

"old" AP.) The old AP then retrieves the security association from its database and sends a handover request that contains the SA parameters to the new AP (lines 47-49). In other words, there is no communication between the mobile terminal and the "new" AP, from which the mobile terminal moved. More importantly, the old AP does not change the definition of the secure connection to be between the second address of the mobile terminal and the original address of the old AP. In contrast, the new AP in Ala's system then creates the new security association and generates a challenge to authenticate the mobile terminal and the handover request is sent to the old AP. The old AP then sends a disassociate message to the mobile terminal (lines 59-60). The mobile terminal updates its security association parameters to include the new AP and sends a challenge to authenticate the new AP. It is important to note that Ala-Laurila requires the set up of a new security association and the mobile terminal never requests the old AP to change the addresses in the security association.

It is submitted that it would not be obvious to modify Ala-Laurila to include the steps required of the amended claim 1. For example, the first terminal in Ala-Laurila's system could not send the request to the first address of the second terminal i.e. the old AP, since the mobile terminal has been disassociated from the old AP when the mobile terminal is at the second address. It is submitted that Ala-Laurila's system would not be operational if the

mobile terminal tried to send the request to the original address of the old AP while the mobile terminal is at the second address.

In summary, Ala-Laurila requires the set up of a new security association for the second address of the mobile terminal and the mobile terminal never sends a request message to the old AP to change the secure connection to be defined between the second address of the mobile terminal and the original first address of the old AP. In contrast, in Ala-Laurila's system the old AP sends this request to the new AP, as described in col. 10, lines 43-49. Also, Ala-Laurila's old AP never changes any address definition in the original secure connection. In contrast, the new AP (not the old AP), at the new second address, creates the new security association between the new AP and the second address of the mobile terminal, as explained in col. 10, lines 50-52.

As correctly stated on page 3 of the Office action, Ala-Laurila fails to teach the entire step c) of the amended claim 1. It is then asserted that Makineni cures this deficiency. Applicants respectfully disagree.

Makineni merely describes a non-secure communication between the roaming client 24 and the home server 14. In paragraph [0028] Makineni explains that in the co-located mode all the functions performed by the relay server 22 are performed by the client 24 itself. This means that the client 24 in step 104 encapsulates the registration message and sends

it to the home server 14. In step 106, the home server 14 transmits a reply message to the client 24 confirming the registration of the new IP address as part of the conventional IKE exchange. By the way, the steps described in Makineni is almost identical to the standardized mobile IP registration procedure described in standard RFC 2002 mentioned in the current application. Only after the IKE exchange is completed is a secure association established in step 107 between the client 24 and the home server 14. This is an important point because the secure association is established AFTER the registration and confirmation of the new IP address. In other words, a previously established or pre-existing secure association is not used after the new IP address is registered. A new secure association is thus always formed after the roaming client has moved to a new address.

As indicated above, an important feature of the present invention is that no new secure connection is formed after the mobile terminal has moved from the first address to the second address. The same pre-existing secure connection, that was previously established while the mobile terminal was at the first address, is used also after the mobile terminal has moved to the second address. In other words, the existing secure connection of the present invention is merely modified in such a way that the same existing secure connection works even when the mobile terminal has moved from the first address to the second address without the need for setting up a new

secure connection (that would require the cumbersome IKE exchange).

It is submitted that even if Ala-Laurila is modified to include the cited features of Makineni, although this is not taught or suggested, all the limitations of the amended claim 1 are not met. The cited references still fail to teach or suggest:

1) While at the second address, the mobile terminal sending a request message to the first address of the other terminal to change the previously established secure connection to be defined between the second address of the mobile terminal and the first address of the other terminal, and

2) The other terminal, at the first address of the other terminal, changing an address definition of the previously established secure connection from the first address of the mobile terminal to the second address of the mobile terminal.

As stated above, Makineni only requests the address change while the communication is non-secure and the security association is only established after the IKE exchange is completed.

It is submitted that the required modifications of Makineni is not obvious because there is no motivation to modify Makineni to establish a secure connection prior to changing the IP address. It has long been held that for a

modification to be obvious, Ala-Laurila, Makineni and the other cited references must explicitly teach or suggest the required step to motivate the artisan to make the required modifications. In re Fine 5 USPQ.2d (Fed. Cir. 1988), the court ruled (on page 1944) that there must be a motivation for the required modification to be obvious. In Winner International Royalty Corp. v. Wing 48 USPQ.2d 1139, the court ruled (on page 1144) that there must have been some explicit teaching or suggestion in the art to motivate one of ordinary skill in the art to make the required modifications.

Applicants submit that the cited references completely lack the required teaching or suggestion to motivate the artisan to make the required modifications to Makineni's invention. In other words, it would not be obvious for an artisan to learn about the step of establishing the secure connection between the mobile terminal and the home server while the client (as described in paragraph [0026]) is operating within its home network 12. There is really no need for the secure connection while the client is within the home network 12 and to require the lengthy IKE negotiation while operating in the home network would make Makineni's system more cumbersome and less effective. Therefore, only after the client has roamed outside of its home network 12 and after the IKE exchange is completed requires Makineni the establishment of the security association (SA) and encrypted tunnel 20 (step 107).

Additionally, even if Makineni is incorporated into Ala-Laurila a system that is distinctly different from the present invention would be derived. Ala-Laurila teaches changing both the end-points and the position of the mobile phone so that a new security connection must always be set up. Similarly, Makineni requires the step of establishing a new security association after the IKE exchange (in a non-secure environment) is completed. In other words, both cited references teach the requirement of establishing a new security connection after the mobile terminal has moved to the second address.

Applicants fail to see why an artisan would look to Ala-Laurila and Makineni to learn about establishing the secure connection prior to reporting the address change and then continue using the existing previously established security connection after the address change when:

a) both Ala-Laurila and Makineni completely fails to teach or suggest this feature;

b) there is no motivation to make the required modifications of Makineni and

c) both reference teaches the requirement of setting up a new security connection after the registration of the address change.

In other words, the combination of Ala-Laurila and Makineni would merely teach a system that requires the set up of a new security connection after the registration of the

address change which is distinctly different from the method of the present invention, as outlined in the amended claim 1.

As described in the current application, the setting up of a new security connection may require 6-9 messages (IKE negotiations) and the fact that the current invention has eliminated this requirement is a very advantageous feature that is not taught or suggested in the cited references.

In view of the above, it is submitted that the amended claim 1 is allowable.

Claims 2-10 are submitted to be allowable because the claims depend upon the allowable base claim 1 and because each claim includes limitations that are not taught or suggested in the cited references.

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

Respectfully submitted,

FASTH LAW OFFICES

/rfasth/
Rolf Fasth
Registration No. 36,999

ATTORNEY DOCKET NO. 290.1052USN

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

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

cc: Lisbeth Soderman, IprBox
(Your ref: S00051US)

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
10/490,932	11/22/2004	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☒ RATE ($)	SMALL ENTITY ☒ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	01/03/2008	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 10	Minus	** 20	= 0	X $25 =	0	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 1	Minus	***3	= 0	X $105 =	0	OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

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

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

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

Legal Instrument Examiner:
SHEILA D. CHAPMAN

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.
10/490,932	11/22/2004	Sami Vaarala	290.1052USN	2427

33369 7590 03/17/2008
FASTH LAW OFFICES (ROLF FASTH)
26 PINECREST PLAZA, SUITE 2
SOUTHERN PINES, NC 28387-4301

EXAMINER	
YALEW, FIKREMARIAM A	
ART UNIT	PAPER NUMBER
2136	
MAIL DATE	DELIVERY MODE
03/17/2008	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.	Applicant(s)	
	10/490,932	VAARALA ET AL.	
	Examiner	Art Unit	
	Fikremariam Yalew	2136	

-- 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 *03 January 2008*.

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) *1-10* 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) *1-10* is/are rejected.

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

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

Application Papers

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

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

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

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

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

Priority under 35 U.S.C. § 119

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

a)☐ All b)☐ Some * c)☐ None of:

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

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

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

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

Attachment(s)

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

DETAILED ACTION

1. 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 01/03/2008 has been entered.

2. The office action is in replay to an amendment filed on 01/03/2008. Claim 1 has been amended. Claims 1-10 are pending.

Response to Arguments

3. Applicant's arguments with respect to claim 1-10 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

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

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

5. Claims 1-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ala-Laurila et al (hereinafter referred as Ala) US Patent No 6,587,680 B1 in view of Aura et al(hereinafter referred as Aura) US Pub No 2003/0166397.

6. As per claim 1: Ala discloses a method for ensuring secure forwarding of a message in a telecommunication network, having at least one mobile terminal and another terminal, the method comprising:

a) establishing a secure connection between a first address of the mobile terminal and the other terminal and first address of the other terminal, the secure connection defined by at least the addresses of the two terminals(col 8 lines 1-22 and Fig 2),

b) the mobile terminal moving from the first address of the mobile terminal to a second address(See col 8 lines 6-9 and Fig 2)

Ala does not explicitly teach c) while at the second address, the mobile terminal sending a request message to the first address of the other terminal to request the other terminal to change the secure connection to be defined between the second address and the first address of the other terminal, and the other terminal, while at the first address of the other terminal, changing and address definition of the other terminal, changing and address definition of the secure connection from the first address to the second address.

However Aura discloses c) while at the second address, the mobile terminal sending a request message to the first address of the other terminal to request the other terminal to change the previously established secure connection to be defined between the second address and the first address of the other terminal, and the other terminal, while at the first address of the other terminal, changing and address definition of the other terminal, changing and address definition of the previously established secure connection from the first address to the second address(See 0039,0041).

Therefore it would have been obvious to one having ordinary skill in the art at that time the invention was made to modify the teaching method of Aura within Ala method inorder to provide authentication and access to reduce the service latency when a mobile unit moves between a first base station and a second base station. (See Aura 0010).

7. As per claim 2: the combination of Ala and Aura disclose the method wherein, the secure connection is established in step a) by forming a Security Association (SA) using the IPSec protocols (See Ala col 5 lines 27-36 and Fig 2).

8. As per claim 3: the combination of Ala and Aura disclose the method wherein that in step c) a reply back to the mobile terminal is sent from the other terminal after the request from the mobile terminal to change the address (See Ala Fig 2 and col 5 lines 43-50).

9. As per claim 4: the combination of Ala and Aura disclose the method wherein the registration request and/or the reply message is encrypted and/or authenticated by using the same SA already established (See Ala col 8 lines 1-22 and Fig 2).

10. As per claim 5: the combination of Ala and Aura disclose the method wherein the change of addresses in the secure connection as a result of the request message is performed by means of a central register of current address of the terminals belonging to the network (See Ala col 8 lines 17-22).

11. As per claim 6: the combination of Ala and Aura disclose the method wherein the method further comprises the other terminal sending back a replay message to the mobile terminal at the second address to confirm address change(See Aura See 0039,0041).

12. As per claim 7: the combination of Ala and Aura disclose the method wherein the mobile terminal and the other terminal forms an end-to-end connection whereby the secure connection is an IPSec transport connection or IPSec tunnel connection (See Ala Fig 2 IPsec tunneling, SA Parameter).

13. As per claim 8: the combination of Ala and Aura disclose the method wherein one of or both of the mobile terminal and the other terminal is a security gateway protecting one or more computers, whereby IPSec tunnel mode or IPSec together with a tunneling protocol is used for the secure connection between the mobile terminal and the other terminal (See Ala Fig2 IPsec tunneling, SA Parameter).

14. As per claim 9: the combination of Ala and Aura disclose the method wherein both terminals are mobile terminals (See Ala col 8 lines 17-22 and Fig 2).

15. As per claim 10: the combination of Ala and Aura disclose the method further comprises providing a central register of current locations of the terminals belonging to the network (See Ala col 7 lines 46-67).

Conclusion

16. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO 892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fikremariam Yalew whose telephone number is 5712723852. The examiner can normally be reached on 9-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Fikremariam Yalew Art Unit 2136
03/10/2007
FA

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136

Notice of References Cited	Application/Control No. 10/490,932	Applicant(s)/Patent Under Reexamination VAARALA ET AL.	
	Examiner Fikremariam Yalew	Art Unit 2136	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,587,680	07-2003	Ala-Laurila et al.	455/411
*	B	US-2003/0166397	09-2003	Aura, Anssi Tuomas	455/410
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	8	IPsec near (mobile or telecommunicat$3) with terminal	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/03/07 15:35
S2	666	(re$autenticat$3 or re $establish$3)with connect$3 same mobil $3	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/03/07 15:40
S3	273	S2 and (IPSEC or SSL or secur$3)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/03/07 15:41
S5	13	S3 and "726"/$.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/03/07 15:41
S6	61	S3 and "709"/$.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/03/07 15:42
S7	8	S3 and "380"/$.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/03/07 15:42
S8	666	(re$autenticat$3 or re $establish$3)with connect$3 same mobil $3	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/03/07 18:10

S9	273	S8 and (IPSEC or SSL or secur$3)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/03/07 18:10
S10	14	S9 and "713"/$.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/03/07 18:10
S11	3	"20020066036"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/03/10 14:47

3/ 10/ 2008 6:23:17 PM
C:\ Documents and Settings\ fyalew\ My Documents\ EAST\ Workspaces\ 10490932.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10490932	VAARALA ET AL.
	Examiner	Art Unit
	Fikremariam Yalew	2136

SEARCHED

Class	Subclass	Date	Examiner
713	161	03/09/2008	FA
380	247 Limited including with text search	03/09/2008	FA

SEARCH NOTES

Search Notes	Date	Examiner
Updated East search,NPL searc,Inventor searchh	03/09/2008	FA

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

Application Number	Application/Control No.	Applicant(s)/Patent under Reexamination	
	10/490,932	VAARALA ET AL.	
	Examiner	Art Unit	
	Fikremariam Yalew	2136	

Index of Claims

Application/Control No.	Applicant(s)/Patent under Reexamination
10/490,932	VAARALA ET AL.
Examiner	**Art Unit**
Fikremariam Yalew	2136

√	Rejected	–	(Through numeral) Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

Claim		Date
Final	Original	3/10/08
	1	√
	2	√
	3	√
	4	√
	5	√
	6	√
	7	√
	8	√
	9	√√
	10	√
	11	
	12	
	13	
	14	
	15	
	16	
	17	
	18	
	19	
	20	
	21	
	22	
	23	
	24	
	25	
	26	
	27	
	28	
	29	
	30	
	31	
	32	
	33	
	34	
	35	
	36	
	37	
	38	
	39	
	40	
	41	
	42	
	43	
	44	
	45	
	46	
	47	
	48	
	49	
	50	

Claim		Date
Final	Original	
	51	
	52	
	53	
	54	
	55	
	56	
	57	
	58	
	59	
	60	
	61	
	62	
	63	
	64	
	65	
	66	
	67	
	68	
	69	
	70	
	71	
	72	
	73	
	74	
	75	
	76	
	77	
	78	
	79	
	80	
	81	
	82	
	83	
	84	
	85	
	86	
	87	
	88	
	89	
	90	
	91	
	92	
	93	
	94	
	95	
	96	
	97	
	98	
	99	
	100	

Claim		Date
Final	Original	
	101	
	102	
	103	
	104	
	105	
	106	
	107	
	108	
	109	
	110	
	111	
	112	
	113	
	114	
	115	
	116	
	117	
	118	
	119	
	120	
	121	
	122	
	123	
	124	
	125	
	126	
	127	
	128	
	129	
	130	
	131	
	132	
	133	
	134	
	135	
	136	
	137	
	138	
	139	
	140	
	141	
	142	
	143	
	144	
	145	
	146	
	147	
	148	
	149	
	150	

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of Art Unit 2136

Sami Vaarala, Antti Nuopponen

Serial No. 10/490,932

Filed: 22 November 2004

For: METHOD AND NETWORK FOR ENSURING SECURE FORWARDING OF MESSAGES

Examiner: Yalew, Fikremariam A

Date: 30 April 2008

ATTORNEY DOCKET NO. 290.1052USN

AMENDMENT

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

This is in response to the Office action of 17 March, 2008. Please amend the above-identified patent application as follows:

In the Claims:

Amend the claims as follows:

1. (Previously presented) A method for ensuring secure forwarding of a message in a telecommunication network, having at least one mobile terminal and another terminal, the method comprising:
a) establishing a secure connection between a first address of the mobile terminal and a first address of the other terminal, the secure connection defined by at least the addresses of the two terminals,
b) the mobile terminal moving from the first address of the mobile terminal to a second address, and
c) while at the second address, the mobile terminal sending a request message to the first address of the other terminal to request the other terminal to change the secure connection to be defined between the second address and the first address of the other terminal, and
the other terminal, while at the first address of the other terminal, changing an address definition of the secure connection from the first address to the second address.

2. (Previously presented) The method of claim 1, wherein the secure connection is established in step a) by forming a Security Association (SA) using IPSec protocols.

3. (Previously presented) The method of claim 1, wherein in step c) a reply back to the mobile terminal is sent from the other terminal after the request from the mobile terminal to change the address.

4. (Previously presented) The method of claim 1, wherein the registration request and/or the reply message is encrypted

and/or authenticated by using the same SA already established.

5. (Previously presented) The method of claim 1, wherein the change of addresses in the secure connection as a result of the request message is performed by means of a central register of current address of the terminals belonging to the network.

6. (Previously presented) The method of claim 1 wherein the method further comprises the other terminal sending back a reply message to the mobile terminal at the second address to confirm the address change.

7. (Previously presented) The method of claim 6, wherein the mobile terminal and the other terminal forms an end-to-end connection whereby the secure connection is an IPSec transport connection or IPSec tunnel connection.

8. (Previously presented) The method of claim 6, wherein one of or both of the mobile terminal and the other terminal is a security gateway protecting one or more computers, whereby IPSec tunnel mode or IPSec together with a tunneling protocol is used for the secure connection between the mobile terminal and the other terminal.

9. (Previously presented) The method of claim 6, wherein both terminals are mobile terminals.

10. (Previously presented) The method of claim 9, wherein the method further comprises providing a central register of current locations of the terminals belonging to the network.

REMARKS

Reconsideration of the application is respectfully requested. Claims 1-10 were rejected under Section 103 as being obvious over Ala-Laurila in view of Aura.

Aura (US Publication Number 2003/0166397) was filed 4 March 2002. The current application is based on PCT/FI02/00770 that was filed on 27 September 2002 and claims priority from Finnish Patent Application No. 20011910, filed 28 Sept. 2001. Attached is a copy of the combined declaration that confirms that the priority back to 28 September 2001 was claimed. PCT/FI02/00770 was filed within 12 months from the filing date of the corresponding Finnish priority Patent Application. Applicants are therefore entitled to the priority filing date of 28 September 2001 which is clearly before the filing date (4 March 2002) of the cited Aura reference. It is therefore submitted that Aura is not a prior art document.

Therefore, it is submitted that claims 1-10 are allowable over the cited reference and that the obviousness rejection should be withdrawn.

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

Respectfully submitted,

FASTH LAW OFFICES

/rfasth/
Rolf Fasth
Registration No. 36,999

ATTORNEY DOCKET NO. 290.1052USN

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

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

cc: Lisbeth Soderman, IprBox
(Your ref: S00051US)

RF 3/28/04 290.1052USN

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 NETWORK FOR ENSURING SECURE FORWARDING OF MESSAGES, the specification of which was filed as International Patent Application No. PCT/FI02/00770, on 27 September 2002.

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
20011910 (Number)	Finland (Country)	28 Sept. 2001 (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:

(not applicable)	(n/a)	(not applicable)
(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.

RF 3/29/04 290.1052USN

Full name of first joint inventor: Sami Vaarala

Inventor's signature Sami Vaarala 10.5.2004
Date

Residence: Helsinki, Finland

Citizenship: Finland

Post Office address: ~~Neljäs Linja 22 A 24~~ SÄTERINRINNE 8 B 37
~~FIN-00530 Helsinki, Finland~~ 02600 ESPOO

Full name of second joint inventor: Antti Nuopponen

Inventor's signature Antti Nuopponen 10.5.2004
Date

Residence: Espoo, Finland

Citizenship: Finland

Post Office address: Kaksoiskiventie 7-9 A 1
FIN-02760 Espoo, Finland

Attorney Docket No. 290.1052USN PATENT
RE:ss 4/30/08

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Sami Vaarala,
Antti Nuopponen

Art Unit 2136
Confirmation No. 2427

Serial No. 10/490,932

Filed: 22 November 2004

For: METHOD AND NETWORK FOR ENSURING SECURE FORWARDING OF MESSAGES

Examiner: Fikremariam A Yalew

Date: 30 April 2008

CERTIFICATE OF MAILING

I HEREBY CERTIFY THAT THIS PAPER AND THE DOCUMENTS REFERRED TO AS BEING ATTACHED OR ENCLOSED HEREWITH ARE BEING SUBMITTED ELECTRONICALLY TO THE UNITED STATES PATENT AND TRADEMARK OFFICE ON **30 April 2008**.

/rfasth/
Rolf Fasth
Attorney for Applicant

TRANSMITTAL LETTER

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

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

(X) Response to Office Action dated 17 March 2008.
(X) Copy of previously submitted Combined Declaration and Power of Attorney.
(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. 290.1052USN

Electronic Acknowledgement Receipt

EFS ID:	3233179
Application Number:	10490932
International Application Number:	
Confirmation Number:	2427
Title of Invention:	Method and nework for ensuring secure forwarding of messages
First Named Inventor/Applicant Name:	Sami Vaarala
Customer Number:	33369
Filer:	Rolf Fasth/Sloan Smith
Filer Authorized By:	Rolf Fasth
Attorney Docket Number:	290.1052USN
Receipt Date:	30-APR-2008
Filing Date:	22-NOV-2004
Time Stamp:	15:16:28
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)
1		AMD.PDF	257377 aaeb98a906232d8e3305e61acf6055ff7c6d5178	yes	8

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment - After Non-Final Rejection	1	1
	Claims	2	3
	Applicant Arguments/Remarks Made in an Amendment	4	5
	Oath or Declaration filed	6	8

Warnings:					
Information:					
2	Miscellaneous Incoming Letter	TRX.PDF	18623 712fdb80aaf9b27850df4cd200badff6987cf27a	no	1
Warnings:					
Information:					
		Total Files Size (in bytes):	276000		

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
10/490,932	11/22/2004	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☒ RATE ($)	SMALL ENTITY ☒ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 04/30/2008	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 10	Minus	** 20	= 0	X $25 =	0	OR	X $ =	
Independent (37 CFR 1.16(h))	* 1	Minus	***3	= 0	X $105 =	0	OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

AMENDMENT	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) 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 $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

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

Legal Instrument Examiner:
/PAMELA v. THERATT/

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of Art Unit 2136

Sami Vaarala, Antti Nuopponen

Serial No. 10/490,932

Filed: 22 November 2004

For: METHOD AND NETWORK FOR ENSURING SECURE FORWARDING OF MESSAGES

Examiner: Yalew, Fikremariam A

Date: 20 May 2008

ATTORNEY DOCKET NO. 290.1052USN

SUPPLEMENTAL AMENDMENT

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

This is in response to the Office action of 17 March, 2008 and a supplement to the amendment filed 30 April 2008. Please amend the above-identified patent application as follows:

In the Claims:

Amend the claims as follows:

1. (Previously presented) A method for ensuring secure forwarding of a message in a telecommunication network, having at least one mobile terminal and another terminal, the method comprising:
a) establishing a secure connection between a first address of the mobile terminal and a first address of the other terminal, the secure connection defined by at least the addresses of the two terminals,
b) the mobile terminal moving from the first address of the mobile terminal to a second address, and
c) while at the second address, the mobile terminal sending a request message to the first address of the other terminal to request the other terminal to change the secure connection to be defined between the second address and the first address of the other terminal, and
the other terminal, while at the first address of the other terminal, changing an address definition of the secure connection from the first address to the second address.

2. (Previously presented) The method of claim 1, wherein the secure connection is established in step a) by forming a Security Association (SA) using IPSec protocols.

3. (Previously presented) The method of claim 1, wherein in step c) a reply back to the mobile terminal is sent from the other terminal after the request from the mobile terminal to change the address.

4. (Previously presented) The method of claim 1, wherein the registration request and/or the reply message is encrypted

and/or authenticated by using the same SA already established.

5. (Previously presented) The method of claim 1, wherein the change of addresses in the secure connection as a result of the request message is performed by means of a central register of current address of the terminals belonging to the network.

6. (Previously presented) The method of claim 1 wherein the method further comprises the other terminal sending back a reply message to the mobile terminal at the second address to confirm the address change.

7. (Previously presented) The method of claim 6, wherein the mobile terminal and the other terminal forms an end-to-end connection whereby the secure connection is an IPSec transport connection or IPSec tunnel connection.

8. (Previously presented) The method of claim 6, wherein one of or both of the mobile terminal and the other terminal is a security gateway protecting one or more computers, whereby IPSec tunnel mode or IPSec together with a tunneling protocol is used for the secure connection between the mobile terminal and the other terminal.

9. (Previously presented) The method of claim 6, wherein both terminals are mobile terminals.

10. (Previously presented) The method of claim 9, wherein the method further comprises providing a central register of current locations of the terminals belonging to the network.

REMARKS

Reconsideration of the application is respectfully requested. Claims 1-10 were rejected under Section 103 as being obvious over Ala-Laurila in view of Aura.

Aura (US Publication Number 2003/0166397) was filed 4 March 2002. The current application is based on PCT/FI02/00770 that was filed on 27 September 2002 and claims priority from Finnish Patent Application No. 20011910, filed 28 Sept. 2001. Attached is a copy of the combined declaration that confirms that the priority back to 28 September 2001 was claimed. PCT/FI02/00770 was filed within 12 months from the filing date of the corresponding Finnish priority Patent Application. Applicants are therefore entitled to the priority filing date of 28 September 2001 which is clearly before the filing date (4 March 2002) of the cited Aura reference. It is therefore submitted that Aura is not a prior art document.

Even if Aura is considered to be prior art, it is submitted that the currently claimed invention is not obvious over Ala-Laurila in view of Aura.

Ala-Laurila merely discloses a conventional system for transferring a security association during a mobile terminal handover. This means the mobile terminal is moved from a first address to a second address and a new access point is established between the mobile-terminal at the second address that belongs to a new coverage area of the new access point. Ala-Laurila's system requires a change of the location of both the mobile terminal and the access points. The original access point is not really used by the mobile terminal while at the second address.

Aura does not cure these deficiencies. Aura is yet another reference that merely discloses a system in which a mobile station changes access point i.e. changes to be served by a new base station. For example, the abstract explains that the mobile node moves between a first base station and a

second base station. Aura is really about a new and easier way of re-authentication when the physical access point is changed. This is completely different from using the same secure connection and changing the address definition of the same secure connection, as required by claim 1. It should be noted that the present invention does not really require the mobile station to physically move from one base station to another base station to trigger the address change. The address change could take place even if the mobile station is stationary but when, for example, the network is changed from a wireless WLAN to a wired Ethernet, while using the same secure connection connected between the same mobile station and the same base station. In contrast, Aura requires that the secure connection is changed to be between the mobile terminal and a new base station.

The Examiner refers to paragraphs 0039, 0041 of Aura that states that the first and second base station may be the same base station at different points in time. A detector module in the mobile node detects that the communication has been terminated due to, for example, electromagnetic interference or shielding, loss of power by either the base station of the mobile node. The mobile station can re-establish its connection with the base station and gain credential authenticated access through the base station without experiencing the delay originating from full authentication.

It is respectfully submitted that this has nothing to do with changing the address definition from a first address to a second address within the same secure connection. It merely describes an easier way to re-authenticate the secure connection that occurs at two different points in time.

Applicants fails to see why a person of ordinary skill in the art would look to Ala-Laurila, Aura and the other cited references to learn about the features of the amended claim 1 when such features are completely missing in the cited

references. All the cited references fail to teach or suggest the step of the mobile terminal, while at the second address, sending a request message to the first address of the other terminal to request the other terminal to change the secure connection to be defined between the second address of the mobile terminal and the first address of the other terminal. As indicated above, Aura merely discloses a way of re-establishing the authentication without experiencing the delay originating from full authentication (see paragraph 0039) which is distinctly different from changing the address from the first address to the second address in the same secure connection.

Even if Ala-Laurila is combined with Aura, although such combination is not taught or suggested by the cited references, all of the limitations of the claims are not satisfied. It is submitted that the cited references fail to teach or suggest:

1) While at the second address, the mobile terminal sending a request message to the first address of the other terminal to change the secure connection to be defined between the second address of the mobile terminal and the first address of the other terminal, and

2) The other terminal, at the first address of the other terminal, changing an address definition of the secure connection from the first address of the mobile terminal to the second address of the mobile terminal.

It is submitted that Ala-Laurila, Aura and the other cited references would require extensive modifications that are not taught or suggested, to meet the requirements of the amended claim 1. It is also submitted that those modifications are not obvious since Ala-Laurila completely fails to teach or suggest the required modifications.

In view of the above, it is submitted that the amended claim 1 is allowable.

Claims 2-10 are submitted to be allowable because

the claims depend upon the allowable base claim 1 and because each claim includes limitations that are not taught or suggested in the cited references.

Therefore, it is submitted that claims 1-10 are allowable over the cited reference and that the obviousness rejection should be withdrawn.

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

Respectfully submitted,

FASTH LAW OFFICES

/rfasth/
Rolf Fasth
Registration No. 36,999

ATTORNEY DOCKET NO. 290.1052USN

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

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

cc: Lisbeth Soderman, IprBox
(Your ref: S00051US)

Attorney Docket No. 290.1052USN PATENT
RF:ss 5/21/08

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Sami Vaarala,
Antti Nuopponen

Art Unit 2136
Confirmation No. 2427

Serial No. 10/490,932

Filed: 22 November 2004

For: METHOD AND NETWORK FOR ENSURING SECURE FORWARDING OF MESSAGES

Examiner: Yalew, Fikremariam A

Date: 21 May 2008

CERTIFICATE OF MAILING

I HEREBY CERTIFY THAT THIS PAPER AND THE DOCUMENTS REFERRED TO AS BEING ATTACHED OR ENCLOSED HEREWITH ARE BEING SUBMITTED ELECTRONICALLY TO THE UNITED STATES PATENT AND TRADEMARK OFFICE ON **21 May 2008**.

/rfasth/

Rolf Fasth
Attorney for Applicant

TRANSMITTAL LETTER

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

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

(X) Response to Office Action dated 17 March 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. 290.1052USN

Electronic Acknowledgement Receipt

EFS ID:	3336157
Application Number:	10490932
International Application Number:	
Confirmation Number:	2427
Title of Invention:	Method and nework for ensuring secure forwarding of messages
First Named Inventor/Applicant Name:	Sami Vaarala
Customer Number:	33369
Filer:	Rolf Fasth/Sloan Smith
Filer Authorized By:	Rolf Fasth
Attorney Docket Number:	290.1052USN
Receipt Date:	21-MAY-2008
Filing Date:	22-NOV-2004
Time Stamp:	14:03:25
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)
1		AMD.PDF	30448 d61fb397e547c1fe0e93d54d148d46cc6d5b2e30	yes	7

	Multipart Description/PDF files in .zip description				
	Document Description	**Start**	**End**		
	Supplemental Response or Supplemental Amendment	1	1		
	Claims	2	3		
	Applicant Arguments/Remarks Made in an Amendment	4	7		
Warnings:					
Information:					
2	Miscellaneous Incoming Letter	TRX.PDF	18353 076a7cc83f4df24fb1f3ba850d5e611b2a177376	no	1
Warnings:					
Information:					
		Total Files Size (in bytes):	48801		

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
10/490,932	11/22/2004	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☒ RATE ($)	SMALL ENTITY ☒ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 05/21/2008	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 10	Minus	** 20	= 0	X $25 =	0	OR	X $ =	
Independent (37 CFR 1.16(h))	* 1	Minus	***3	= 0	X $105 =	0	OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

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

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

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

Legal Instrument Examiner:
/THERESA I. OKON/

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.
10/490,932	11/22/2004	Sami Vaarala	290.1052USN	2427

33369 7590 09/26/2008

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

EXAMINER	
YALEW, FIKREMARIAM A	
ART UNIT	PAPER NUMBER
2136	
MAIL DATE	DELIVERY MODE
09/26/2008	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.	Applicant(s)	
	10/490,932	VAARALA ET AL.	
	Examiner	Art Unit	
	Fikremariam Yalew	2136	

-- 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 *21 May 2008*.

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) *1-10* 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) *1-10* is/are rejected.

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

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

Application Papers

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

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

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

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

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

Priority under 35 U.S.C. § 119

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

a)☐ All b)☐ Some * c)☐ None of:

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

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

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

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

Attachment(s)

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

DETAILED ACTION

1. The office action is in replay to an amendment filed on 05/21/2008. Claims 1-10 are pending.

Response to Arguments

2. Applicant's arguments with respect to claims 1-10 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

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

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

4. Claims 1-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ala-Laurila et al (hereinafter referred as Ala) US Patent No 6,587,680 B1 in view of Ishiyama et al(hereinafter referred as Aura) US Patent No 6,904,466 B1.

5. As per claim 1: Ala discloses a method for ensuring secure forwarding of a message in a telecommunication network, having at least one mobile terminal and another terminal, the method comprising:

a) establishing a secure connection between a first address of the mobile terminal and the other terminal and first address of the other terminal, the secure connection defined by at least the addresses of the two terminals(col 8 lines 1-22 and Fig 2),

b) the mobile terminal moving from the first address of the mobile terminal to a second address(See col 8 lines 6-9 and Fig 2)

Ala does not explicitly teach c) while at the second address, the mobile terminal sending a request message to the first address of the other terminal to request the other terminal to change the secure connection to be defined between the second address and the first address of the other terminal, and the other terminal, while at the first address of the other terminal, changing and address definition of the other terminal, changing and address definition of the secure connection from the first address to the second address.

However Ishiyama discloses c) while at the second address, the mobile terminal sending a request message to the first address of the other terminal to request the other terminal to change the previously established secure connection to be defined between the second address and the first address of the other terminal, and the other terminal, while at the first address of the other terminal, changing and address definition of the other terminal, changing and address definition of the previously established secure connection from the first address to the second address(See col 6 lines 13-23,col 6line 54 through col 7 line 23,col l1 line 29-58).

Therefore it would have been obvious to one having ordinary skill in the art at that time the invention was made to modify the teaching method of Ishiyama within Ala method inorder to providing a sufficient level of security.

6. As per claim 2: the combination of Ala and Ishiyama disclose the method wherein, the secure connection is established in step a) by forming a Security Association (SA) using the IPSec protocols (See Ala col 5 lines 27-36 and Fig 2).

7. As per claim 3: the combination of Ala and Ishiyama disclose the method wherein that in step c) a reply back to the mobile terminal is sent from the other terminal after the request from the mobile terminal to change the address (See Ala Fig 2 and col 5 lines 43-50).

8. As per claim 4: the combination of Ala and Ishiyama disclose the method wherein the registration request and/or the reply message is encrypted and/or authenticated by using the same SA already established (See Ala col 8 lines 1-22 and Fig 2).

9. As per claim 5: the combination of Ala and Ishiyama disclose the method wherein the change of addresses in the secure connection as a result of the request message is performed by means of a central register of current address of the terminals belonging to the network (See Ala col 8 lines 17-22).

10. As per claim 6: the combination of Ala and Ishiyama disclose the method wherein the method further comprises the other terminal sending back a replay message to the mobile terminal at the second address to confirm address change(See Ishiyama col 2 line 63 through col 3 line 14).

11. As per claim 7: the combination of Ala and Ishiyama disclose the method wherein the mobile terminal and the other terminal forms an end-to-end connection whereby the secure connection is an IPSec transport connection or IPSec tunnel connection (See Ala Fig 2 IPsec tunneling, SA Parameter).

12. As per claim 8: the combination of Ala and Ishiyama disclose the method wherein one of or both of the mobile terminal and the other terminal is a security gateway protecting one or more computers, whereby IPSec tunnel mode or IPSec together with a tunneling protocol is used for the secure connection between the mobile terminal and the other terminal (See Ala Fig2 IPsec tunneling, SA Parameter).

13. As per claim 9: the combination of Ala and Ishiyama disclose the method wherein both terminals are mobile terminals (See Ala col 8 lines 17-22 and Fig 2).

14. As per claim 10: the combination of Ala and Ishiyama disclose the method further comprises providing a central register of current locations of the terminals belonging to the network (See Ala col 7 lines 46-67).

Conclusion

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO 892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fikremariam Yalew whose telephone number is 5712723852. The examiner can normally be reached on 9-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Fikremariam Yalew
09/24/2008
FA

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2136

Notice of References Cited	Application/Control No. 10/490,932	Applicant(s)/Patent Under Reexamination VAARALA ET AL.	
	Examiner Fikremariam Yalew	Art Unit 2136	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,587,680	07-2003	Ala-Laurila et al.	455/411
*	B	US-6,904,466	06-2005	Ishiyama et al.	709/245
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10490932	VAARALA ET AL.
	Examiner	Art Unit
	Fikremariam Yalew	2136

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

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

CLAIM		DATE								
Final	Original	09/24/2008								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10490932	VAARALA ET AL.
	Examiner	Art Unit
	Fikremariam Yalew	2136

SEARCHED

Class	Subclass	Date	Examiner
713	161	09/24/2008	FA
380	247 Limited including with text search	09/24/2008	FA

SEARCH NOTES

Search Notes	Date	Examiner
Updated East search,NPL searc,Inventor searchh	09/24/2008	FA

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	66	secure with connection same chang$3 with address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:05
L2	16	L1 and IPsec with protocol	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:05
L3	1	address with change same IPsec with protocol and central with register	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:11
L6	2	L2 and "455"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:12
L7	3	"380"/$.ccls.and L1	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:13
L8	35	((terminal or mobile or cellular with phone) near request)same address with change	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:28
L10	3	L8 and "713"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:29

L12	7	L8 and "455"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:29
L15	24	((current or previous) with address) same IPsec with protocol	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:34
L16	2	"20050083947"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 17:25
L17	1	IPsec same ((RREQ or RREP) with signal$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:03
L18	2	(updat$3 or upgrad$3 or renew$3) same ((single or group) with IPsec with connection)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:07
L19	2	(updat$3 or upgrad$3 or renew$3 or modify $3) same ((single or group) with IPsec with connection)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:09
L20	25	(updat$3 or upgrad$3 or renew$3 or modify $3) and ((single or group) with IPsec with connection)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:35
L21	6	L20 and "713"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:36

L22	5	L20 and "380"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:36
L23	2	L20 and "455"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:36
L24	1	WO-0041427-$.did.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 19:06
L25	0	different with SAs same different with addreess	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 19:21
L26	14	(chang$3 or updat$3 or upgrad$3 or renew $3)near (SA with address or IPSec with address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 19:27

9/ 23/ 2008 7:46:19 PM
C:\ Documents and Settings\ fyalew\ My Documents\ EAST\ Workspaces\ 10490932.wspp.wsp

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of Art Unit 2136

Sami Vaarala, Antti Nuopponen

Serial No. 10/490,932

Filed: 22 November 2004

For: METHOD AND NETWORK FOR ENSURING SECURE FORWARDING OF MESSAGES

Examiner: Yalew, Fikremariam A

Date: 19 December 2008

ATTORNEY DOCKET NO. 290.1052USN

AMENDMENT

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

This is in response to the Office action of 26 September, 2008. Please amend the above-identified patent application as follows:

In the Claims:

Amend the claims as follows:

1. (Currently amended) A method for ensuring secure forwarding of a message in a telecommunication network, having at least one mobile terminal and another terminal and a security gateway therebetween, the method comprising:
a) establishing a secure connection between a first address of the mobile terminal and an ~~first~~ address of the security gateway ~~other terminal~~, the secure connection defined by at least the addresses of the mobile terminal and the security gateway ~~two terminals~~,
b) the mobile terminal changing ~~moving~~ from the first address ~~of the mobile terminal~~ to a second address, and
c) while at the second address, the mobile terminal sending a request message to the ~~first~~ address of the security gateway ~~other terminal~~ to request the security gateway ~~other terminal~~ to change the secure connection to be defined between the second address and the ~~first~~ address of the security gateway ~~other terminal~~, and
in response to the request message from the mobile terminal, the security gateway ~~other terminal, while at the first address of the other terminal,~~ changing an address definition of the secure connection from the first address to the second address, and
the mobile terminal sending a secure message in the secure connection from the second address of the mobile terminal to the other terminal via the security gateway.

2. (Previously presented) The method of claim 1, wherein the secure connection is established in step a) by forming a Security Association (SA) using IPSec protocols.

3. (Currently amended) The method of claim 1, wherein in step c) a reply back to the mobile terminal is sent from the security gateway ~~other terminal~~ after the request from the mobile terminal to change the address.

4. (Currently amended) The method of claim 2 ~~1~~, wherein the ~~registration~~ request message and/or ~~the~~ a reply message is encrypted and/or authenticated by using the same SA already established.

5. (Canceled)

6. (Currently amended) The method of claim 1 wherein the method further comprises the security gateway ~~other terminal~~ sending back a reply message to the mobile terminal at the second address to confirm the address change.

7. (Currently amended) The method of claim 6, wherein the mobile terminal and the other terminal ~~forms~~ form an end-to-end connection whereby the secure connection is an IPSec transport connection or IPSec tunnel connection.

8. (Currently amended) The method of claim 6, wherein ~~one of or both of the mobile terminal and the other terminal is a security gateway protecting one or more computers, whereby IPSec tunnel mode or IPSec together with~~ a tunneling protocol is used for the secure connection between the mobile terminal and the security gateway ~~other terminal~~.

9. (Currently amended) The method of claim 6, wherein the other terminal is a mobile terminal ~~both terminals are mobile terminals~~.

10. (Canceled)

11. (New) A method for ensuring secure forwarding of a message in a telecommunication network, having at least one mobile terminal and another terminal and a security gateway therebetween, the method comprising:

a) establishing a secure connection between a first address of the mobile terminal and an address of the security gateway, the secure connection defined by at least the addresses of the mobile terminal and the security gateway,

b) the mobile terminal moving from the first address to a second address, and

c) while at the second address, the mobile terminal sending a request message to the address of the security gateway to request the security gateway to change the secure connection to be defined between the second address and the address of the security gateway, and

the security gateway changing an address definition of the secure connection from the first address to the second address, and

the other terminal sending a secure message in the secure connection to the second address of the mobile terminal via the security gateway.

REMARKS/ARGUMENTS

Reconsideration of the application is respectfully requested. Claims 1-4 and 6-9 are pending in the present invention. Claims 5 and 10 have been canceled to facilitate the prosecution of the current application. Claim 11 has been added to the application. No new matter has been added to the application in this response.

1. Rejection of Claims 1-10 under 35 USC § 103(a).

Claims 1-10 were rejected under Section 103 as being obvious over Ala-Laurila in view of Ishiyama. This § 103 rejection is respectfully traversed in part and overcome in part as follows:

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

The current amended claim 1 recites, among other method steps, the mobile terminal sending a request message to the address of the security gateway to request the security gateway to change the secure connection to be defined between the second address of the mobile terminal and the address of the security gateway and the mobile terminal sending a secure message in the secure connection from the second address to the other

terminal via the security gateway. Such steps are not taught or suggested in the cited references.

The Examiner states on page 3 of the Office action that Ala fails to teach "..while at the first address of the other terminal, changing an[d] address definition of the other terminal.." Similarly, the Examiner asserts of page 3 of the Office action that Ishiyama teaches "changing an[d] address definition of the other terminal." This may be correct but it is not what the original or the amended claim 1 requires. Claim 1 requires the step of changing the address definition of the secure connection and it is the address of the mobile terminal (not the other terminal) that is changed from the first address to the second address. Claim 1 has never required the change of the address definition of the other terminal.

More importantly, the amended claim 1 now requires sending the request message to the security gateway to request the security gateway to change the address definition of the secure connection from the first address to the second address and the mobile terminal sending a secure message in the secure connection from the second address to the other terminal via the security gateway. None of the cited references teaches these steps. For example, Ishiyama merely teaches an updating of the mobile computer address and there is no teaching or

suggestion of the correspondent being a security gateway for another computer. There is only correspondence between the correspondent and the mobile terminal. In claim 1, Ishiyama teaches that the packet is sent directly to the correspondent. In the abstract and other places in the detailed description, Ishiyama teaches that the use of a home agent (third computer) should be avoided so that the correspondence can be made directly between the end-to-end connection of the mobile terminal and the correspondent.

The cited references are void any discussion of teaching of a security gateway changing the address definition from the first address to the second address of a mobile terminal in response to the request message from the mobile terminal and the mobile terminal sending a secure message in the secure connection from the second address to the other terminal via the security gateway. Ishiyama merely teaches an end-to-end connection between two computers (mobile computer and correspondent). Both references completely fail to teach sending the request message to the security gateway and while at the second address the mobile terminal sending a secure message in the secure connection to the other terminal via the security gateway.

It is submitted that Ala and Ishiyama completely fail to teach or suggest the above-outlined steps. Accordingly, the

combination of the cited references fails to teach, suggest or provide motivation or incentive for this aspect of the invention. Therefore, the rejection of claim 1 under § 103(a) is improper, and should be removed.

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

Even assuming *arguendo* that the requisite method steps of claim 1 are shown by the combination of Ala and Ishiyama, *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.

As provided in M.P.E.P. § 2142, the Supreme Court in *KSR International v. Teleflex Inc.*, 82 USPQ2d 1385, 1396 (2007) specified that the analysis supporting a rejection under 35 U.S.C. § 103 should be made explicit. "[R]ejections on obviousness cannot be sustained with mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *In re Kahn*, 441 F.3dd 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 1 is at the bottom of page 3 of the Office action, which merely asserts it would have been obvious to modify the teaching method of Ishiyama with Ala method in order to "providing a sufficient level of security." (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

perhaps to avoid in many cases, is nonetheless impermissible in making a *prima facie* showing of obviousness.

According to M.P.E.P. 2142, "the examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness." 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 as to claim 1, and any additional remaining claims to the extent they may depend therefrom.

c. Dependent Claims 2-4 and 6-9

Because dependent claims 2-4 and 6-9 depend from the allowable independent claim 1, and as detailed above, their rejection is now moot. However, claims 2-4 and 6-9 also recite additional characteristics that are not found in the cited art.

Accordingly, the rejection of claims 2-4 and 6-9 under §103(a) is improper.

3. New claim 11

New claim 11 has been added. No new matter has been added to

the claim. Claim 11 is submitted to be allowable for reasons similar to the reasons put forth for the allowability of the amended claim 1. More particularly, the cited references are void any discussion of teaching of a security gateway changing the address definition from the first address to the second address and the other terminal sending a secure message in the secure connection to the second address of the mobile terminal via the security gateway.

4. Conclusion

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.

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.

Respectfully submitted,

FASTH LAW OFFICES

/rfasth/
Rolf Fasth
Registration No. 36,999

ATTORNEY DOCKET NO. 290.1052USN

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

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

cc: Lisbeth Soderman, Borenius
(Your ref: S00051US)

Attorney Docket No. 290.1052USN PATENT
RF:ss 12/19/08

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Sami Vaarala, Antti Nuopponen

Art Unit 2136
Confirmation No. 2427

Serial No. 10/490,932

Filed: 22 November 2004

For: METHOD AND NETWORK FOR ENSURING SECURE FORWARDING OF MESSAGES

Examiner: Fikremariam A. Yalew

Date: 19 December 2008

CERTIFICATE OF MAILING

I HEREBY CERTIFY THAT THIS PAPER AND THE DOCUMENTS REFERRED TO AS BEING ATTACHED OR ENCLOSED HEREWITH ARE BEING SUBMITTED ELECTRONICALLY TO THE UNITED STATES PATENT AND TRADEMARK OFFICE ON **19 December 2008**.

/rfasth/
Rolf Fasth
Attorney for Applicant

TRANSMITTAL LETTER

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

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

(X) Response to Office Action dated 26 September 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. 290.1052USN

Electronic Acknowledgement Receipt

EFS ID:	4496098
Application Number:	10490932
International Application Number:	
Confirmation Number:	2427
Title of Invention:	Method and nework for ensuring secure forwarding of messages
First Named Inventor/Applicant Name:	Sami Vaarala
Customer Number:	33369
Filer:	Rolf Fasth/Sloan Smith
Filer Authorized By:	Rolf Fasth
Attorney Docket Number:	290.1052USN
Receipt Date:	19-DEC-2008
Filing Date:	22-NOV-2004
Time Stamp:	18:03:43
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	38355 9c0e85ffcaf7e086df1a7347c927df826c5ba3 8c	yes	12

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	4
	Applicant Arguments/Remarks Made in an Amendment	5	12

Warnings:					
Information:					
2	Miscellaneous Incoming Letter	TRX.PDF	18398 d710980f49e5886f83c9985a9464b063bcd a129	no	1
Warnings:					
Information:					
		Total Files Size (in bytes):	56753		

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
10/490,932	11/22/2004	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☒ RATE ($)	SMALL ENTITY ☒ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	12/19/2008	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 9	Minus	** 20	= 0	X $26 =	0	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $110 =	0	OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

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

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

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

Legal Instrument Examiner:
/TERRY MALLOY ROSS/

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.
10/490,932	11/22/2004	Sami Vaarala	290.1052USN	2427

33369 7590 03/16/2009

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

EXAMINER	
YALEW, FIKREMARIAM A	
ART UNIT	PAPER NUMBER
2436	
MAIL DATE	DELIVERY MODE
03/16/2009	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.

Office Action Summary	Application No.	Applicant(s)	
	10/490,932	VAARALA ET AL.	
	Examiner	Art Unit	
	Fikremariam Yalew	2436	

-- 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 December 2008*.

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) *1-4,6-9 and 11* 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) *1-4,6-9 and 11* is/are rejected.

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

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

Application Papers

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

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

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

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

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

Priority under 35 U.S.C. § 119

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

a)☐ All b)☐ Some * c)☐ None of:

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

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

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

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

Attachment(s)

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

DETAILED ACTION

1. The office action is in replay to an amendment filed on 12/19/2008. Claims 1-4,6-9 and 11 have been amended. Claims 5,10 are canceled and claim 11 is new added. Claims 1-4,6-9,11 are pending.

Response to Arguments

2. Applicant's arguments with respect to claims 1-4,6-9,11 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:
The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 1,11 are rejected under 35 U.S.C 112, first paragraph, as falling to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was failed, had possession of the claimed invention. The specification fails to mention or teach limitation c) while at the second address, the mobile terminal sending a request message to the address of **the security gateway to request the security gateway to change the secure connection to be defined between the second address and the first address of the security gateway and in response to the request message from the mobile terminal changing an address definition of the secure connection from the first address to the second address and the mobile terminal sending a secure message in the secure connection from the second address of the mobile terminal to the**

other terminal via a security gateway as claims 1,11.The applicant should explicitly explain how the specification support the new added claim limitations such as claim limitation C) as recited above.

Claim Rejections - 35 USC § 103

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

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

6. Claims 1-4,6-9,11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ahonen(US Patent No 6,976,177 B2) in view of Luo et al(hereinafter referred as Luo) US Patent No 7,146,428 B2.

5. As per claims 1,11: Ahonen discloses a method for ensuring secure forwarding of a message in a telecommunication network, having at least one mobile terminal and another terminal and a security gateway there between, the method comprising:

a) establishing a secure connection between a first address of the mobile terminal and the other terminal and an address of the security gateway, the secure connection defined by at least the addresses of the mobile terminal and security gateway (See col 2 lines 11-30 and col 3 line 57 through col 4 line 1),

b) the mobile terminal changing from the first address to a second address(See col 9 lines 7-65); the mobile terminal sending a secure message in the secure connection from the second address of the mobile terminal to the other terminal via the security gateway(See Fig 5 and col 2

lines 11-37); and the mobile terminal the security gateway changing an address definition of the secure connection from the first address to the second address(See col 2 lines 11-37 and col 9 lines 7-65).

Ahonnen does not explicitly teach while at the second address, the mobile terminal sending a request message to the first address of the address of the security gateway to request the security gateway to change the secure connection to be defined between the second address and the first address of the security gateway.

However Luo teaches while at the second address, the mobile terminal sending a request message to the first address of the address of the security gateway to request the security gateway to change the secure connection to be defined between the second address and the first address of the security gateway(See col 4 lines 35-67,col 5 lines 18-40 and col 6 lines 40-57) and in response to the request message from the mobile terminal the security gateway changing an address definition of the secure connection from the first address to the second address (See col 4 lines 35-67,col 5 lines 18-40 and col 6 lines 40-57).

Therefore it would have been obvious to one having ordinary skill in the art at that time the invention was made to modify the teaching method of Luo within Ahonen method inorder to provide a secure communication method for allowing a mobile host to communicate with a correspondent host over a VPN via a security gateway (See Ahonen col 1 lines 43-46).

6. As per claim 2: the combination of Ahonen and Luo disclose the method wherein, the secure connection is established in step a) by forming a Security Association (SA) using the IPSec protocols (See Ahonen Fig 5 and col 8 lines 17-59).

7. As per claim 3: the combination of Ahonen and Luo disclose the method wherein that in step c) a reply back to the mobile terminal is sent from the other terminal after the request from the mobile terminal to change the address (See Luo col 4 lines 35-67,col 5 lines 18-40 and col 6 lines 40-57).

8. As per claim 4: the combination of Ahonen and Luo disclose the method wherein the registration request and/or the reply message is encrypted and/or authenticated by using the same SA already established (See Ahonen col 2 lines 11-37 and Fig 5).

9. As per claim 6: the combination of Ahonen and Luo disclose the method wherein the method further comprises the other terminal sending back a replay message to the mobile terminal at the second address to confirm address change(See Luo col 4 lines 35-67,col 5 lines 18-40 and col 6 lines 40-57).

11. As per claim 7: the combination of Ahonen and Luo disclose the method wherein the mobile terminal and the other terminal forms an end-to-end connection whereby the secure connection is an IPSec transport connection or IPSec tunnel connection (See Ahonen Fig 5).

12. As per claim 8: the combination of Ahonen and Luo disclose the method wherein one of or both of the mobile terminal and the other terminal is a security gateway protecting one or more computers, whereby IPSec tunnel mode or IPSec together with a tunneling protocol is used for the secure connection between the mobile terminal and the other terminal (See Ahonen Fig 5).

13. As per claim 9: the combination of Ahonen and Luo disclose the method wherein both terminals are mobile terminals (See Ahonen col 1 lines 43-53).

Conclusion

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

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

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fikremariam Yalew whose telephone number is 5712723852. The examiner can normally be reached on 9-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Fikremariam Yalew
03/11/2009
FA

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436

Notice of References Cited	Application/Control No. 10/490,932	Applicant(s)/Patent Under Reexamination VAARALA ET AL.	
	Examiner Fikremariam Yalew	Art Unit 2436	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,976,177	12-2005	Ahonen, Pasi Matti Kalevi	726/3
*	B	US-7,146,428	12-2006	Luo, Hui	709/237
*	C	US-6,170,057	01-2001	Inoue et al.	713/153
*	D	US-7,174,018	02-2007	Patil et al.	380/258
*	E	US-6,904,466	06-2005	Ishiyama et al.	709/245
*	F	US-6,839,338	01-2005	Amara et al.	370/338
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10490932	VAARALA ET AL.
	Examiner	Art Unit
	Fikremariam Yalew	2436

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

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

CLAIM		DATE								
Final	Original	03/11/2009								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	-								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	-								
	11	✓								

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10490932	VAARALA ET AL.
	Examiner	Art Unit
	Fikremariam Yalew	2436

SEARCHED

Class	Subclass	Date	Examiner
713	161	3/11/2009	FA
380	247 Limited including with text search	3/11/2009	FA

SEARCH NOTES

Search Notes	Date	Examiner
Updated East search,NPL searc,Inventor searchh	3/11/2009	FA

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	124	(security with gateway or firewall or NAT or secure with gatekeeper or secure with router) near (chang$3 or upgrad$3 or renew or updat$3) with (address or mobile with address or location with address or ip with address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/11 11:07
L2	1	L1 and "380"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/11 11:08
L3	9	L1 and "713"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/11 11:08
L4	30	L1 and "726"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/11 11:08
L5	58	L1 and "709"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/11 11:08
L6	17	L5 and IPSEC	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/11 11:08
L7	11	L4 and IPSEC	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/11 11:09

L8	5	L3 and IPSEC	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/11 11:09
L9	2	"6587680".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/11 12:16
L10	2	"6904466".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/11 12:33
S1	66	secure with connection same chang$3 with address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:05
S2	16	S1 and IPsec with protocol	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:05
S3	1	address with change same IPsec with protocol and central with register	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:11
S6	2	S2 and "455"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:12
S7	3	"380"/$.ccls.and S1	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:13

S8	35	((terminal or mobile or cellular with phone) near request) same address with change	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:28
S10	3	S8 and "713"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:29
S12	7	S8 and "455"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:29
S15	24	((current or previous) with address) same IPsec with protocol	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:34
S16	2	"20050083947"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 17:25
S17	1	IPsec same ((RREQ or RREP) with signal$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:03
S18	2	(updat$3 or upgrad$3 or renew$3) same ((single or group) with IPsec with connection)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:07
S19	2	(updat$3 or upgrad$3 or renew$3 or modify$3) same ((single or group) with IPsec with connection)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:09

S20	25	(updat$3 or upgrad$3 or renew$3 or modify$3) and ((single or group) with IPsec with connection)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:35
S21	6	S20 and "713"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:36
S22	5	S20 and "380"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:36
S23	2	S20 and "455"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:36
S24	1	WO-0041427-$.did.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 19:06
S25	0	different with SAs same different with addreess	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 19:21
S26	14	(chang$3 or updat$3 or upgrad$3 or renew$3) near (SA with address or IPSec with address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 19:27
S27	239	(modify$3 or updat$3 or upgrad$3)same (IPSEC or (Security with gateway) or SA) same(request$3 or send$3)with message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/04 18:52

S28	239	(modify$3 or updat$3 or upgrad$3)same (IPSEC or (Security with gateway) or SA or router with IPSEC or firewall with IPSEC) same (request$3 or send$3)with message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/04 18:53
S29	31	S28 and "713"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/04 18:53
S30	9	S28 and "380"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/04 18:53
S31	53	S28 and "709"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/04 18:54
S33	9	S31 and mobility$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/04 18:55
S34	11	S29 and mobility$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/04 18:55
S35	4	S30 and mobility$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/04 18:55
S36	142	(security with gateway or firewall or secure with router)same (moblie with terminal or mobile with device or cellphone or telecommunication with terminal or PDA)same (visit$3 or home)with network	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/10 17:47

S37	9	S36 and "713"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/10 17:48
S38	5	S36 and "380"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/10 17:48
S39	16	S36 and "726"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/10 17:48
S40	39	("5303303" | "5444782" | "5559883" | "5812671" | "5850449" | "5870479" | "5884025" | "5898784").PN. OR ("6170057").URPN.	US-PGPUB; USPAT; USOCR	OR	OFF	2009/03/10 18:02

3/11/2009 3:09:00 PM
C:\Documents and Settings\fyalew\My Documents\EAST\Workspaces\10490932.wspp.wsp

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of Art Unit 2436

Sami Vaarala, Antti Nuopponen

Serial No. 10/490,932

Filed: 22 November 2004

For: METHOD AND NETWORK FOR ENSURING SECURE FORWARDING OF MESSAGES

Examiner: Yalew, Fikremariam A

Date: 30 April 2009

ATTORNEY DOCKET NO. 290.1052USN

AMENDMENT

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

This is in response to the Office action of 16 March, 2009. Please amend the above-identified patent application as follows:

In the Claims:

Amend the claims as follows:

1. (Previously presented) A method for ensuring secure forwarding of a message in a telecommunication network, having at least one mobile terminal and another terminal and a security gateway therebetween, the method comprising:
a) establishing a secure connection between a first address of the mobile terminal and an address of the security gateway, the secure connection defined by at least the addresses of the mobile terminal and the security gateway,
b) the mobile terminal changing from the first address to a second address, and
c) while at the second address, the mobile terminal sending a request message to the address of the security gateway to request the security gateway to change the secure connection to be defined between the second address and the address of the security gateway, and
in response to the request message from the mobile terminal, the security gateway changing an address definition of the secure connection from the first address to the second address, and
the mobile terminal sending a secure message in the secure connection from the second address of the mobile terminal to the other terminal via the security gateway.

2. (Previously presented) The method of claim 1, wherein the secure connection is established in step a) by forming a Security Association (SA) using IPSec protocols.

3. (Previously presented) The method of claim 1, wherein in step c) a reply back to the mobile terminal is sent from the security gateway after the request from the mobile terminal to

change the address.

4. (Previously presented) The method of claim 2, wherein the request message and/or a reply message is encrypted and/or authenticated by using the same SA already established.

5. (Canceled)

6. (Previously presented) The method of claim 1 wherein the method further comprises the security gateway sending back a reply message to the mobile terminal at the second address to confirm the address change.

7. (Previously presented) The method of claim 6, wherein the mobile terminal and the other terminal form an end-to-end connection whereby the secure connection is an IPSec transport connection or IPSec tunnel connection.

8. (Previously presented) The method of claim 6, wherein a tunneling protocol is used for the secure connection between the mobile terminal and the security gateway.

9. (Previously presented) The method of claim 6, wherein the other terminal is a mobile terminal.

10. (Canceled)

11. (Original) A method for ensuring secure forwarding of a message in a telecommunication network, having at least one mobile terminal and another terminal and a security gateway therebetween, the method comprising:
a) establishing a secure connection between a first address of the mobile terminal and an address of the security gateway, the secure connection defined by at least the addresses of the mobile terminal and the security gateway,

b) the mobile terminal moving from the first address to a second address, and

c) while at the second address, the mobile terminal sending a request message to the address of the security gateway to request the security gateway to change the secure connection to be defined between the second address and the address of the security gateway, and

the security gateway changing an address definition of the secure connection from the first address to the second address, and

the other terminal sending a secure message in the secure connection to the second address of the mobile terminal via the security gateway.

REMARKS

Reconsideration of the application is respectfully requested. Claims 1 and 11 were rejected under Section 112. It is submitted that support for the amendments can be found on page 11, lines 27-29; page 15, lines 15-16;, page 17, lines 17-24; Claim 3; Figs. 4-5; Fig. 1; page 12, lines 12-14; and page 15, lines 12-20. It is respectfully submitted that claims 1 and 11 should conform to the requirements of Section 112.

Claims 1-4, 6-9 and 11 were rejected under Section 103 as being obvious over Ahonen in view of Luo.

Luo (US Patent No. 7,146,428) was filed 18 Nov. 2002 and claims priority back to US provisional patent application no. 60/339,953, filed 12 December 2001. The current application is based on PCT/FI02/00770 that was filed on 27 September 2002 and claims priority from Finnish Patent Application No. 20011910, filed 28 September 2001. Attached is a copy of the combined declaration that confirms that the priority back to 28 September 2001 was claimed. PCT/FI02/00770 was filed within 12 months from the filing date of the corresponding Finnish priority Patent Application. Applicants are therefore entitled to the priority filing date of 28 September 2001 which is clearly before the filing date of the priority document (12 December 2001) of the cited Luo reference. It is therefore submitted that Luo is not a prior art document.

Therefore, it is submitted that claims 1-4, 6-9 and 11 are allowable over the cited reference and that the obviousness rejection should be withdrawn.

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

Respectfully submitted,

FASTH LAW OFFICES

/rfasth/

Rolf Fasth
Registration No. 36,999

ATTORNEY DOCKET NO. 290.1052USN

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

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

cc: Lisbeth Soderman, Borenius
(Your ref: S00051US)

Attorney Docket No. 290.1052USN PATENT

RF:ss 4/30/09

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Sami Vaarala,
Antti Nuopponen

EXPEDITED PROCEDURE UNDER 37 CFR 1.114

Art Unit 2436
Confirmation No. 2427

Serial No. 10/490,932

Filed: 22 November 2004

For: METHOD AND NETWORK FOR ENSURING SECURE FORWARDING OF MESSAGES

CERTIFICATE OF MAILING

I HEREBY CERTIFY THAT THIS PAPER AND THE DOCUMENTS REFERRED TO AS BEING ATTACHED OR ENCLOSED HEREWITH ARE BEING SUBMITTED ELECTRONICALLY TO THE UNITED STATES PATENT AND TRADEMARK OFFICE ON 30 April 2009.

Examiner: Fikremariam A. Yalew

/rfasth/

Date: 30 April 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 16 March 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

Attorney Docket No. 290.1052USN

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

Electronic Acknowledgement Receipt

EFS ID:	5249266
Application Number:	10490932
International Application Number:	
Confirmation Number:	2427
Title of Invention:	Method and nework for ensuring secure forwarding of messages
First Named Inventor/Applicant Name:	Sami Vaarala
Customer Number:	33369
Filer:	Rolf Fasth/Sloan Smith
Filer Authorized By:	Rolf Fasth
Attorney Docket Number:	290.1052USN
Receipt Date:	30-APR-2009
Filing Date:	22-NOV-2004
Time Stamp:	12:26:21
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	28530 5280d096789a45f9f0754ad2709f52676feb4026	yes	6

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment After Final	1	1
	Claims	2	4
	Applicant Arguments/Remarks Made in an Amendment	5	6

Warnings:					
Information:					
2	Miscellaneous Incoming Letter	TRX.PDF	18540 8e9b1661 1a25e1b4a10a72424f5732f91735bf667	no	1
Warnings:					
Information:					
		Total Files Size (in bytes):	47070		

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
10/490,932	11/22/2004	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☒ RATE ($)	SMALL ENTITY ☒ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 04/30/2009	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 9	Minus	** 20	= 0	X $26 =	0	OR	X $ =	
Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $110 =	0	OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

AMENDMENT	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) 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 $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

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

Legal Instrument Examiner:
/Fennell A. Pearlie/

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.
10/490,932	11/22/2004	Sami Vaarala	290.1052USN	2427

33369 7590 05/12/2009
FASTH LAW OFFICES (ROLF FASTH)
26 PINECREST PLAZA, SUITE 2
SOUTHERN PINES, NC 28387-4301

EXAMINER	
YALEW, FIKREMARIAM A	
ART UNIT	PAPER NUMBER
2436	
MAIL DATE	DELIVERY MODE
05/12/2009	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.

Office Action Summary	Application No.	Applicant(s)	
	10/490,932	VAARALA ET AL.	
	Examiner	Art Unit	
	Fikremariam Yalew	2436	

-- 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 *30 April 2009*.

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

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

Disposition of Claims

4)☒ Claim(s) *1-4,6-9 and 11* 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) *1-4,6-9,11* is/are rejected.

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

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

Application Papers

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

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

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

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

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

Priority under 35 U.S.C. § 119

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

a)☐ All b)☐ Some * c)☐ None of:

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

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

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

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

Attachment(s)

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

DETAILED ACTION

1. The office action is in replay to an amendment filed on 04/30/2009. Claims 1-4, 6-9,11 are pending.

2. The examiner agree with the applicant's argument that the prior art (Luo reference) filing date is not good to use it as a prior art therefore the examiner withdraws the previous final rejection and reopen the case. Also the examiner withdraws the previous 35 USC 112 first rejection based on the applicant's persuasive argument.

Claim Rejections - 35 USC § 103

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

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

4. Claims 1-4, 6-9,11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ahonen(US Patent No 6,976,177 B2) in view of Inoue et al(hereinafter referred as Inoue) US Patent No 6,170,057 B1.

5. As per claims 1,11: Ahonen discloses a method for ensuring secure forwarding of a message in a telecommunication network, having at least one mobile terminal and another terminal and a security gateway there between, the method comprising:

a) establishing a secure connection between a first address of the mobile terminal and the other terminal and an address of the security gateway, the secure connection defined by at least

the addresses of the mobile terminal and security gateway (See col. 2 lines 11-30 and col. 3 line 57 through col. 4 line 1),

b) the mobile terminal changing from the first address to a second address(See col. 9 lines 7-65); the mobile terminal sending a secure message in the secure connection from the second address of the mobile terminal to the other terminal via the security gateway(See Fig 5 and col. 2 lines 11-37); and the mobile terminal the security gateway changing an address definition of the secure connection from the first address to the second address(See col. 2 lines 11-37 and col. 9 lines 7-65).

Ahonnen does not explicitly teach while at the second address, the mobile terminal sending a request message to the first address of the address of the security gateway to request the security gateway to change the secure connection to be defined between the second address and the first address of the security gateway.

However Inoue teaches while at the second address, the mobile terminal sending a request message to the first address of the address of the security gateway to request the security gateway to change the secure connection to be defined between the second address and the first address of the security gateway(See col.6 lines 2-67 and col.1ines 10-22) and in response to the request message from the mobile terminal the security gateway changing an address definition of the secure connection from the first address to the second address (See col.6 lines 2-67 and col.1ines 10-22).

Therefore it would have been obvious to one having ordinary skill in the art at that time the invention was made to modify the teaching method of Inoue within Ahonen method in order

to provide a secure communication method for allowing a mobile host to communicate with a correspondent host over a VPN via a security gateway (See Ahonen col. 1 lines 43-46).

6. As per claim 2: the combination of Ahonen and Inoue teaches the method wherein, the secure connection is established in step a) by forming a Security Association (SA) using the IPSec protocols (See Ahonen Fig 5 and col. 8 lines 17-59).

7. As per claim 3: the combination of Ahonen and Inoue teaches the method wherein that in step c) a reply back to the mobile terminal is sent from the other terminal after the request from the mobile terminal to change the address (See Inoue col.6 lines 2-67 and col.1ines 10-22).

8. As per claim 4: the combination of Ahonen and Inoue teaches the method wherein the registration request and/or the reply message is encrypted and/or authenticated by using the same SA already established (See Ahonen col. 2 lines 11-37 and Fig 5).

9. As per claim 6: the combination of Ahonen and Inoue teaches the method wherein the method further comprises the other terminal sending back a replay message to the mobile terminal at the second address to confirm address change(See Inoue col.6 lines 2-67 and col.1ines 10-22).

11. As per claim 7: the combination of Ahonen and Inoue teaches the method wherein the mobile terminal and the other terminal forms an end-to-end connection whereby the secure connection is an IPSec transport connection or IPSec tunnel connection (See Ahonen Fig 5).

12. As per claim 8: the combination of Ahonen and Inoue teaches the method wherein one of or both of the mobile terminal and the other terminal is a security gateway protecting one or more computers, whereby IPSec tunnel mode or IPSec together with a tunneling protocol is used

for the secure connection between the mobile terminal and the other terminal (See Ahonen Fig 5).

13. As per claim 9: the combination of Ahonen and Inoue teaches the method wherein both terminals are mobile terminals (See Ahonen col. 1 lines 43-53).

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO 892.

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

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fikremariam Yalew whose telephone number is 5712723852. The examiner can normally be reached on 9-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Fikremariam Yalew/
Examiner, Art Unit 2436
05/11/2009

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436

Notice of References Cited	Application/Control No. 10/490,932	Applicant(s)/Patent Under Reexamination VAARALA ET AL.	
	Examiner Fikremariam Yalew	Art Unit 2436	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,976,177	12-2005	Ahonen, Pasi Matti Kalevi	726/3
*	B	US-6,170,057	01-2001	Inoue et al.	713/153
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

OK TO ENTER: /F.Y./

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of Art Unit 2436

Sami Vaarala, Antti Nuopponen

Serial No. 10/490,932

Filed: 22 November 2004

For: METHOD AND NETWORK FOR ENSURING SECURE FORWARDING OF MESSAGES

Examiner: Yalew, Fikremariam A

Date: 30 April 2009

ATTORNEY DOCKET NO. 290.1052USN

AMENDMENT

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

This is in response to the Office action of 16 March, 2009. Please amend the above-identified patent application as follows:

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L7	11185	secur$4 with connection and gateway	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/05/11 08:40
L8	192	(secur$4 with connection with gateway)(address with change)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2009/05/11 08:41
L9	165	(secur$4 with connection with gateway)(address with change)(security with gateway)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2009/05/11 08:41
L10	12	L9 and (chang$3 or updat $3)with secure with connection	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2009/05/11 08:43
S1	66	secure with connection same chang$3 with address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:05
S2	16	S1 and IPsec with protocol	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:05
S3	1	address with change same IPsec with protocol and central with register	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:11

S6	2	S2 and "455"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:12
S7	3	"380"/$.ccls.and S1	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:13
S8	35	((terminal or mobile or cellular with phone)near request)same address with change	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:28
S10	3	S8 and "713"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:29
S12	7	S8 and "455"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:29
S15	24	((current or previous) with address) same IPsec with protocol	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:34
S16	2	"20050083947"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 17:25
S17	1	IPsec same ((RREQ or RREP) with signal$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:03

S18	2	(updat$3 or upgrad$3 or renew$3) same ((single or group) with IPsec with connection)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:07
S19	2	(updat$3 or upgrad$3 or renew$3 or modify$3) same ((single or group) with IPsec with connection)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:09
S20	25	(updat$3 or upgrad$3 or renew$3 or modify$3) and ((single or group) with IPsec with connection)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:35
S21	6	S20 and "713"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:36
S22	5	S20 and "380"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:36
S23	2	S20 and "455"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:36
S24	1	WO-0041427-$.did.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 19:06
S25	0	different with SAs same different with addreess	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 19:21

S26	14	(chang$3 or updat$3 or upgrad$3 or renew$3) near (SA with address or IPSec with address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 19:27
S27	239	(modify$3 or updat$3 or upgrad$3) same (IPSEC or (Security with gateway) or SA) same(request$3 or send$3)with message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/04 18:52
S28	239	(modify$3 or updat$3 or upgrad$3) same (IPSEC or (Security with gateway) or SA or router with IPSEC or firewall with IPSEC) same (request$3 or send$3)with message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/04 18:53
S29	31	S28 and "713"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/04 18:53
S30	9	S28 and "380"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/04 18:53
S31	53	S28 and "709"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/04 18:54
S33	9	S31 and mobility$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/04 18:55
S34	11	S29 and mobility$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/04 18:55

S35	4	S30 and mobility$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/04 18:55
S36	142	(security with gateway or firewall or secure with router)same (moblie with terminal or mobile with device or cellphone or telecommunication with terminal or PDA)same (visit $3 or home)with network	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/10 17:47
S37	9	S36 and "713"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/10 17:48
S38	5	S36 and "380"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/10 17:48
S39	16	S36 and "726"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/10 17:48
S40	39	("5303303" | "5444782" | "5559883" | "5812671" | "5850449" | "5870479" | "5884025" | "5898784").PN. OR ("6170057").URPN.	US-PGPUB; USPAT; USOCR	OR	OFF	2009/03/10 18:02

5/11/2009 10:00:01 AM
C:\Documents and Settings\fyalew\My Documents\EAST\Workspaces\10490932.wspp.wsp

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10490932	VAARALA ET AL.
	Examiner	Art Unit
	Fikremariam Yalew	2436

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

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

CLAIM		DATE								
Final	Original	05/11/2009								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	-								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	-								
	11	✓								

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10490932	VAARALA ET AL.
	Examiner	Art Unit
	Fikremariam Yalew	2436

SEARCHED

Class	Subclass	Date	Examiner
713	161	5/11/2009	FA
380	247 Limited including with text search	5/11/2009	FA

SEARCH NOTES

Search Notes	Date	Examiner
Updated East search,NPL searc,Inventor search	5/11/2009	FA

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of Art Unit 2436

Sami Vaarala, Antti Nuopponen

Serial No. 10/490,932

Filed: 22 November 2004

For: METHOD AND NETWORK FOR ENSURING SECURE FORWARDING OF MESSAGES

Examiner: Yalew, Fikremariam A

Date: 25 June 2009

ATTORNEY DOCKET NO. 290.1052USN

AMENDMENT

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

This is in response to the Office action of 12 May, 2009. Please amend the above-identified patent application as follows:

In the Claims:

Amend the claims as follows:

1. (Currently amended) A method for ensuring secure forwarding of a message in a telecommunication network, having at least one mobile terminal and another terminal and a security gateway therebetween, the method comprising:
a) establishing a secure connection between a first address of the mobile terminal and an address of the security gateway, the secure connection defined by at least the addresses of the mobile terminal and the security gateway,
b) the mobile terminal changing from the first address to a second address, ~~and~~
c) while at the second address, the mobile terminal sending a request message to the address of the security gateway to request the security gateway to change the secure connection to be defined between the second address and the address of the security gateway, ~~and~~
in response to the request message from the mobile terminal, the security gateway changing an address definition of the secure connection from the first address to the second address, and
the mobile terminal sending a secure message in the secure connection from the second address of the mobile terminal to the other terminal via the security gateway.

2. (Previously presented) The method of claim 1, wherein the secure connection is established in step a) by forming a Security Association (SA) using IPSec protocols.

3. (Previously presented) The method of claim 1, wherein in step c) a reply back to the mobile terminal is sent from the security gateway after the request from the mobile terminal to

change the address.

4. (Previously presented) The method of claim 2, wherein the request message and/or a reply message is encrypted and/or authenticated by using the same SA already established.

5. (Canceled)

6. (Previously presented) The method of claim 1 wherein the method further comprises the security gateway sending back a reply message to the mobile terminal at the second address to confirm the address change.

7. (Previously presented) The method of claim 6, wherein the mobile terminal and the other terminal form an end-to-end connection whereby the secure connection is an IPSec transport connection or IPSec tunnel connection.

8. (Previously presented) The method of claim 6, wherein a tunneling protocol is used for the secure connection between the mobile terminal and the security gateway.

9. (Previously presented) The method of claim 6, wherein the other terminal is a mobile terminal.

10. (Canceled)

11. (Currently amended) A method for ensuring secure forwarding of a message in a telecommunication network, having at least one mobile terminal and another terminal and a security gateway therebetween, the method comprising:
a) establishing a secure connection between a first address of the mobile terminal and an address of the security gateway, the secure connection defined by at least the addresses of the mobile terminal and the security gateway,

b) the mobile terminal moving from the first address to a second address, ~~and~~

c) while at the second address, the mobile terminal sending a request message to the address of the security gateway to request the security gateway to change the secure connection to be defined between the second address and the address of the security gateway, ~~and~~

the security gateway changing an address definition of the secure connection from the first address to the second address, and

the other terminal sending a secure message in the secure connection to the second address of the mobile terminal via the security gateway.

REMARKS/ARGUMENTS

Reconsideration of the application is respectfully requested. Claims 1-4, 6-9 and 11 are pending in the present invention. Claims 5 and 10 have been canceled to facilitate the prosecution of the current application. No new matter has been added to the application in this response.

1. Rejection of Claims 1-4, 6-9 and 11 under 35 USC § 103(a).

Claims 1-4, 6-9 and 11 were rejected under Section 103 as being obvious over Ahonen in view of Inoue. This § 103 rejection is respectfully traversed in part and overcome in part as follows:

a. The Requisite Steps of Independent Claims 1 and 11 Are Neither Taught Nor Suggested in the Cited Art.

The current claims 1 and 11 recite, among other method steps, "the security gateway changing an address definition of the secure connection from the first address to the second address." In other words, the address definition of the same secure connection is changed from the first address to the second address. Such steps are not taught or suggested in the cited references.

The Examiner correctly states on page 3 of the Office action that Ahonen fails to teach "while at the second address, the mobile terminal sending a request message to the first address of the address of the security gateway to request the security connection to be defined between the second address and the first address of the security gateway" (emphasis added). Ahonen also fails to teach or suggest the step of "in response to the request message from the mobile terminal, the security gateway changing an address definition of the secure connection from the first address to the second address" (emphasis added).

The Examiner then cited Inoue as teaching the missing steps. Applicants respectfully disagree. Inoue merely teaches the mobile computer 2 transmitting a registration message containing information of the current location to the home agent 5 (see col. 6, lines 27-31). The mobile computer 2 does not send the registration message to the gateway 4a. A setting is made in a management table of the gateway 4a and the visited network 1b is registered into the management table of the gateway 4b (see col. 6, lines 27-67). An important feature of Inoue's invention is that the mobile computer 2 compares the security parameters of the new network 1b with the security parameters of the home network 1a (col. 7, line 5-12, 37-42). When they are the same, the mobile computer sets its encryption processing unit to OFF and entrust the

gateway to do the encryption and authentication for improved processing efficiency (col. 9, line 7-21). When the security parameters are not the same, then the mobile computer 2 carries out the encryption and authentication process (see col. 10, 10-21). However, in both cases the encryption and authentication process must take place before the new secure connection can be activated.

It is important to realize that the currently available standardized protocols require that the tunnel endpoints are fixed and if one of the endpoints changes (such as when the terminal moves from one network to another network) then the tunnel has to be re-defined which means all key exchange messages and parameter definitions must be repeated. In general, the standardized protocols such as the IPSec standards do not support moving. If there is a secure connection defined between two terminals and one or both of them moves to another address, the standardized conventional protocols require that a new security connection must be defined between the new addresses or a pre-existing security connection must be used. This involves the activation of the encryption and authentication process unit discussed by Inoue.

Inoue mentions the use of a home agent HA and its function is to manage information on a current location at visited sites of the mobile computers belonging to the network. Inoue also

mentions gateways that have encryption and authentication functions. For example, in col. 5, lines 41 – 50 reference is made to standards which are IPSec standards. In practice, this means that there is an IPSec tunnel, i.e. a secure connection, between the gateway and the mobile computer.

In Inoue, however, the mobile computer 2 does NOT communicate with the other end point of the IPSec tunnel, i.e. the home gateway 4a, when informing that it has moved to a different network. Instead, the mobile computer sends a message to the home agent 5, and the home agent solely takes care of the registration of the new address.

Inoue's home agent 5 does not do ANY changes to any secure connection (and could not even do since the secure connection is between the gateway and the mobile, not between the home agent and the mobile). See col. 6, lines 27-31. The registration with the home agent does not effect the secure connection itself at all.

Inoue refers to standard protocols such as DHCP or PPP (see col. 6, lines 22-26). DHCP manages IP addresses and information about client configuration parameters such as default gateway, domain name, DNS servers and other servers such as time servers but NOT secure connections. With the Point-to-Point Protocol (PPP), a temporary care-of address

from the visited network can be achieved but this protocol does not handle encryption either.

This means that when Inoue's mobile computer is using the visited network 1b a different secure connection, such as a pre-existing or new secure connection, is used compared to when the mobile computer is using the first network 1a. There is nothing in Inoue or any other cited reference about using the same secure connection even though the mobile terminal has moved to a second different address. In other words, Inoue's gateway 4a is not changing the address definition of the same secure connection.

The solution of the present invention handles this problem by requiring the mobile terminal that moved to just send a request to the other endpoint terminal (gateway) and request the gateway "to change the secure connection to be defined between the second address and the address of the security gateway, and in response to the request message from the mobile terminal, the security gateway changing an address definition of the secure connection from the first address to the second address".

It is submitted this simple solution is a very inventive way of handling the problem that occurs when the mobile terminal moves to a different network, i.e. by requesting the other endpoint to change the ADDRESS PARAMETER DEFINITION in the

secure connection and the other definitions, keys and everything else remain the same. It is submitted that nobody has realized that it is possible to solve the problem in this simple way.

One important difference between the cited references and the present invention is that in the present invention a direct change is made to the same secure connection. In Inoue, when the mobile computer has moved to a new network, it is necessary to establish a new secure connection. As indicated above, the main feature of Inoue is to determine whether the new gateway or the mobile terminal itself should carry out the encryption and authentication process. This is confirmed by Inoue referring to the standard IPSec solution (i.e. the RFC standards). According to these standard protocols, when the mobile has moved to a different network it is necessary to establish a new secure connection which involves the cumbersome exchange of keys etc.

It is submitted the cited references do not teach or suggest the step of updating an existing secure connection (IPSec Connection). In contrast, the cited references rely on using either a pre-existing secure connection or establishing a new secure connection, but the secure connection they use after such a move is NOT the same as before the move.

In order to accomplish a seamless move according to the cited

references, this is only possible if there is a gateway having a pre-existing secure connection to the home network.

In summary, the cited references are void any discussion of teaching of a security gateway changing the address definition from the first address to the second address of a mobile terminal in response to the request message from the mobile terminal and the mobile terminal sending a secure message in the SAME secure connection from the second address to the other terminal via the security gateway. It is submitted that Ahonen and Inoue completely fail to teach or suggest the above-outlined steps. Accordingly, the combination of the cited references fails to teach, suggest or provide motivation or incentive for this aspect of the invention. Therefore, the rejection of claims 1 and 11 under § 103(a) is improper, and should be removed.

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

Even assuming *arguendo* that the requisite method steps of claims 1 and 11 are shown by the combination of Ahonen and Inoue, *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.

As provided in M.P.E.P. § 2142, the Supreme Court in *KSR International v. Teleflex Inc.*, 82 USPQ2d 1385, 1396 (2007) specified that the analysis supporting a rejection under 35 U.S.C. § 103 should be made explicit. "[R]ejections on obviousness cannot be sustained with mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *In re Kahn*, 441 F.3dd 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 claims 1 and 11 is at the top of page 4 of the Office action, which merely asserts it would have been obvious to modify the teaching method of Inoue with Ahonen in order "to provide a secure communication method for allowing a mobile host to communicate with a correspondent host over a VPN via a security gateway." (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 perhaps to avoid in many cases, is nonetheless impermissible in making a *prima facie* showing of obviousness.

According to M.P.E.P. 2142, "the examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness." 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 as to claim 1, and any additional remaining claims to the extent they may depend therefrom.

c. Dependent Claims 2-4 and 6-9

Because dependent claims 2-4 and 6-9 depend from the allowable independent claim 1, and as detailed above, their rejection is now moot. However, claims 2-4 and 6-9 also recite additional characteristics that are not found in the cited art.

Accordingly, the rejection of claims 2-4 and 6-9 under §103(a) is improper.

3. Conclusion

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.

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.

Respectfully submitted,

FASTH LAW OFFICES

/rfasth/
Rolf Fasth
Registration No. 36,999

ATTORNEY DOCKET NO. 290.1052USN

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

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

RF:nr 6/29/09 290.1052USN PATENT

Attorney Matter No. 290.1052USN

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of Sami Vaarala, Antti Nuopponen

Serial No. 10/490,932 Art Unit 2436

Filed: 22 November 2004

For: METHOD AND NETWORK FOR ENSURING SECURE FORWARDING OF MESSAGES

Examiner: Fikremariam A. Yalew Date: June 29, 2009

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

TO: COMMISSIONER FOR PATENTS

This Information Disclosure Statement and the enclosed references listed on Form PTO/SB/08 are being filed to comply with the Applicant's duty of disclosure. It is requested that the Examiner review the enclosed information and cite this information as having been considered in connection with this present application.

The Commissioner is hereby authorized to charge the fees required in connection with the filing of this correspondence 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. 290.1052USN

Doc code :IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (03-08)
Approved for use through 06/30/2008. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	10490932
	Filing Date	2004-22-11
	First Named Inventor	Sami Vaarala
	Art Unit	2436
	Examiner Name	Fikremariam A. Yalew
	Attorney Docket Number	290.1052USN

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6839770		2005-04-01	DILLON	
	2	7245405		2007-17-05	FRIEDMAN	
	3	7325063		2008-29-01	DILLON	
If you wish to add additional U.S. Patent citation information please click the Add button.						

U.S.PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					
If you wish to add additional U.S. Published Application citation information please click the Add button.						

FOREIGN PATENT DOCUMENTS								
Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

EFS Web 2.1.2

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	10490932
	Filing Date	2004-22-11
	First Named Inventor	Sami Vaarala
	Art Unit	2436
	Examiner Name	Fikremariam A. Yalew
	Attorney Docket Number	290.1052USN

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

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	IBM, "IP Mobility Support," Memo: October 1996.	☐
	2	THE INTERNET SOCIETY, "Securing L2TP using IPsec," Memo: November 2001.	☐
	3	THE INTERNET SOCIETY, "IP Mobility Support for IPv4," Memo: August 2002.	☐
	4	THE INTERNET SOCIETY, "Layer Two Tunneling Protocol - Version 3 (L2TPv3)," Memo: March 2005.	☐

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	10490932
	Filing Date	2004-22-11
	First Named Inventor	Sami Vaarala
	Art Unit	2436
	Examiner Name	Fikremariam A. Yalew
	Attorney Docket Number	290.1052USN

CERTIFICATION STATEMENT

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

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

OR

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

☒ See attached certification statement.

☐ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ None

SIGNATURE

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

Signature	/rfasth/	Date (YYYY-MM-DD)	2009-06-29
Name/Print	Rolf Fasth	Registration Number	36,999

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

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

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.

Attorney Docket No. 290.1052USN PATENT
RF:ss 6/29/09

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Sami Vaarala, Antti Nuopponen

Art Unit 2436
Confirmation No. 2427

Serial No. 10/490,932

Filed: 22 November 2004

For: METHOD AND NETWORK FOR ENSURING SECURE FORWARDING OF MESSAGES

Examiner: Fikremariam A. Yalew

Date: 29 June 2009

CERTIFICATE OF MAILING

I HEREBY CERTIFY THAT THIS PAPER AND THE DOCUMENTS REFERRED TO AS BEING ATTACHED OR ENCLOSED HEREWITH ARE BEING SUBMITTED ELECTRONICALLY TO THE UNITED STATES PATENT AND TRADEMARK OFFICE ON **29 June 2009**.

/rfasth/

Rolf Fasth
Attorney for Applicant

TRANSMITTAL LETTER

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

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

(X) Response to Office Action dated 12 May 2009.
(X) Supplemental Information Disclosure Statement
(X) PTO/SB08A
(X) Copies of non-patent literature cited
(X) The Commissioner is hereby authorized to charge any fees which may be required in connection with the filing of this correspondence, or credit over-payment, to Account No. 06-0243.

Respectfully submitted,

FASTH LAW OFFICES

/rfasth/

Rolf Fasth
Registration No. 36,999

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

Attorney Docket No. 290.1052USN

Electronic Patent Application Fee Transmittal

Application Number:	10490932
Filing Date:	22-Nov-2004
Title of Invention:	Method and nework for ensuring secure forwarding of messages
First Named Inventor/Applicant Name:	Sami Vaarala
Filer:	Rolf Fasth/Sloan Smith
Attorney Docket Number:	290.1052USN

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($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Electronic Acknowledgement Receipt

EFS ID:	5604008
Application Number:	10490932
International Application Number:	
Confirmation Number:	2427
Title of Invention:	Method and nework for ensuring secure forwarding of messages
First Named Inventor/Applicant Name:	Sami Vaarala
Customer Number:	33369
Filer:	Rolf Fasth/Sloan Smith
Filer Authorized By:	Rolf Fasth
Attorney Docket Number:	290.1052USN
Receipt Date:	29-JUN-2009
Filing Date:	22-NOV-2004
Time Stamp:	13:58:00
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	$180
RAM confirmation Number	158
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	NPL Documents	NPL_A.PDF	134254 f57b711244c086e6578e6824cb7d328907c 8412a	no	88
Warnings:					
Information:					
2	NPL Documents	NPL_B.PDF	56583 c7dddefb6180b50fa9d7fa5503be86604b7 8c4be	no	32
Warnings:					
Information:					
3	NPL Documents	NPL_C.PDF	164902 3dab2d8cd8750fd4a41e03151d880192080 f6762	no	110
Warnings:					
Information:					
4	NPL Documents	NPL_D.PDF	152944 5774202bdeea2c27d065306cf31a9ca9d38 17184	no	103
Warnings:					
Information:					
5		AMD.PDF	42950 386fa7844aa16e281b82fa7e2c0a38b8034d 13d2	yes	15

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Claims	2	4
Applicant Arguments/Remarks Made in an Amendment	5	15

Warnings:					
Information:					
6	Transmittal Letter	IDS.PDF	17341 116d08ecea015cfa81e68d3c549ccc547aa ee3bd	no	1
Warnings:					

Information:					
7	Information Disclosure Statement (IDS) Filed (SB/08)	SBO8.PDF	35589 25449c5eb913a76066092c5941c10ac3f1c07bfc	no	4
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
8	Miscellaneous Incoming Letter	TRX.PDF	18280 2197cee9c8637b253514c4e5f4cd9c10f439e046	no	1
Warnings:					
Information:					
9	Fee Worksheet (PTO-875)	fee-info.pdf	30071 9e678a21aea22e7f1d9aae10fe36d25370ad992f	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	652914	

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
10/490,932	11/22/2004	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☒ RATE ($)	SMALL ENTITY ☒ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	06/29/2009	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 9	Minus	** 20	= 0	X $26 =	0	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $110 =	0	OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

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

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

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

Legal Instrument Examiner:
/DESHONNE T. MARTINO/

PLUS Search Results for S/N 10490932, Searched Thu Sep 10 13:04:03 EDT 2009

The Patent Linguistics Utility System (PLUS) is a USPTO automated search system for U.S. Patents from 1971 to the present PLUS is a query-by-example search system which produces a list of patents that are most closely related linguistically to the application searched. This search was prepared by the staff of the Scientific and Technical Information Center, SIRA.

20050083947 88
20050177722 88
6963982 75
6438612 72
7155740 72
20020046348 72
20020062344 72
7516486 71
20060185012 71
20060041742 70
7434045 68
7346770 68
7386881 68
7536719 68
20040088537 68
20040133798 68
20040143758 68
20060227770 68
20060227807 68
20070204154 68
6832322 67
6886103 67
7028183 67
7107614 67
7143282 67
7296155 67
20010047474 67
20030093691 67
20040210766 67
20070214502 67
20020097724 66
20080155645 64
7308711 64
20050010765 64
20070157312 64
7386723 63
7389357 63
20040103277 63
20050182833 63
6957346 63
7058973 63
20020181400 63
20060256815 63
7401354 62
6931529 62
20020091921 62
20080192739 62
6948074 62
20060095768 62
20070162744 62

UNITED STATES PATENT AND TRADEMARK OFFICE

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

33369 7590 09/29/2009

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

EXAMINER	
YALEW, FIKREMARIAM A	
ART UNIT	PAPER NUMBER
2436	

DATE MAILED: 09/29/2009

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/490,932	11/22/2004	Sami Vaarala	290.1052USN	2427

TITLE OF INVENTION: METHOD AND NEWORK FOR ENSURING SECURE FORWARDING OF MESSAGES

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$755	$300	$0	$1055	12/29/2009

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

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

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

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

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

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

If the SMALL ENTITY is shown as NO:

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

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

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

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

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

PTOL-85 (Rev. 08/07) Approved for use through 08/31/2010.

PART B - FEE(S) TRANSMITTAL

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

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

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

33369 7590 09/29/2009

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

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

Certificate of Mailing or Transmission

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

(Depositor's name)

(Signature)

(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/490,932	11/22/2004	Sami Vaarala	290.1052USN	2427

TITLE OF INVENTION: METHOD AND NEWORK FOR ENSURING SECURE FORWARDING OF MESSAGES

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$755	$300	$0	$1055	12/29/2009

EXAMINER	ART UNIT	CLASS-SUBCLASS
YALEW, FIKREMARIAM A	2436	713-161000

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

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

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____

2 _____

3 _____

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

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

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

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

4a. The following fee(s) are submitted:

☐ Issue Fee

☐ Publication Fee (No small entity discount permitted)

☐ Advance Order - # of Copies _____

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

☐ A check is enclosed.

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

☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

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

☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

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

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

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/490,932	11/22/2004	Sami Vaarala	290.1052USN	2427

33369 7590 09/29/2009

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

EXAMINER	
YALEW, FIKREMARIAM A	
ART UNIT	PAPER NUMBER
2436	

DATE MAILED: 09/29/2009

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

The Patent Term Adjustment to date is 536 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 536 day(s).

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

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

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

PTOL-85 (Rev. 08/07) Approved for use through 08/31/2010.

Notice of Allowability	Application No.	Applicant(s)	
	10/490,932	VAARALA ET AL.	
	Examiner	Art Unit	
	Fikremariam Yalew	2436	

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

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

1. ☒ This communication is responsive to *06/29/2009*.

2. ☒ The allowed claim(s) is/are *1,3,6-9 and 11*.

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

   * Certified copies not received: _____.

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

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

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

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

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 06/29/2009
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☒ Other *See comment*.

DETAILED ACTION

1. This correspondence is in response to **AMENDMENTS and REMARKS** filed on 06/29/2009.

2. **Claims 1, 3, 6-9, 11** are pending. Claims 2, 4-5 and 10 are canceled.

EXAMINER'S AMENDMENT

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

Authorization for this examiner's amendment was given in a telephone interview with Rolf Fasth on 09/10/2009.

The applicant has been amended as follows:

1. (Currently amended) A method for ensuring secure forwarding of a message in a telecommunication network, having at least one mobile terminal and another terminal and a security gateway therebetween, the method comprising:

a) establishing a secure connection between a first address of the mobile terminal and an address of the security gateway, the secure connection defined by at least the addresses of the mobile terminal and the security gateway,

b) the mobile terminal changing from the first address to a second address,

c) while at the second address, the mobile terminal sending a request message to the address of the security gateway to request the security gateway to change the secure connection to be defined between the second address and the address of the security gateway,

in response to the request message from the mobile terminal, the security gateway changing an address definition of the secure connection from the first address to the second address, ~~and~~ the mobile terminal sending a secure message in the secure connection from the second address of the mobile terminal to the other terminal via the security gateway,
the secure connection being established by forming a Security Association (SA) using IPSec protocols, and the request message and/or a reply message being encrypted and/or authenticated by using the same SA already established.

Claim 2. (Canceled)

Claim 4. (Canceled)

Response to Arguments

4. Applicant's arguments with respect to the rejection of the pending claims over prior arts of record have been fully considered and are persuasive. The rejections of Claims 1, 3, 6-9, 11 have been withdrawn.

Allowable Subject Matter

5 **Claims 1, 3, 6-9, 11** are allowed. No reason for allowance is needed as the record is clear in light of further search conducted and applicant's arguments filed on 06/29/2009.

CONTACT INFORMATION

6. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays should be clearly labeled "Comments on statement of Reasons for allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fikremariam Yalew whose telephone number is 5712723852. The examiner can normally be reached on 9-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser, can be reached on 5712738300. The fax phone number for the organization where this application or proceeding is assigned is 571-272-4195.

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.

/Fikremariam Yalew/
Examiner, Art Unit 2436
09/10/2009

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L4	124	(security with gateway or firewall or NAT or secure with gatekeeper or secure with router) near (chang$3 or upgrad$3 or renew or updat$3) with (address or mobile with address or location with address or ip with address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/11 19:21
L5	30	L4 and "726"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/11 19:21
L6	11	L5 and IPSEC	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/11 19:21
S1	66	secure with connection same chang$3 with address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:05
S2	16	S1 and IPsec with protocol	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:05
S3	1	address with change same IPsec with protocol and central with register	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:11
S6	2	S2 and "455"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:12

S7	3	"380"/$.ccls.and S1	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:13
S8	35	((terminal or mobile or cellular with phone)near request)same address with change	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:28
S10	3	S8 and "713"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:29
S12	7	S8 and "455"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:29
S15	24	((current or previous) with address) same IPsec with protocol	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:34
S16	2	"20050083947"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 17:25
S17	1	IPsec same ((RREQ or RREP) with signal$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:03
S18	2	(updat$3 or upgrad$3 or renew$3) same ((single or group) with IPsec with connection)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:07

S19	2	(updat$3 or upgrad$3 or renew$3 or modify$3) same ((single or group) with IPsec with connection)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:09
S20	25	(updat$3 or upgrad$3 or renew$3 or modify$3) and ((single or group) with IPsec with connection)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:35
S21	6	S20 and "713"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:36
S22	5	S20 and "380"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:36
S23	2	S20 and "455"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:36
S24	1	WO-0041427-$.did.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 19:06
S25	0	different with SAs same different with addreess	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 19:21
S26	14	(chang$3 or updat$3 or upgrad$3 or renew$3) near (SA with address or IPSec with address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 19:27

S27	239	(modify$3 or updat$3 or upgrad$3)same (IPSEC or (Security with gateway) or SA) same(request$3 or send$3)with message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/04 18:52
S28	239	(modify$3 or updat$3 or upgrad$3)same (IPSEC or (Security with gateway) or SA or router with IPSEC or firewall with IPSEC) same (request$3 or send$3)with message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/04 18:53
S29	31	S28 and "713"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/04 18:53
S30	9	S28 and "380"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/04 18:53
S31	53	S28 and "709"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/04 18:54
S33	9	S31 and mobility$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/04 18:55
S34	11	S29 and mobility$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/04 18:55
S35	4	S30 and mobility$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/04 18:55

S36	142	(security with gateway or firewall or secure with router)same (moblie with terminal or mobile with device or cellphone or telecommunication with terminal or PDA)same (visit$3 or home)with network	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/10 17:47
S37	9	S36 and "713"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/10 17:48
S38	5	S36 and "380"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/10 17:48
S39	16	S36 and "726"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/10 17:48
S40	39	("5303303" | "5444782" | "5559883" | "5812671" | "5850449" | "5870479" | "5884025" | "5898784").PN. OR ("6170057").URPN.	US-PGPUB; USPAT; USOCR	OR	OFF	2009/03/10 18:02
S41	124	(security with gateway or firewall or NAT or secure with gatekeeper or secure with router)near (chang$3 or upgrad$3 or renew or updat$3)with (address or mobile with address or location with address or ip with address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/11 11:07
S42	1	S41 and "380"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/11 11:08

S43	9	S41 and "713"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/11 11:08
S44	30	S41 and "726"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/11 11:08
S45	58	S41 and "709"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/11 11:08
S46	17	S45 and IPSEC	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/11 11:08
S48	5	S43 and IPSEC	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/11 11:09
S49	2	"6587680".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/11 12:16
S50	2	"6904466".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/11 12:33

3/11/2009 8:28:22 PM
C:\Documents and Settings\fyalew\My Documents\EAST\Workspaces\10490932.wspp.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10490932	VAARALA ET AL.
	Examiner	Art Unit
	Fikremariam Yalew	2436

SEARCHED

Class	Subclass	Date	Examiner
713	161(limited including with text search)	9/10/2009	FA
380	247 (limited including with text search)	9/10/2009	FA
713	151(limited including with text search)	9/10/2009	FA
455	432(limited including with text search)	9/10/2009	FA
455	436(limited including with text search)	9/10/2009	FA
370	401(limited including with text search)	9/10/2009	FA

SEARCH NOTES

Search Notes	Date	Examiner
Updated East search,NPL (Google,ACM,IEEE)search,Inventor search,Plus search	9/10/2009	FA

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner
See above		9/10/2009	FA

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. 2427

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
10/490,932	11/22/2004	455	2436	290.1052USN

APPLICANTS

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

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

This application is a 371 of PCT/FI02/00770 09/27/2002

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

FINLAND 20011910 09/28/2001

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

Foreign Priority claimed	35 USC 119(a-d) conditions met	Verified and Acknowledged	Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
☑ Yes ☐ No	☑ Yes ☐ No	/FIKREMARIAM A YALEW/ Examiner's Signature	☐ FA Initials	FINLAND	0	10	1

ADDRESS

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

TITLE

Method and nework for ensuring secure forwarding of messages

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

Issue Classification

Application/Control No.	Applicant(s)/Patent Under Reexamination
10490932	VAARALA ET AL.
Examiner	**Art Unit**
Fikremariam Yalew	2436

ORIGINAL		INTERNATIONAL CLASSIFICATION	
CLASS	SUBCLASS	CLAIMED	NON-CLAIMED
713	161	H 0 4 L 9 / 00 (2006.01.01)	

CROSS REFERENCE(S)

CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)
713	151
380	247
455	432.1
455	436
370	401

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

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1														
	2														
2	3														
	4														
	5														
3	6														
4	7														
5	8														
6	9														
	10														
7	11														

/Fikremariam Yalew/ Examiner.Art Unit 2436 (Assistant Examiner)	09/10/2009 (Date)	**Total Claims Allowed:** 7
/NASSER G MOAZZAMI/ Supervisory Patent Examiner.Art Unit 2436 (Primary Examiner)	09/11/2009 (Date)	O.G. Print Claim(s) 1 O.G. Print Figure 1

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	10490932
Filing Date	2004-22-11
First Named Inventor	Sami Vaarala
Art Unit	2436
Examiner Name	Fikremariam A. Yalew
Attorney Docket Number	290.1052USN

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6839770		2005-04-01	DILLON	
	2	7245405		2007-17-05	FRIEDMAN	
	3	7325063		2008-29-01	DILLON	

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

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

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

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

EFS Web 2.1.2

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /F.Y./

Receipt date: 06/29/2009	Application Number	10490932	10490932 - GAU: 2436
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date	2004-22-11	
(Not for submission under 37 CFR 1.99)	First Named Inventor	Sami Vaarala	
	Art Unit	2436	
	Examiner Name	Fikremariam A. Yalew	
	Attorney Docket Number	290.1052USN	

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

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	IBM, "IP Mobility Support," Memo: October 1996.	☐
	2	THE INTERNET SOCIETY, "Securing L2TP using IPsec," Memo: November 2001.	☐
	3	THE INTERNET SOCIETY, "IP Mobility Support for IPv4," Memo: August 2002.	☐
	4	THE INTERNET SOCIETY, "Layer Two Tunneling Protocol - Version 3 (L2TPv3)," Memo: March 2005.	☐

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

EXAMINER SIGNATURE

Examiner Signature	/Fikremariam Yalew/	Date Considered	09/23/2009

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

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /F.Y./

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10490932	VAARALA ET AL.
	Examiner	Art Unit
	Fikremariam Yalew	2436

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

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

CLAIM		DATE								
Final	Original	09/10/2009								
1	1	=								
	2	-								
2	3	=								
	4	-								
	5	-								
3	6	=								
4	7	=								
5	8	=								
6	9	=								
	10	-								
7	11	=								

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	34	(dynamic$3 or movabl$3) same ((SA or IPSEC) with session)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/09/10 10:01
L3	34	L2 and(dynamic$3 or movabl$3)same ((SA or IPSEC) with session)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/09/10 10:01
L4	7	"713"/$.ccls. and(dynamic $3 or movabl$3)same ((SA or IPSEC) with session)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/09/10 10:01
L5	8	"726"/$.ccls. and(dynamic $3 or movabl$3)same ((SA or IPSEC) with session)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/09/10 10:01
L6	4	"380"/$.ccls. and(dynamic $3 or movabl$3)same ((SA or IPSEC) with session)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/09/10 10:01
L7	30	security with gateway same (SA or IPSEC)with (chang$3 or updat$3 or replace$3)with (address or IP)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/09/10 10:09
L8	6	L7 and "713"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/09/10 10:10

L9	12	L7 and "726"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/09/10 10:10
L10	1	L7 and "380"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/09/10 10:10
L11	301	(dynamic$3 or (real with time))same (endpoint with chang$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/09/10 10:12
L12	1	(dynamic$3 or (real with time))same (endpoint with chang$3)same (IPSEC or SA)with session	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/09/10 10:13
L13	1	(dynamic$3 or (real with time))same (endpoint with chang$3)same (IPSEC or SA)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/09/10 10:13
L14	380	(IPSEC or SA)same ((mov $3 or dynamic$3 or realtime)with tunnel)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/09/10 10:19
L15	14	L14 and "713"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/09/10 10:19
L16	3	L14 and "380"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/09/10 10:19

L17	23	L14 and "726"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/09/10 10:19
L18	16	L14 and "709"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/09/10 10:19
L19	1	(chang$3 or updat$3 or renew$3 or refresh$3) near ((identical or fix$3) with (IPSEC or SA))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/09/10 10:27
L20	38	(chang$3 or updat$3 or renew$3 or refresh$3) near5 ((identical or fix$3) with (IPSEC or SA))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/09/10 10:27
L21	542	713/161.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/09/10 11:09
L22	1	L21 and L2	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/09/10 11:10
L23	0	L21 and L7	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/09/10 11:10
L24	12	(IPSEC and chang$3 with address and security with gateway).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/09/10 11:11

L25	1	(IPSEC and chang$3 with address and security with gateway and SA).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/09/10 11:12
L26	3	(IPSEC and chang$3 with address and security with gateway and mov$3).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/09/10 11:13
L28	1	(IPSEC and chang$3 with address and security with gateway and SA).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/09/10 11:15
L29	670	713/151.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/09/10 11:17
L30	1	L29 and L11	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/09/10 11:17
L31	0	L29 and L20	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/09/10 11:17
S1	66	secure with connection same chang$3 with address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:05
S2	16	S1 and IPsec with protocol	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:05

S3	1	address with change same IPsec with protocol and central with register	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:11
S6	2	S2 and "455"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:12
S7	3	"380"/$.ccls.and S1	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:13
S8	35	((terminal or mobile or cellular with phone)near request)same address with change	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:28
S10	3	S8 and "713"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:29
S12	7	S8 and "455"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:29
S15	24	((current or previous) with address) same IPsec with protocol	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 16:34
S16	2	"20050083947"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 17:25

S17	1	IPsec same ((RREQ or RREP) with signal$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:03
S18	2	(updat$3 or upgrad$3 or renew$3) same ((single or group) with IPsec with connection)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:07
S19	2	(updat$3 or upgrad$3 or renew$3 or modify$3) same ((single or group) with IPsec with connection)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:09
S20	25	(updat$3 or upgrad$3 or renew$3 or modify$3) and ((single or group) with IPsec with connection)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:35
S21	6	S20 and "713"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:36
S22	5	S20 and "380"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:36
S23	2	S20 and "455"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 18:36
S24	1	WO-0041427-$.did.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 19:06

S25	0	different with SAs same different with addreess	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 19:21
S26	14	(chang$3 or updat$3 or upgrad$3 or renew$3) near (SA with address or IPSec with address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/09/23 19:27
S27	239	(modify$3 or updat$3 or upgrad$3)same (IPSEC or (Security with gateway) or SA) same(request$3 or send$3)with message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/04 18:52
S28	239	(modify$3 or updat$3 or upgrad$3)same (IPSEC or (Security with gateway) or SA or router with IPSEC or firewall with IPSEC) same (request$3 or send$3)with message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/04 18:53
S29	31	S28 and "713"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/04 18:53
S30	9	S28 and "380"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/04 18:53
S31	53	S28 and "709"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/04 18:54
S33	9	S31 and mobility$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/04 18:55

S34	11	S29 and mobility$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/04 18:55
S35	4	S30 and mobility$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/04 18:55
S36	142	(security with gateway or firewall or secure with router)same (moblie with terminal or mobile with device or cellphone or telecommunication with terminal or PDA)same (visit $3 or home)with network	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/10 17:47
S37	9	S36 and "713"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/10 17:48
S38	5	S36 and "380"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/10 17:48
S39	16	S36 and "726"/$.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2009/03/10 17:48
S40	39	("5303303" | "5444782" | "5559883" | "5812671" | "5850449" | "5870479" | "5884025" | "5898784").PN. OR ("6170057").URPN.	US-PGPUB; USPAT; USOCR	OR	OFF	2009/03/10 18:02
S45	11185	secur$4 with connection and gateway	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/05/11 08:40

S46	192	(secur$4 with connection with gateway)(address with change)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2009/05/11 08:41
S47	165	(secur$4 with connection with gateway)(address with change)(security with gateway)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2009/05/11 08:41
S48	12	S47 and (chang$3 or updat $3)with secure with connection	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2009/05/11 08:43

EAST Search History (Interference)

< This search history is empty>

9/ 10/ 2009 11:19:23 AM
C:\ Documents and Settings\ fyalew\ My Documents\ EAST\ Workspaces\ 10490932.wspp.wsp

PART B - FEE(S) TRANSMITTAL

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

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

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

33369 7590 09/29/2009

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

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

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

Sloan Smith	(Depositor's name)
Sloan Smith	(Signature)
7 October 2009	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/490,932	11/22/2004	Sami Vaarala	290.1052USN	2427

TITLE OF INVENTION: METHOD AND NEWORK FOR ENSURING SECURE FORWARDING OF MESSAGES

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$755	$300	$0	$1055	12/29/2009

EXAMINER	ART UNIT	CLASS-SUBCLASS
YALEW, FIKREMARIAM A	2436	713-161000

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

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

1 FASTH LAW OFFICES
Rolf Fasth
2
3

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

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

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

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

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

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

5. **Change in Entity Status** (from status indicated above)
- ☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.
- ☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

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

Authorized Signature /rfasth/ Date 7 October 2009
Typed or printed name Rolf Fasth Registration No. 36,999

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

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

RF:ss 10/7/09 290.1052USN PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Sami Vaarala, Antti Nuopponen

Serial No. 10/490,932

Filed: 22 November 2004

For: METHOD AND NETWORK FOR ENSURING SECURE FORWARDING OF MESSAGES

Examiner: Fikremariam Yalew

Date: 7 October 2009

Art Unit 2436

Confirmation No. 2427

CERTIFICATE OF MAILING

I HEREBY CERTIFY THAT THIS PAPER AND THE DOCUMENTS REFERRED TO AS BEING ATTACHED OR ENCLOSED HEREWITH ARE BEING ELECTRONICALLY SUBMITTED TO THE COMMISSIONER FOR PATENTS, P.O. BOX 1450, ALEXANDRIA, VA 22313-1450 ON 7 October 2009.

/rfasth/

Rolf Fasth
Attorney for Applicant

TRANSMITTAL LETTER

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

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

(X) Form PTOL-85 (Part B - Fee Transmittal)
(X) Issue Fee and Publication Fee ($1055;)to be charged to Account No. 06-0243.
(X) The Commissioner is hereby authorized to charge any additional fees which may be required in connection with the issuance of a patent or credit over-payment to Account No. 06-0243.

Respectfully submitted,

FASTH LAW OFFICES

/rfasth/

Rolf Fasth
Registration No. 36,999

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

Attorney Docket No. 290.1052USN

Electronic Patent Application Fee Transmittal

Application Number:	10490932
Filing Date:	22-Nov-2004
Title of Invention:	METHOD AND NEWORK FOR ENSURING SECURE FORWARDING OF MESSAGES
First Named Inventor/Applicant Name:	Sami Vaarala
Filer:	Rolf Fasth/Sloan Smith
Attorney Docket Number:	290.1052USN

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:				
Utility Appl issue fee	2501	1	755	755
Publ. Fee- early, voluntary, or normal	1504	1	300	300

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**1055**

Electronic Acknowledgement Receipt

EFS ID:	6215245
Application Number:	10490932
International Application Number:	
Confirmation Number:	2427
Title of Invention:	METHOD AND NEWORK FOR ENSURING SECURE FORWARDING OF MESSAGES
First Named Inventor/Applicant Name:	Sami Vaarala
Customer Number:	33369
Filer:	Rolf Fasth/Sloan Smith
Filer Authorized By:	Rolf Fasth
Attorney Docket Number:	290.1052USN
Receipt Date:	07-OCT-2009
Filing Date:	22-NOV-2004
Time Stamp:	07:07:27
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	$1055
RAM confirmation Number	6682
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	Issue Fee Payment (PTO-85B)	PART_B.PDF	85853 651ea1fed3605fb533d2e070c6acf7aad81c887e59	no	1
Warnings:					
Information:					
2	Miscellaneous Incoming Letter	TRX.PDF	20413 1d3939eca2351a9c171a7fc08b059b3cde694380	no	1
Warnings:					
Information:					
3	Fee Worksheet (PTO-875)	fee-info.pdf	31605 6f91d35eb0464aa56f12a9d75c055530e921a8e51	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	137871		

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.

Receipt date: 06/29/2009

Doc code :IDS

Doc description: Information Disclosure Statement (IDS) Filed

10490932 - GAU: 2436

PTO/SB/08a (8-08)

Approved for use through 06/30/2008. OMB 0651-0031

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	10490932
Filing Date	2004-22-11
First Named Inventor	Sami Vaarala
Art Unit	2436
Examiner Name	Fikremariam A. Yalew
Attorney Docket Number	290.1052USN

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6839770		1/2005 ~~2005-04-01~~	DILLON	
TS 10/12/09	2	7245405		7/2007 ~~2007-17-05~~	FRIEDMAN	
	3	7325063		1/2008 ~~2008-29-01~~	DILLON	

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

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

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

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

EFS Web 2.1.2

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /F.Y./

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/490,932	11/17/2009	7620810	290.1052USN	2427

33369 7590 10/28/2009

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

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

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

The Patent Term Adjustment is 536 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

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

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

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

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

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