

DT02 Rec'd PCT/PTO 2 6 MAR 2004

RF:nr 3/26/04 290.105308N

EXPRESS MAIL LABEL NO. ER625088340US

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.: 290.1053USN

Int'l. Application No.: PCT/FI02/00771
 Int'l. Filing Date: 27 SEPTEMBER 2002
 Priority Date Claimed: 28 SEPTEMBER 2001
 Title of Invention: METHOD AND SYSTEM FOR ENSURING
 SECURE FORWARDING OF MESSAGES
 Applicant(s) for DO/ES/US: Sami Vaarala, Antti Nuopponen, Panu
 Pietikainen

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

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

0111 Rec'd P0T/PTO 26 MAR 2004

RF:nr 3/26/04 290.1053USN

EXPRESS MAIL LABEL NO. ER625088340US

Date of Mailing: 26 March 2004

- 12. An assignment document for recording. A cover sheet in compliance with 37 C.F.R. 3.28 and 3.31 is included.
- 13. A FIRST preliminary amendment.
- 14. Applicant qualifies for Small Entity Status (37 C.F.R. 1.9(f) and 1.27(b)).
- 16. Other items or information: (if any)
- 17. Basic National Filing Fee of **\$1080.00** is submitted (Neither international preliminary examination fee (37 C.F.R. 1.482) nor international search fee 37 C.F.R. 1.44.5(a) (2) paid to U.S.P.T.O.).

CLAIMS AS FILED			
For	Number Filed	Number Extra	Basic Fee \$1080.00 Rate
Total Claims	17 - 20	= 0	x \$18.00 = \$0.00
Ind. Claims	2 - 3	= 0	x \$86.00 = \$0.00

- 19. Reduction by 1/2 for filing by small entity, if applicable. Applicant qualifies as small entity. TOTAL FILING FEE: **\$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. A check in the amount of **\$540.00** to cover the above fee is enclosed.
- 23. The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 06-0243.

Respectfully submitted,

Rolf Fasth
Registration Number 36,999

Send all correspondence to:

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

METHOD AND SYSTEM FOR ENSURING SECURE FORWARDING OF MESSAGES**TECHNICAL FIELD**

5

The method and system of the invention are intended to secure connections in telecommunication networks. Especially, the invention is meant to be used in wireless networks as a part of a mobile IP solution or an IPSec solution.

10

TECHNICAL BACKGROUND

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

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

In fixed networks, there exist solutions to fill the need to protect data and resources from disclosure, to guarantee the authenticity of data, and to protect systems from network based attacks. IPSec is one such technology by means of which security is obtained.

The IP security protocols (IPSec) provides the capability to secure communications 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 (as remote access IPSec

use), or to secure communication with other organisations, ensuring authentication and confidentiality and providing a key exchange mechanism. Even if some applications already have built in security protocols, the use of IPSec further enhances the security.

- 5 IPSec can encrypt and/or authenticate traffic at IP level. Traffic going in to a WAN is typically encrypted and/or authenticated and traffic coming from a WAN is decrypted and/or authenticated. IPSec is defined by certain documents, which contain rules for the IPSec architecture.
- 10 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). Both AH and ESP are vehicles for access control based on the distribution of cryptographic keys and the management of
- 15 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-

20 way relationship is needed, then two security associations are required.

The term IPSec connection is used in what follows in place of an IPSec bundle of one or more security associations SAs, or a pair of IPSec bundles – one bundle for each direction – of one or more security associations. This term thus covers both

25 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

30 Security Parameters Index (SPI), is a 32-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.

5

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

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

Tunnel mode provides protection to the entire IP packet and is used for sending messages through more than two components. 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 setup 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 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
5 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 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 involving
10 encapsulation of the packet in an outer IP header. The source IP address of this outer
IP packet 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
15 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 and selected fields of the outer IP header.

20

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
25 (IKE) is a newer name for the ISAKMP/Oakley. IKE is based on the Diffie-Hellman key
exchange algorithm, and supports RSA signature authentication among other modes.
IKE is easily extensible for future and vendor-specific features without breaking
backwards compatibility.

30 The IPSec protocol solves the known security problems of the Internet Protocol (IP) in
a satisfactory manner. However, it is designed for a static Internet, where the hosts
using IPSec are relatively static. Thus, IPSec does not work well with mobile devices.

For instance, if a mobile terminal moves from one network to another, an IPSec connection set up is required, typically using the IKE key exchange protocol. Such a set up is expensive in terms of latency, since IKE may require several seconds to complete. It is also expensive in terms of computation, because the Diffie-Hellman and authentication-related calculations of IKE are extremely time consuming.

Routing means moving information across an internetwork from one source to another. Along the way, usually at least one intermediate node is encountered. Routing involves both the determination of the optimal routing path and the transport of information packets. To aid the routing of information packets, routing algorithms initialise and maintain routing tables, which contain route information. Routers communicate with each other and maintain their routing tables through the transmission of a variety of messages. The routing update message is one such message that generally consists the whole or part of a routing table.

The fundamental problem with IP mobility is the fact that IP routing is based on fixed addresses. The address space has been divided into subnetworks, that reside in practically fixed locations with respect to network topology (the routing can be changed, but that is a slow process, possibly in the order of minutes). When a mobile host moves away from its home network (where its IP address is proper), there is a problem with the routing of the packets to the new location if the IP network in question does not support such movement.

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.

Standard Mobile IP for IPv4 utilises e.g. IP-IP and Generic Routing Encapsulation (GRE) tunnelling to overcome this problem (See more details in figure 1 with accompanying text). There are also other methods of tunnelling, and hence, IP-IP and GRE tunnelling are used only as examples in this text. Mobile IPv4 has two modes of operation. In the co-located care-of address mode the mobile terminal performs IP-IP

encapsulation and decapsulation. This mode requires a borrowed address - the co-located care-of address - from the visited network. The other mode is the foreign agent mode, where the IP-IP or other tunnelling is performed by a special host in the visited network, called the Foreign Agent (FA). The mobile terminal communicates directly
5 with the FA (an IP address is not required for this direct communication), and does not require a borrowed address in this mode.

In IP-IP tunnelling, an IP address (the so called co-located care-of address) is borrowed from a network being visited. This address is topologically correct, i.e.
10 routable from other parts of the network. When a mobile terminal needs to send a packet to a given target computer, it first constructs an IP packet, whose source address is its home address, i.e. the address that is not topologically correct in the new network, and whose destination address is the target computer.

15 Since this packet may not be directly routable, it is encapsulated into another IP packet (by so called IP-IP encapsulation, or IP-IP tunnelling). The source address of this IP packet is the care-of address, and the target address is the so called home server of the mobile terminal. Upon receiving such an encapsulated packet, the home server unwraps the IP-IP tunnel, and proceeds to route the packet, which was inside the
20 encapsulation.

Reverse packets from the target computer to the mobile terminal are handled similarly; the packet is first routed to the home server, then encapsulated in IP-IP and delivered to the current network the mobile terminal is in. The current mobility binding
25 determines which current care-of address matches a given home address. (There may also be so-called simultaneous bindings, in which case the home address matches a set of care-of addresses; the packet is encapsulated and sent to each care-of address separately.)

30 When the mobile terminal moves to a new network, an authenticated signalling message exchange is done between the mobile terminal and the home server. A Registration Request is sent by the mobile terminal to the home server, requesting an

update of the current mobility binding. The server responds using a Registration Reply that may either accept or deny the request. When the Foreign Agent mode of operation is used, the registration messages go through the Foreign Agent.

- 5 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
- 10 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.
- 15 The IPSec protocol solves the known security problems of the Internet Protocol (IP) in a satisfactory manner. However, it is designed for a static Internet, where the hosts using IPSec are relatively static. Thus, IPSec does not work well with mobile devices. For instance, if a mobile terminal moves from one network to another, an IPSec connection set up is required, typically using the IKE key exchange protocol. Such a
- 20 set up is expensive in terms of latency, since IKE may require several seconds to complete. It is also expensive in terms of computation, because the Diffie-Hellman and authentication-related calculations of IKE are extremely time consuming.

The above description presents the essential ideas of Mobile IP.

25

The mobile IP approach of prior art has some disadvantages and problems.

- The standard Mobile IP protocol provides a mobile terminal with a mobile connection, and defines mechanisms for performing efficient handovers from one network to
- 30 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. In the manual prior art key management, the signalling authentication mechanism requires the mobile host and the home server to share a secret authentication key and the distribution of that key, which is carried out manually, is not very practical. Finally, the current Mobile IP protocol does not define a method for working through Network Address Translation (NAT) devices.

Said problem with Network Address Translation (NAT) devices, even if NAT devices are able to translate addresses of private networks in messages to public IP addresses so that the messages can be sent through internet, is, however, that currently no standard for making Mobile IP work through NAT devices. NAT devices are widely deployed because the use of private addresses requires less public IP addresses than would otherwise be needed.

15

REFERENCES

The following is a list of useful references for understanding the technology behind the invention.

20

IP in general, UDP and TCP:

[RFC768]

25 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.

30

<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.

5 <ftp://ftp.isi.edu/in-notes/rfc793.txt>

[RFC826]

D.C. Plummer, *An Ethernet Address Resolution Protocol*, RFC 826, November 1982.

10 <ftp://ftp.isi.edu/in-notes/rfc826.txt>

[RFC2460]

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

15

Mobile IP; IP-IP; DHCP:

[RFC2002]

C. Perkins, *IP Mobility Support*, RFC 2002, October 1996.

20 <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>

25

[RFC2131]

R. Droms, *Dynamic Host Configuration Protocol*, RFC 2131, March 1997.

<ftp://ftp.isi.edu/in-notes/rfc2131.txt>

30 [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.

5 [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.

10

IPSec standards:

[RFC2401]

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

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

[RFC2402]

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

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

[RFC2403]

25 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.

30

[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>

5

[RFC2407]

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

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

10

[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>

15

[RFC2409]

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

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

20

[RFC2410]

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

25

[RFC2411]

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

30

[RFC2412]

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

NAT:

[RFC2694]

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

[RFC3022]

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

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

15 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 described above.

20 SUMMARY OF THE INVENTION

25 The method of the invention for ensuring secure forwarding of a message is performed in a telecommunication network, comprising at least one terminal from which the message is sent and at least one other terminal to which the message is sent. In the method, one or more secure connections are established between different addresses of the first terminal and address of the other terminal, the connections defining at least said addresses of the two terminals. When the first terminal moves from one address to another address, a secure connection, whose endpoints are the new address of the first terminal and the address of the other terminal, is registered to be at least one of
30 the active connections.

If there does not already exist such a secure connection between the new address and the other terminal, a new secure connection between the new address and the other terminal address has to be formed.

- 5 The terminals might have several active connections. In the invention, the terminal might in one embodiment also have only one secure active connection at a time, which can be changed in according with the invention to be defined to be between the address the terminal moves to and the address of the other terminal.
- 10 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 invention is moreover concerned with a system, which is able to perform the method of the invention. The characteristics of the system are defined by the system
15 main claim, the subclaim defining the functions that can be performed by the system of the invention.

The secure connections are preferably established by forming Security Associations (SAs) using the IPSec protocols and the message to be forwarded consists of IP
20 packets. The key exchange being a part of the forming of a secure connection is performed manually or automatically with IKE or some other automated key exchange protocol.

When a new secure connection is formed, it is registered for immediate and/or later
25 use. The registration for later use is made using a connection table, which is maintained by both hosts participating in the forming of the secure connection. The connection table is also used e.g. when the first terminal moves, and needs to determine whether a secure tunnel already exists for the new address. The table can be e.g. a Security Association DataBase (SADB), which is the nominal place to store
30 IPSec SAs in the IPSec model.

In the preferred embodiment, IPsec security associations are used as secure connections. The table, through which the existence of a given IPsec SA (in either the first terminal or the other terminal) is determined, is then the IPsec Security Association DataBase (SADB).

5

The actual connection(s) to be used is registered by means of a signalling message or signalling message exchange between the first terminal and the other terminal, for example by means of Registration Request and possibly Registration Reply messages.

10

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.

15

The new address of the first terminal can also be updated automatically by the other terminal when the first terminal sends a message from its new address.

The active SA is a stored mobility binding that maps a given terminal address to one or more IPsec tunnel mode SAs (or zero such SAs, if the terminal in question is not connected). These mobility bindings are manipulated when Registration Request and Registration Reply messages are processed when sending packets to the first terminal. It is possible to restrict traffic from the first terminal to only the IPsec SAs that are currently registered in the mobility binding, but allowing traffic from all shared SAs is also reasonable.

20

The mobility binding is necessary, since each of the shared IPsec security associations is valid for securing traffic. There has to be some way for the first terminal

to determine which security association(s) to actually use when processing packets. The mobility binding serves this purpose in the invention.

5 The first terminal may use any IPSec tunnel SA it shares with the other terminal. It is possible to restrict traffic from the first terminal to only the IPSec SAs that are currently registered, but this is not an essential feature. Thus, the first terminal may use any IPSec tunnel SA it shares with the other terminal when sending packets. The other terminal may restrict traffic only to IPSec SAs that are currently active in the mobility binding, but allowing traffic from all shared SAs is also reasonable.

10

The invention can be used for direct end-to-end communication, in which case the secure tunnel is established between these end computers. If applied to IPSec, this could correspond to either an IPSec transport mode or tunnel mode SA. The message might also be sent first to an intermediate computer, whereby the outer address of the
15 IPSec tunnel is unwrapped by the intermediate computer and the message is forwarded as plain text to the end destination computer.

20 Thus, in the solution of the invention, an IPSec security association is used instead of the IP-IP tunnelling. The invention can also be used for tunnelling with IPSec transport mode and an external tunnelling mechanism, such as Layer 2 Tunnelling Protocol (L2TP).

The invention provides the following advantages.

25 IPSec key management and strong authentication can be leveraged for this application involving asymmetric (RSA) authentication, the use of the Diffie-Hellman key exchange algorithm, the possibility to use certificates etc.

30 The IPSec symmetric encryption and authentication methods can be used to protect both signalling and data traffic. This provides confidentiality and integrity and any future developments of IPSec can be taken advantage of.

The NAT traversal problem can be solved by using any available NAT traversal mechanisms for IPsec. One is currently being standardised for IPsec, but any other IPsec NAT traversal mechanism may be used.

- 5 The invention can be used in different networks, such as IPv4 and IPv6.

In the following the invention is described more in detail by means of an advantageous embodiment in an example network but is not restricted to the details thereof.

10

FIGURES

Figure 1 describes the mobile IP tunnelling of prior art by means of a signalling diagram

15

Figure 2 describes the method of the invention by means of a signalling diagram

DETAILED DESCRIPTION

20

The data communication in figure 1 takes place from a mobile terminal to a target host X via an intermediate computer, which works as a home server for host X.

25 Packets sent from the home address of the mobile terminal can be directly routed to the target address X by the intermediate computer, since the home address is registered in routing tables by means of which the routing takes place.

30 Figure 1 describes a method of prior art, wherein IP-IP tunnelling is used for routing data packets when the mobile host moves from one address to another, i.e. from the home address to a new address.

Mobile IP also supports the so-called triangular routing mode, where the packets sent by the mobile terminal are routed directly to the recipient of the packet, bypassing the home server, while packets sent to the mobile terminal are first routed to the home server and then IP-IP tunnelled to the mobile terminal. This mode is more efficient, but is incompatible with so-called ingress filtering routers, which do not route IP packets whose source addresses are topologically incorrect, as is the case with a mobile terminal that is away from the home network. The details of this mode are different, but the general idea is the same. The more general case where IP-IP tunnelling is used for traffic between the mobile terminal and the home server in both directions is discussed in the following text.

In figure 1, when a mobile terminal being in a visited network intends to send a packet to a target host X using its current care-of address, which is an address borrowed from the visited network, it first constructs a data packet, whose source address is its home address – which is not a topologically correct address in the current network the mobile terminal is in – and whose destination address is X. Because the source address of the packet is topologically incorrect, i.e., does not belong to the network the mobile terminal is in, some routers, especially the ones that implement the so-called ingress filtering algorithm, will not route the packet properly. To overcome this, the packet is encapsulated into another IP packet; this process is called IP-IP tunnelling or IP-IP encapsulation. The new, outer IP header source address is the care-of address from the visited network – which is a topologically correct address – and the outer IP header destination address is the home server of the mobile terminal. Thus, the inner IP header source address is the home address of the mobile terminal, while the inner IP header destination address is that of the host X. This is indicated in figure 1 with IP | IP | data, which describes a message containing data and the original IP header, which is encapsulated further in an outer IP header for routing purposes. This IP packet is then sent to the home server in step 1 of figure 1.

Upon receiving the encapsulated IP packet, the home server unwraps the IP-IP tunnel, and proceeds in step 2 of figure 2 with routing a packet indicated with IP/Data, which packet was inside the encapsulation (inside the outer IP header). The routing is

performed in accordance with the inner destination address, the packet now, after the unwrapping, having the home address of the mobile terminal as its source address and host X as its destination address.

- 5 Reverse packets from X to the mobile terminal are handled similarly; the packet is first routed to the home server in step 3, then encapsulated in IP-IP and delivered to the current network (in step 4) the mobile terminal is in. The mobility binding determines which care-of address(es) the packet is forwarded to.
- 10 In the method of the invention, an IPSec tunnel mode or transport mode security association is used instead of the IP - IP tunnelling. Figure 2 describes an example of the method of the invention for sending messages when a mobile terminal moves to a new address.
- 15 A secure connection, preferably an IPSec security association (SA) or more specifically one IPsec SA bundle for each direction of communication is established between the care-of-address and the home server address, e.g. the care-of-address of the mobile terminal and the home server address. The SA can also include additional parameters and attributes, possibly relating to standard or non-standard IPSec
- 20 extensions, such as NAT traversal, which are conventionally used in SAs. A message to be sent through this tunnel is marked IP/IPSec/IP/Data in figure 2, illustrating that the message contains a data part with a destination IP address and can be sent through an IPSec tunnel, while encapsulated with an outer IP header.
- 25 Reverse packets from X to the mobile terminal are handled similarly; the packet is first routed to the home server in step 3, then IPSec processed using the IPSec tunnel mode SA, during which an outer IP header is added to the packet and delivered to the current network(s) (in step 4) the mobile terminal is in.
- 30 When IPSec transport mode is used, the mobile terminal may either communicate directly with the home server, or alternatively some external tunnelling protocol (apart from IPSec tunnelling) can be used to allow routing of packets further. For example,

the Layer 2 Tunnelling Protocol (L2TP) can be used with IPsec transport mode to provide functionality similar to IPsec tunnelling.

When the mobile terminal moves to a new network, it first obtains a care-of address
5 from the visited network. The mobile terminal then checks whether an SA (or more precisely, a pair of SA bundles) SA already exists between the new care-of address and the home server address.

This check is normally done by inspecting the contents of a Security Association
10 DataBase (SADB), as specified by the IPsec protocol. The actual implementation may somewhat deviate from the nominal processing. The nominal model and the actual operations often are in reality somewhat different (for instance, hardware IPsec implementations have a radically different "SADB" implementation than simple lookup.)
15 If an IPsec security association (SA) between the mobile terminal and the home server defining the care-of address of the mobile terminal at one end (the new address of the mobile terminal) and the address of the home server at the other end already exists, this SA is registered to be the actual SA to be used.

This happens by means of a signalling message or signalling message exchange done
20 between the mobile terminal and the home server, described by steps 5 and 6 in figure 2. The messages are preferably authenticated and/or encrypted by using IPsec, and preferably by using the same IPsec SA that is used for the ordinary traffic protection. In some embodiments no reply is used. Step 5 is a registration request from the mobile host to the home server to register the new address and step 6 is a registration reply
25 back to the mobile terminal.

When a SA does not exist between the new care-of address and the home server, an SA setup occurs between steps 4 and 5 of figure 2. This SA setup may be manual, or may involve some automatic key exchange protocol, such as the Internet Key
30 Exchange (IKE).

Upon receiving the IPsec protected packet sent using the new SA, the home server processes the IPsec headers and uncovers the original packet from the IPsec tunnel, and then routes the IP packet to host X. If IPsec transport mode is used, the home server processes the IPsec headers and processes the resulting plaintext packet
5 directly without routing it onwards. However, if an external tunnelling protocol, such as L2TP, is used, the tunnelling protocol may forward the packet after IPsec processing.

In figure 2, the RREQ and RREP messages are shown without IPsec protection. In an IPsec embodiment, the IPsec protected messages would be expressed e.g. as
10 IP|IPsec|IP|RREQ resp. IP|IPsec|IP|RREP instead of IP|RREQ resp. IP|RREP. Thus, RREQ/RREP can be protected and one method of protection would be IPsec. If they are protected using IPsec, one can leverage the existing IPsec SA for that purpose. The IPsec protection of signalling message(s) may use either tunnel or transport mode.

15

The abbreviation RREQ in figure 2 stands for Registration Request while the abbreviation RREP stands for Registration Reply. These are preferably the Mobile IP Registration Request and Registration Reply messages, used in conjunction with IPsec in the invention, but other registration formats may be used. It is also within the
20 scope of the invention to only use a Registration Request message (not necessarily using the exact Mobile IP format), but not using a Registration Reply message.

The invention also covers both the case wherein properly authenticated traffic is used as an implicit registration request, and a mobility binding update is performed
25 automatically. As a specific example, an IPsec tunnel mode SA bundle, including an AH used for sending traffic, in which case the addresses of the outermost IP header are covered by AH authentication, is used between the mobile terminal and the home server. When the mobile terminal moves to a new network, it sends a data packet which may be an empty data packet if there is no data to send that is processed using
30 the IPsec SA bundle and sent to the home server. Once the home server properly authenticates the message, including the outermost IP header, and determines that it is coming from an address that differs from the current mobility binding, it may update

the mobility binding automatically. Updating the binding results in that all subsequent packets being destined to the mobile terminal, will be sent using the updated mobility binding, i.e. the new address that the client is using. Thus, no explicit mobility binding update signalling is required in this case.

5

The description of the invention above has been simplified for clarity of description. The invention can be extended in several ways without changing the underlying idea. Some extensions are described in what follows.

- 10 The Mobile IP concept of simultaneous bindings, and associated traffic n-casting from the home server to the mobile terminal can be used. In this case, packets sent towards the mobile terminal would be processed using several IPsec SAs, one for each simultaneous registration, and sent to the different visited networks used by the mobile terminal. The registration message(s) in this case contain fields that indicate
- 15 how the mobility binding is to be modified, e.g. whether to replace existing bindings, or to add a new binding in addition to the existing ones. The implicit registration based on data packets can also be used, possibly together with registration message(s) to maintain the bindings.
- 20 When an IPsec SA does not exist between the new care-of address and the home server address, and an IPsec SA is set up e.g. using an automated key exchange protocol, the completion of the SA setup can be used as an implicit registration, removing the additional registration in steps 5 and possibly 6 in figure 2.
- 25 When in the above "a Security Association SA" or "a bundle of Security Associations SAs" is referred to, this means in practice, an IPsec SA bundle in both cases – one or more IPsec security associations applied in sequence – can be used for each direction of traffic.
- 30 The invention is not specific to IPv4 or IPv6, and can be used with Mobile IP for IPv4 and Mobile IP for IPv6. The invention is also straightforward to extend to future IPsec versions

ART 34 AMDT

22

CLAIMS

1. Method for ensuring secure forwarding of a message in a telecommunication network, comprising at least one first terminal from which the message is sent and
5 at least one other terminal to which the message is sent,
characterized by
 - a) establishing one or more secure connections between different addresses of the first terminal and address of the other terminal, these connections defining at least said addresses of the two terminals,
 - 10 b) the first terminal moving from one address to another address,
 - c) a secure connection between said other address and the other terminal address is registered to be at least one of the active connections to be used.
2. Method of claim 1, characterized in that a new secure connection between
15 the other address of the first terminal and the address of the other terminal is formed for the registration in step c) if such a secure connections does not already exist.
3. Method of claim 1, characterized in that, the secure connection is
20 established in step a) and claim 2 by forming one or more Security Associations (SAs) using the IPSec protocols, such as a bundle of SAs.
4. Method of any of claims 1 - 3, characterized in that the message to be
25 forwarded consists of IP packets.
5. Method of any of claims 1 - 4, characterized in that, after step b), when the first terminal intend to send a message from the address it has moved to it first checks whether a secure connection between the new address and the other terminal already exists.
- 30 6. Method of claim 5, characterized in that the existence of the new secure connection is checked by means of a connection table.

- 7. Method of any of claims 1 - 6, characterized in that, in step c), the actual connection(s) to be used is/are registered by means of a signalling message or signalling message exchange between the mobile terminal and the other terminal.
- 5 8. Method of any of claims 1 - 6, characterized in that, the new (second) address of the mobile terminal is updated automatically by the other terminal when the first terminal sends a message from its new address.
- 9. Method of any of claims 1 - 8, characterized in that the a key exchange being a part of the forming of the secure connection in step a) and claim 2 is performed manually.
- 10 10. Method of any of claims 1 - 8, characterized in that a key exchange being a part of the forming of the secure connection in step a) and claim 2 is performed with IKE or some other automated key exchange protocol.
- 15 11. Method of any of claims 1 - 10, characterized in that the secure connection between the new address of the first terminal and the other terminal is in step c) registered for immediate and/or later use.
- 20 12. Method of claim 11, characterized in that the registration for later use is made by the other terminal in a connection table.
- 13. Method of any of claims 3 - 12, characterized in that when sending message through the secure connection IPSec transport mode is used to secure traffic between the mobile computer and the destination computer.
- 25 14. Method of claim 13, characterized in that a tunnelling protocol is used together with IPSec to provide a tunnelling capability.
- 30

15. Method of claim 14, characterized in that where the Layer 2 Tunnelling Protocol (L2TP) tunnelling protocol is used together with IPSec to provide a tunnelling capability.

5 16. Method of any of claims 3 – 15, characterized in that when sending message through the secure connection IPSec tunnel mode is used to secure traffic between the mobile computer and the destination computer.

10 17. System for ensuring secure forwarding of a message in a telecommunication network, comprising at least one first terminal from which the message is sent and at least one other terminal to which the message is sent,
characterized by
means for forming secure connections between the address of the other terminal and different addresses of the first terminal,
15 tables with lists of said secure connections, and
registrations means for forming such lists.

18. System of claim 17, characterized in that it has means for performing the method of any of claims 1 - 16.

490, 933

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

(19) World Intellectual Property Organization
International Bureau



28 MAR 2004
[Barcode]

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

PCT

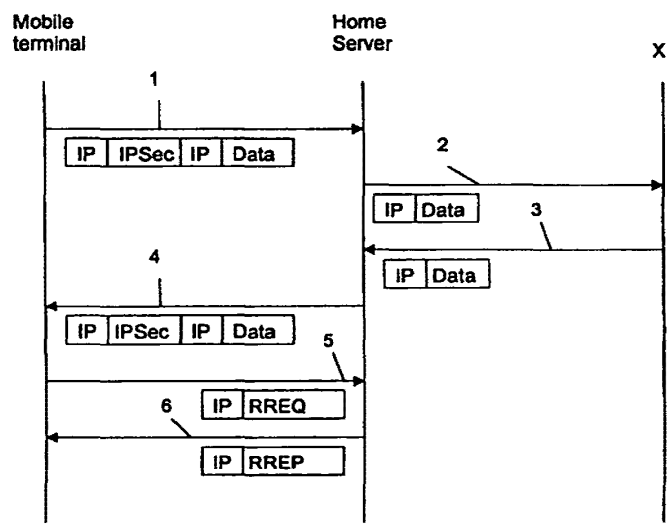
(10) International Publication Number
WO 03/030488 A1

- (51) International Patent Classification?: **H04L 29/06**, H04Q 7/38
- (74) Agent: **INNOPAT LTD**; P.O. Box 556, FIN-02151 Espoo (FI).
- (21) International Application Number: PCT/FI02/00771
- (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.
- (22) International Filing Date: 27 September 2002 (27.09.2002)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data: 20011911 28 September 2001 (28.09.2001) FI
- (84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, 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).
- (71) Applicant (*for all designated States except US*): **IN-TRASECURE NETWORKS OY** [FI/FI]; P.O. Box 38, FIN-02210 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). **PIETIKÄINEN, Panu** [FI/FI]; Täysikuu 10 C 103, FIN-02210 Espoo (FI).

Published: — with international search report

[Continued on next page]

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



(57) Abstract: The invention is concerned with a method for ensuring secure forwarding of a message is performed in a telecommunication network, comprising at least one terminal from which the message is sent and at least one other terminal to which the message is sent. In the method, one or more secure connections are established between different addresses of the first terminal and address of the other terminal, the connections defining at least said addresses of the two terminals. When the first terminal moves from one address to another address, a secure connection, whose endpoints are the new address of the first terminal and the address of the other terminal, is registered to be at least one of the active connections.

WO 03/030488 A1

1/2

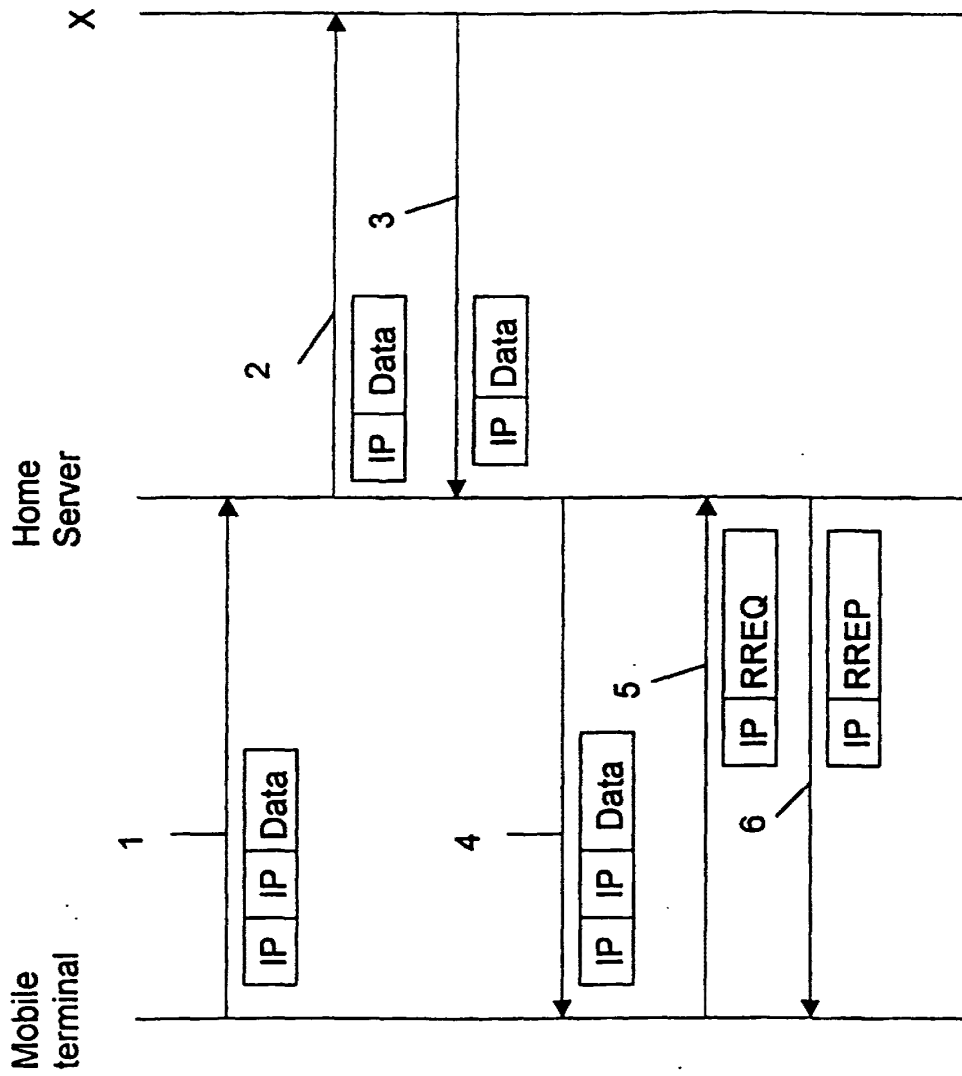


FIG. 1

2/2

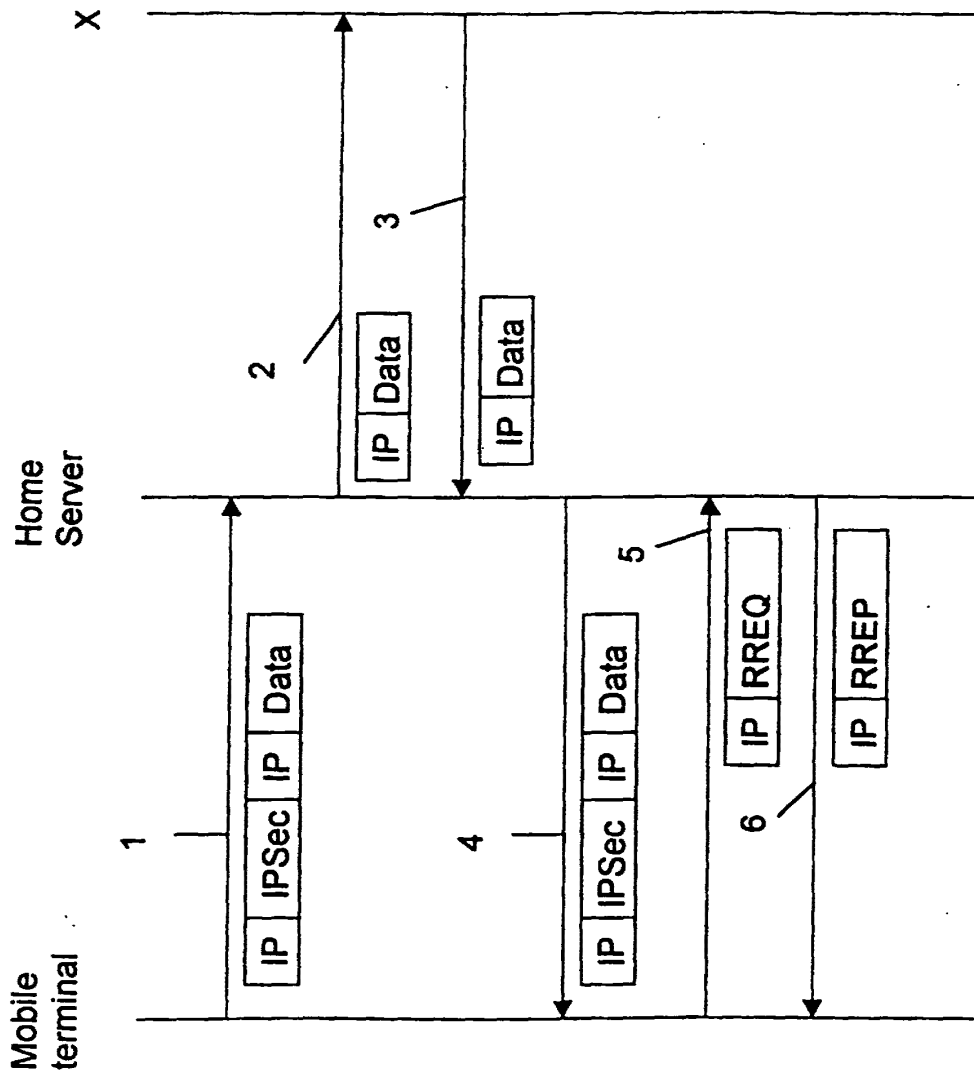


FIG. 2

**COMBINED DECLARATION AND POWER OF ATTORNEY
FOR PATENT APPLICATION**

As a below named inventor, I hereby declare that:

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

I believe I an original, first and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled METHOD AND SYSTEM FOR ENSURING SECURE FORWARDING OF MESSAGES, the specification of which was filed as International Patent Application No. PCT/FI02/00771, 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
<u>20011911</u> (Number)	<u>Finland</u> (Country)	<u>28 Sept. 2001</u> (Day/Month/Year)	[X] [] Yes No

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

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

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

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

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

Address all correspondence to:

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

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

Full name of first joint inventor: Sami Vaarala	
Inventor's signature _____	Date
Residence: Helsinki, Finland	
Citizenship: Finland	
Post Office address: Neljas Linja 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	
Full name of third joint inventor: Panu Pietikainen	
Inventor's signature _____	Date
Residence: Espoo, Finland	
Citizenship: Finland	
Post Office address: Taysikuu 10 C 103 FIN-02210 Espoo, Finland	

**MULTIPLE DEPENDENT CLAIM
FEE CALCULATION SHEET
(FOR USE WITH FORM PTO-875)**

SERIAL NO. **10/490933** FILING DATE
APPLICANT(S)

CLAIMS

	AS FILED		AFTER 1st AMENDMENT		AFTER 2nd AMENDMENT			IND.		DEP.			IND.		DEP.	
	IND.	DEP.	IND.	DEP.	IND.	DEP.		IND.	DEP.	IND.	DEP.		IND.	DEP.	IND.	DEP.
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																
TOTAL IND.	2															
TOTAL DEP.	15															
TOTAL CLAIMS	17															
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																
TOTAL IND.																
TOTAL DEP.																
TOTAL CLAIMS																

BEST AVAILABLE COPY

PATENT APPLICATION SERIAL NO. 10 / 490933

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

12/01/2004 SAHMED1 00000001 10490933
~~04/01/2004 GFREY1 00000078 10490933 DP~~
~~01-FC-2611 -540.00 DP~~
Repln. Ref: 12/01/2004 SAHMED1 0008403800
DA#:060243 Name/Number:10490933
FC: 9204 \$80.00 CR
Adjustment date: 12/01/2004 SAHMED1
04/01/2004 GFREY1 00000078 10490933
~~01-FC-2611 -540.00 DP~~

PTO-1556
(5/87)

PATENT APPLICATION FEE DETERMINATION RECORD
Effective October 1, 2003

Application or Docket Number:

10 / 490933

CLAIMS AS FILED - PART I

	(Column 1)	(Column 2)
TOTAL CLAIMS		
FOR	NUMBER FILED	NUMBER EXTRA
TOTAL CHARGEABLE CLAIMS	17 minus 20 =	*
INDEPENDENT CLAIMS	2 minus 3 =	*
MULTIPLE DEPENDENT CLAIM PRESENT <input type="checkbox"/>		

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

CLAIMS AS AMENDED - PART II

	(Column 1)	(Column 2)	(Column 3)
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
	Total	Minus **	=
	Independent	Minus ***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <input type="checkbox"/>			

SMALL ENTITY TYPE OR

OTHER THAN SMALL ENTITY

RATE	FEE	OR	RATE	FEE
BASIC FEE	460	OR	BASIC FEE	
XS 9=		OR	XS18=	
X43=		OR	X86=	
+145=		OR	+290=	
TOTAL	460	OR	TOTAL	

525

SMALL ENTITY OR

OTHER THAN SMALL ENTITY

RATE	ADDITIONAL FEE	OR	RATE	ADDITIONAL FEE
XS 9=		OR	XS18=	
X43=		OR	X86=	
+145=		OR	+290=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

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

	(Column 1)	(Column 2)	(Column 3)
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
	Total	Minus **	=
	Independent	Minus ***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <input type="checkbox"/>			

RATE	ADDITIONAL FEE	OR	RATE	ADDITIONAL FEE
XS 9=		OR	XS18=	
X43=		OR	X86=	
+145=		OR	+290=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

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

	(Column 1)	(Column 2)	(Column 3)
AMENDMENT C	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
	Total	Minus **	=
	Independent	Minus ***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <input type="checkbox"/>			

RATE	ADDITIONAL FEE	OR	RATE	ADDITIONAL FEE
XS 9=		OR	XS18=	
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.

BEST AVAILABLE COPY

D111 Rec'd P&T/PTO 26 MAR 2004

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of Art Unit

5 Sami Vaarala, Antti Nuopponen, Panu Pietikainen

Serial No.

10 Filed: Herewith

For: METHOD AND SYSTEM FOR ENSURING SECURE FORWARDING OF
MESSAGES

15 Examiner:

Date: 26 March 2004

20 PRELIMINARY AMENDMENT

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

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

In the specification:

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

--Prior Applications

35 This is a US national phase patent application that
claims priority from PCT/FI02/00771, filed 27 September 2002,
that claims priority from Finnish Patent Application No.
20011911, filed 28 September 2001.-

RP 290.1053USM 3/26/04

- 2 -

In the Claims:

Amend the claims as follows:

- 5
1. (Currently amended) A method Method for ensuring secure forwarding of a message in a telecommunication network, comprising at least one first terminal from which the message is sent and at least one other terminal to which the message
- 10 is sent, ~~characterized by the method comprising:~~ the method comprising:
- a) establishing one or more secure connections between different addresses of the first terminal and address of the other terminal, these connections defining at least said addresses of the two terminals,
- 15 b) the first terminal moving from one address to another address, and
- c) registering a secure connection between said other address and the other terminal address ~~is registered~~ to be at least one of the active connections to be used.
- 20
2. (Currently amended) The method Method of claim 1, characterized in that a new secure connection between the other address of the first terminal and the address of the other terminal is formed for the registration in step c) if
- 25 such a secure connections does not already exist.
3. (Currently amended) The method Method of claim 1, characterized in that, the secure connection is established in step a) and ~~claim 2~~ by forming one or more Security Associations (SAs) using the IPsec protocols, ~~such as a~~
- 30 ~~bundle of SAs.~~
4. (Currently amended) The method of claim 1 Method of any of ~~claims 1-3~~, characterized in that the message to be forwarded
- 35 consists of IP packets.

RF 290.1053USM 3/26/04

- 3 -

- 5 5. (Currently amended) The method of claim 1 ~~Method of any of claims 1-4~~, characterized in that, after step b), when the first terminal intend to send a message from the address it has moved to it first checks whether a secure connection between the new address and the other terminal already exists.
- 10 6. (Currently amended) The method ~~Method~~ of claim 5, characterized in that the existence of the new secure connection is checked by means of a connection table.
- 15 7. (Currently amended) The method of claim 1 ~~Method of any of claims 1-6~~, characterized in that, in step c), the actual connection (s) to be used is/are registered by means of a signaling message or signaling message exchange between the mobile terminal and the other terminal.
- 20 8. (Currently amended) The method of claim 1 ~~Method of any of claims 1-6~~, characterized in that, the new (second) address of the mobile terminal is updated automatically by the other terminal when the first terminal sends a message from its new address.
- 25 9. (Currently amended) The method of claim 1 ~~Method of any of claims 1-8~~, characterized in that the a key exchange being a part of the forming of the secure connection in step a) and ~~claim 2~~ is performed manually.
- 30 10. (Currently amended) The method of claim 1 ~~Method of any of claims 1-8~~, characterized in that a key exchange being a part of the forming of the secure connection in step a) and claim 2 is performed with IKE or some other automated key exchange protocol.

35

RF 290.1053USN 3/26/04

- 4 -

11. (Currently amended) The method of claim 1 ~~Method of any of claims 1-10~~, characterized in that the secure connection between the new address of the first terminal and the other terminal is in step c) registered for immediate and/or later use.

12. (Currently amended) The method ~~Method~~ of claim 11, characterized in that the registration for later use is made by the other terminal in a connection table.

13. (Currently amended) The method of claim 3 ~~Method of any of claims 3-12~~, characterized in that when sending message through the secure connection IPSec transport mode is used to secure traffic between the mobile computer and the destination computer.

14. (Currently amended) The method ~~Method~~ of claim 13, characterized in that a tunneling ~~tunnelling~~ protocol is used together with IPSec to provide a tunneling ~~tunnelling~~ capability.

15. (Currently amended) The method ~~Method~~ of claim 14, characterized in that where the Layer 2 Tunneling ~~Tunnelling~~ Protocol (L2TP) tunneling ~~tunnelling~~ protocol is used together with IPSec to provide a tunneling ~~tunnelling~~ capability.

16. (Currently amended) The method of claim 3 ~~Method of any of claims 3-15~~, characterized in that when sending message through the secure connection IPSec tunnel mode is used to secure traffic between the mobile computer and the destination computer.

17. (Currently amended) A system ~~System~~ for ensuring secure forwarding of a message in a telecommunication network,

RP 290.1053UBEN 3/26/04

- 5 -

comprising at least one first terminal from which the message
is sent and at least one other terminal to which the message
is sent, characterized by means for forming secure
connections between the address of the other terminal and
5 different addresses of the first terminal,
tables with lists of said secure connections, and
registrations means for forming such lists.

18. (Canceled)

10

RP 290.1053USN 3/26/04

- 6 -

In the Abstract:

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

5

--Abstract

The method is for ensuring secure forwarding of a message is performed in a telecommunication network that has at least one terminal from which the message is sent and at least one other terminal to which the message is sent. One or more
10 secure connections are established between different addresses of the first terminal and address of the other terminal. The connections define at least said addresses of the two terminals. When the first terminal moves from one address to another address, a secure connection, which
15 endpoints are the new address of the first terminal and the address of the other terminal, is registered to be at least one of the active connections.--

RF 290.1053USN 3/26/04

- 7 -

REMARKS

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

5 The claims have been amended to better conform to US patent practice. Claim 18 has been canceled to facilitate the prosecution of this application. The claims contain no new matter.

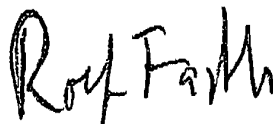
10 An abstract has been added to a separate page following the claims. The added abstract contains no new matter.

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

15 Respectfully submitted,

FASTH LAW OFFICES

20



Rolf Fasth
Registration No. 36,999

25

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

30

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

cc: Paivi Soderman
(Your ref: S00052US)

10/490933

DO/US WORKSHEET

International Appl No. FI02/00771

Application filed by: 20 months 30 months

INTERNATIONAL APPLICATION PAPERS IN THE APPLICATION FILE:

- International application (RECORD COPY)
- Article 19 amendments
- PCT/IB/331
- PCT/IPEA/409 IPER (PCT/IPEA/416 on front)
- Annexes to 409
- Priority document(s) No. _____
- INTERNATIONAL APPLICATION ON DOUBLE SIDED PAPER (COPIES MADE)
- Request form PCT/RO/101
- PCT/IB/302
- PCT/ISA/210-Search Report
- Search Report references
- Other _____

RECEIPTS FROM THE APPLICANT: (other than checked above)

- Basic National Fee (paid or authorized to charge)
- Preliminary amendment(s) filed
- Translation of international application as filed:
 - Description
 - Claims
 - Words in the drawing figure(s)
 - Article 19 amendments
 - Annexes to 409
- Oath / Declaration *Not Executed*
- DNA diskette
- Information Disclosure Statement
- Assignment document
- Power of attorney/Change of address
- Substitute specification
- Verified small status claim
- Other _____

Notes: Use IA from IB

No data sheet filed.

35 U.S.C. 371 - Receipt of Request (PTO-1390)

20 MAR 2004

Date acceptable oath / declaration received

18 Apr '05

Date complete 35 U.S.C 371 requirements met

"

102(e) Date

"

Date of completion of DO/EO 906 - Notification of Missing 102(e) Requirements

Date of completion of DO/EO 907 - Notification of Acceptance for 102(e) date

Date of completion of DO/EO 911 - Application accepted under 35 U.S.C. 1.11

Date of completion of DO/EO 905 - Notification of Missing Requirements

02 DEC '04

Date of completion of DO/EO 916 - Notification of Defective Response

Date of completion of DO/EO 903 - Notification of Acceptance

25 Apr '05

Date of completion of DO/EO 909 - Notification of Abandonment

WIPO Publication

Publication No. WO03/030488 A1

Publication Date

10 Apr '03

Publication Language

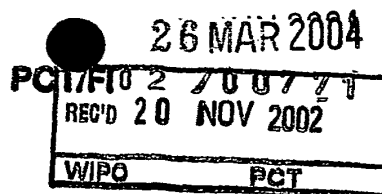
English

Not Published

- U.S. only
- Designated
- EP request

Screening done by: SA

Helsinki 5.11.2002



ETUOIKEUSTODISTUS
PRIORITY DOCUMENT



Hakija Applicant	IntraSecure Networks Oy Espoo
Patenttihakemus nro Patent application no	20011911
Tekemispäivä Filing date	28.09.2001
Kansainvälinen luokka International class	H04Q
Keksinnön nimitys Title of invention	

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

"Method and system for ensuring secure forwarding of messages"
(Menetelmä ja järjestelmä 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

Marketta Tehikoski
Apulaistarkastaja

**CERTIFIED COPY OF
PRIORITY DOCUMENT**

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 Puhelin: 09 6939 500 Telefax: 09 69 39 5328
P.O.Box 1160 Telephone: + 358 9 6939 500 Telefax: + 358 9 69 39 5328
FIN-00101 Helsinki, FINLAND

METHOD AND SYSTEM FOR ENSURING SECURE FORWARDING OF MESSAGES

TECHNICAL FIELD

5

The method and system of the invention are intended to secure connections in telecommunication networks. Especially, the invention is meant to be used in wireless networks as a part of a mobile IP solution or an IPSec solution.

10

TECHNICAL BACKGROUND

15

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

20

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

25

In fixed networks, there exist solutions to fill the need to protect data and resources from disclosure, to guarantee the authenticity of data, and to protect systems from network based attacks. IPSec is one such technology by means of which security is obtained.

30

The IP security protocols (IPSec) provides the capability to secure communications 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 (as remote access IPSec

use), or to secure communication with other organisations, ensuring authentication and confidentiality and providing a key exchange mechanism. Even if some applications already have built in security protocols, the use of IPSec further enhances the security.

- 5 IPSec can encrypt and/or authenticate traffic at IP level. Traffic going in to a WAN is typically encrypted and/or authenticated and traffic coming from a WAN is decrypted and/or authenticated. IPSec is defined by certain documents, which contain rules for the IPSec architecture.
- 10 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). Both AH and ESP are vehicles for access control based on the distribution of cryptographic keys and the management of
- 15 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-

20: way relationship is needed, then two security associations are required.

25: The term IPSec connection is used in what follows in place of an IPSec bundle of one or more security associations SAs, or a pair of IPSec bundles – one bundle for each direction – of one or more security associations. This term thus covers both

30: 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.

35: A security association is uniquely identified by three parameters. The first one, the Security Parameters Index (SPI), is a 32-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

40: 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.

5

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

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

Tunnel mode provides protection to the entire IP packet and is used for sending messages through more than two components. 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 setup 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 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 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 involving encapsulation of the packet in an outer IP header. The source IP address of this outer IP packet 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 and selected fields of the outer IP header.

20:

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. IKE is based on the Diffie-Hellman key exchange algorithm, and supports RSA signature authentication among other modes. IKE is easily extensible for future and vendor-specific features without breaking backwards compatibility.

30: The IPSec protocol solves the known security problems of the Internet Protocol (IP) in a satisfactory manner. However, it is designed for a static Internet, where the hosts using IPSec are relatively static. Thus, IPSec does not work well with mobile devices.

For instance, if a mobile terminal moves from one network to another, an IPSec connection set up is required, typically using the IKE key exchange protocol. Such a set up is expensive in terms of latency, since IKE may require several seconds to complete. It is also expensive in terms of computation, because the Diffie-Hellman and authentication-related calculations of IKE are extremely time consuming.

Routing means moving information across an internetwork from one source to another. Along the way, usually at least one intermediate node is encountered. Routing involves both the determination of the optimal routing path and the transport of information packets. To aid the routing of information packets, routing algorithms initialise and maintain routing tables, which contain route information. Routers communicate with each other and maintain their routing tables through the transmission of a variety of messages. The routing update message is one such message that generally consists the whole or part of a routing table.

The fundamental problem with IP mobility is the fact that IP routing is based on fixed addresses. The address space has been divided into subnetworks, that reside in practically fixed locations with respect to network topology (the routing can be changed, but that is a slow process, possibly in the order of minutes). When a mobile host moves away from its home network (where its IP address is proper), there is a problem with the routing of the packets to the new location if the IP network in question does not support such movement.

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.

Standard Mobile IP for IPv4 utilises e.g. IP-IP and Generic Routing Encapsulation (GRE) tunnelling to overcome this problem (See more details in figure 1 with accompanying text). There are also other methods of tunnelling, and hence, IP-IP and GRE tunnelling are used only as examples in this text. Mobile IPv4 has two modes of operation. In the co-located care-of address mode the mobile terminal performs IP-IP

encapsulation and decapsulation. This mode requires a borrowed address - the co-located care-of address - from the visited network. The other mode is the foreign agent mode, where the IP-IP or other tunnelling is performed by a special host in the visited network, called the Foreign Agent (FA). The mobile terminal communicates directly
5 with the FA (an IP address is not required for this direct communication), and does not require a borrowed address in this mode.

In IP-IP tunnelling, an IP address (the so called co-located care-of address) is borrowed from a network being visited. This address is topologically correct, i.e.
10 routable from other parts of the network. When a mobile terminal needs to send a packet to a given target computer, it first constructs an IP packet, whose source address is its home address, i.e. the address that is not topologically correct in the new network, and whose destination address is the target computer.

15 Since this packet may not be directly routable, it is encapsulated into another IP packet (by so called IP-IP encapsulation, or IP-IP tunnelling). The source address of this IP packet is the care-of address, and the target address is the so called home server of the mobile terminal. Upon receiving such an encapsulated packet, the home server unwraps the IP-IP tunnel, and proceeds to route the packet, which was inside the
20 encapsulation.

Reverse packets from the target computer to the mobile terminal are handled similarly;
the packet is first routed to the home server, then encapsulated in IP-IP and delivered
to the current network the mobile terminal is in. The current mobility binding
25 determines which current care-of address matches a given home address. (There may also be so-called simultaneous bindings, in which case the home address matches a set of care-of addresses; the packet is encapsulated and sent to each care-of address separately.)

30 When the mobile terminal moves to a new network, an authenticated signalling message exchange is done between the mobile terminal and the home server. A Registration Request is sent by the mobile terminal to the home server, requesting an

update of the current mobility binding. The server responds using a Registration Reply that may either accept or deny the request. When the Foreign Agent mode of operation is used, the registration messages go through the Foreign Agent.

5 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
10 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.

15 The IPSec protocol solves the known security problems of the Internet Protocol (IP) in a satisfactory manner. However, it is designed for a static Internet, where the hosts using IPSec are relatively static. Thus, IPSec does not work well with mobile devices. For instance, if a mobile terminal moves from one network to another, an IPSec connection set up is required, typically using the IKE key exchange protocol. Such a
20 set up is expensive in terms of latency, since IKE may require several seconds to complete. It is also expensive in terms of computation, because the Diffie-Hellman and authentication-related calculations of IKE are extremely time consuming.

25 The above description presents the essential ideas of Mobile IP.

The mobile IP approach of prior art has some disadvantages and problems.

30 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. In the manual prior art key management, the signalling authentication mechanism requires the mobile host and the home server to share a secret authentication key and the distribution of that key, which is carried out manually, is not very practical. Finally, the current Mobile IP protocol does not define a method for working through Network Address Translation (NAT) devices.

Said problem with Network Address Translation (NAT) devices, even if NAT devices are able to translate addresses of private networks in messages to public IP addresses so that the messages can be sent through internet, is, however, that currently no standard for making Mobile IP work through NAT devices. NAT devices are widely deployed because the use of private addresses requires less public IP addresses than would otherwise be needed.

REFERENCES

The following is a list of useful references for understanding the technology behind the invention.

IP in general, UDP and TCP:

[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.

5 <ftp://ftp.isi.edu/in-notes/rfc793.txt>

[RFC826]

D.C. Plummer, *An Ethernet Address Resolution Protocol*, RFC 826, November 1982.

10 <ftp://ftp.isi.edu/in-notes/rfc826.txt>

[RFC2460]

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

15

Mobile IP; IP-IP; DHCP:

[RFC2002]

C. Perkins, *IP Mobility Support*, RFC 2002, October 1996.

20 <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>

25

[RFC2131]

R. Droms, *Dynamic Host Configuration Protocol*, RFC 2131, March 1997.

<ftp://ftp.isi.edu/in-notes/rfc2131.txt>

30

[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.

5 [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.

10

IPSec standards:

[RFC2401]

15

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

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

[RFC2402]

20

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

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

[RFC2403]

25

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

[RFC2404]

30

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>

5

[RFC2407]

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

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

10

[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>

15

[RFC2409]

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

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

20

[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
5 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.

10 <ftp://ftp.isi.edu/in-notes/rfc3022.txt>

THE OBJECT OF THE INVENTION

15

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

20 SUMMARY OF THE INVENTION

25

The method of the invention for ensuring secure forwarding of a message is performed in a telecommunication network, comprising at least one terminal from which the message is sent and at least one other terminal to which the message is sent. In the method, one or more secure connections are established between different addresses of the first terminal and address of the other terminal, the connections defining at least said addresses of the two terminals. When the first terminal moves from one address to another address, a secure connection, whose endpoints are the new address of the first terminal and the address of the other terminal, is registered to be at least one of the active connections.

30

If there does not already exist such a secure connection between the new address and the other terminal, a new secure connection between the new address and the other terminal address has to be formed.

- 5 The terminals might have several active connections. In the invention, the terminal might in one embodiment also have only one secure active connection at a time, which can be changed in according with the invention to be defined to be between the address the terminal moves to and the address of the other terminal.
- 10 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 invention is moreover concerned with a system, which is able to perform the method of the invention. The characteristics of the system are defined by the system
15 main claim, the subclaim defining the functions that can be performed by the system of the invention.

The secure connections are preferably established by forming Security Associations (SAs) using the IPSec protocols and the message to be forwarded consists of IP
20 packets. The key exchange being a part of the forming of a secure connection is performed manually or automatically with IKE or some other automated key exchange protocol.

When a new secure connection is formed, it is registered for immediate and/or later
25 use. The registration for later use is made using a connection table, which is maintained by both hosts participating in the forming of the secure connection. The connection table is also used e.g. when the first terminal moves, and needs to determine whether a secure tunnel already exists for the new address. The table can be e.g. a Security Association DataBase (SADB), which is the nominal place to store
30 IPSec SAs in the IPSec model.

In the preferred embodiment, IPSec security associations are used as secure connections. The table, through which the existence of a given IPSec SA (in either the first terminal or the other terminal) is determined, is then the IPSec Security Association DataBase (SADB).

5

The actual connection(s) to be used is registered by means of a signalling message or signalling message exchange between the first terminal and the other terminal, for example by means of Registration Request and possibly Registration Reply messages.

10

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.

15

20

The new address of the first terminal can also be updated automatically by the other terminal when the first terminal sends a message from its new address.

25

30

35

40

45

50

55

60

65

70

75

80

85

The active SA is a stored mobility binding that maps a given terminal address to one or more IPSec tunnel mode SAs (or zero such SAs, if the terminal in question is not connected). These mobility bindings are manipulated when Registration Request and Registration Reply messages are processed when sending packets to the first terminal. It is possible to restrict traffic from the first terminal to only the IPSec SAs that are currently registered in the mobility binding, but allowing traffic from all shared SAs is also reasonable.

The mobility binding is necessary, since each of the shared IPSec security associations is valid for securing traffic. There has to be some way for the first terminal

to determine which security association(s) to actually use when processing packets. The mobility binding serves this purpose in the invention.

5 The first terminal may use any IPsec tunnel SA it shares with the other terminal. It is possible to restrict traffic from the first terminal to only the IPsec SAs that are currently registered, but this is not an essential feature. Thus, the first terminal may use any IPsec tunnel SA it shares with the other terminal when sending packets. The other terminal may restrict traffic only to IPsec SAs that are currently active in the mobility binding, but allowing traffic from all shared SAs is also reasonable.

10

The invention can be used for direct end-to-end communication, in which case the secure tunnel is established between these end computers. If applied to IPsec, this could correspond to either an IPsec transport mode or tunnel mode SA. The message might also be sent first to an intermediate computer, whereby the outer address of the IPsec tunnel is unwrapped by the intermediate computer and the message is forwarded as plain text to the end destination computer.

15

Thus, in the solution of the invention, an IPsec security association is used instead of the IP-IP tunnelling. The invention can also be used for tunnelling with IPsec transport mode and an external tunnelling mechanism, such as Layer 2 Tunnelling Protocol (L2TP).

20:

:

:

:

:

25:

:

:

:

:

30:

:

:

The invention provides the following advantages.

25: IPsec key management and strong authentication can be leveraged for this application involving asymmetric (RSA) authentication, the use of the Diffie-Hellman key exchange algorithm, the possibility to use certificates etc.

30: The IPsec symmetric encryption and authentication methods can be used to protect both signalling and data traffic. This provides confidentiality and integrity and any future developments of IPsec can be taken advantage of.

The NAT traversal problem can be solved by using any available NAT traversal mechanisms for IPsec. One is currently being standardised for IPsec, but any other IPsec NAT traversal mechanism may be used.

- 5 The invention can be used in different networks, such as IPv4 and IPv6.

In the following the invention is described more in detail by means of an advantageous embodiment in an example network but is not restricted to the details thereof.

10

FIGURES

Figure 1 describes the mobile IP tunnelling of prior art by means of a signalling diagram

15

Figure 2 describes the method of the invention by means of a signalling diagram

DETAILED DESCRIPTION

20:

20: The data communication in figure 1 takes place from a mobile terminal to a target host
 25: X via an intermediate computer, which works as a home server for host X.

30:

30: Packets sent from the home address of the mobile terminal can be directly routed to
 35: the target address X by the intermediate computer, since the home address is
 40: registered in routing tables by means of which the routing takes place.

45:

45: Figure 1 describes a method of prior art, wherein IP-IP tunnelling is used for routing
 50: data packets when the mobile host moves from one address to another, i.e. from the
 55: home address to a new address.

60:

65:

70:

Mobile IP also supports the so-called triangular routing mode, where the packets sent by the mobile terminal are routed directly to the recipient of the packet, bypassing the home server, while packets sent to the mobile terminal are first routed to the home server and then IP-IP tunnelled to the mobile terminal. This mode is more efficient, but is incompatible with so-called ingress filtering routers, which do not route IP packets whose source addresses are topologically incorrect, as is the case with a mobile terminal that is away from the home network. The details of this mode are different, but the general idea is the same. The more general case where IP-IP tunnelling is used for traffic between the mobile terminal and the home server in both directions is discussed in the following text.

In figure 1, when a mobile terminal being in a visited network intends to send a packet to a target host X using its current care-of address, which is an address borrowed from the visited network, it first constructs a data packet, whose source address is its home address – which is not a topologically correct address in the current network the mobile terminal is in – and whose destination address is X. Because the source address of the packet is topologically incorrect, i.e., does not belong to the network the mobile terminal is in, some routers, especially the ones that implement the so-called ingress filtering algorithm, will not route the packet properly. To overcome this, the packet is encapsulated into another IP packet; this process is called IP-IP tunnelling or IP-IP encapsulation. The new, outer IP header source address is the care-of address from the visited network – which is a topologically correct address – and the outer IP header destination address is the home server of the mobile terminal. Thus, the inner IP header source address is the home address of the mobile terminal, while the inner IP header destination address is that of the host X. This is indicated in figure 1 with IP | IP | data, which describes a message containing data and the original IP header, which is encapsulated further in an outer IP header for routing purposes. This IP packet is then sent to the home server in step 1 of figure 1.

Upon receiving the encapsulated IP packet, the home server unwraps the IP-IP tunnel, and proceeds in step 2 of figure 2 with routing a packet indicated with IP/Data, which packet was inside the encapsulation (inside the outer IP header). The routing is

performed in accordance with the inner destination address, the packet now, after the unwrapping, having the home address of the mobile terminal as its source address and host X as its destination address.

5 Reverse packets from X to the mobile terminal are handled similarly; the packet is first routed to the home server in step 3, then encapsulated in IP-IP and delivered to the current network (in step 4) the mobile terminal is in. The mobility binding determines which care-of address(es) the packet is forwarded to.

10 In the method of the invention, an IPSec tunnel mode or transport mode security association is used instead of the IP - IP tunnelling. Figure 2 describes an example of the method of the invention for sending messages when a mobile terminal moves to a new address.

15 A secure connection, preferably an IPSec security association (SA) or more specifically one IPsec SA bundle for each direction of communication is established between the care-of-address and the home server address, e.g. the care-of-address of the mobile terminal and the home server address. The SA can also include additional parameters and attributes, possibly relating to standard or non-standard IPSec
:20 extensions, such as NAT traversal, which are conventionally used in SAs. A message to be sent through this tunnel is marked IP/IPSec/IP/Data in figure 2, illustrating that
:25 the message contains a data part with a destination IP address and can be sent through an IPSec tunnel, while encapsulated with an outer IP header.

Reverse packets from X to the mobile terminal are handled similarly; the packet is first
:25 routed to the home server in step 3, then IPSec processed using the IPSec tunnel mode SA, during which an outer IP header is added to the packet and delivered to the current network(s) (in step 4) the mobile terminal is in.

30 When IPSec transport mode is used, the mobile terminal may either communicate directly with the home server, or alternatively some external tunnelling protocol (apart from IPSec tunnelling) can be used to allow routing of packets further. For example,

the Layer 2 Tunnelling Protocol (L2TP) can be used with IPSec transport mode to provide functionality similar to IPSec tunnelling.

5 When the mobile terminal moves to a new network, it first obtains a care-of address from the visited network. The mobile terminal then checks whether an SA (or more precisely, a pair of SA bundles) SA already exists between the new care-of address and the home server address.

10 This check is normally done by inspecting the contents of a Security Association DataBase (SADB), as specified by the IPSec protocol. The actual implementation may somewhat deviate from the nominal processing. The nominal model and the actual operations often are in reality somewhat different (for instance, hardware IPSec implementations have a radically different "SADB" implementation than simple lookup.)
15 If an IPSec security association (SA) between the mobile terminal and the home server defining the care-of address of the mobile terminal at one end (the new address of the mobile terminal) and the address of the home server at the other end already exists, this SA is registered to be the actual SA to be used.

20 This happens by means of a signalling message or signalling message exchange done between the mobile terminal and the home server, described by steps 5 and 6 in figure 2. The messages are preferably authenticated and/or encrypted by using IPSec, and preferably by using the same IPSec SA that is used for the ordinary traffic protection.
25 In some embodiments no reply is used. Step 5 is a registration request from the mobile host to the home server to register the new address and step 6 is a registration reply back to the mobile terminal.

30 When a SA does not exist between the new care-of address and the home server, an SA setup occurs between steps 4 and 5 of figure 2. This SA setup may be manual, or may involve some automatic key exchange protocol, such as the Internet Key Exchange (IKE).

Upon receiving the IPsec protected packet sent using the new SA, the home server processes the IPsec headers and uncovers the original packet from the IPsec tunnel, and then routes the IP packet to host X. If IPsec transport mode is used, the home server processes the IPsec headers and processes the resulting plaintext packet
 5 directly without routing it onwards. However, if an external tunnelling protocol, such as L2TP, is used, the tunnelling protocol may forward the packet after IPsec processing.

In figure 2, the RREQ and RREP messages are shown without IPsec protection. In an IPsec embodiment, the IPsec protected messages would be expressed e.g. as
 10 IP|IPsec|IP|RREQ resp. IP|IPsec|IP|RREP instead of IP|RREQ resp. IP|RREP. Thus, RREQ/RREP can be protected and one method of protection would be IPsec. If they are protected using IPsec, one can leverage the existing IPsec SA for that purpose. The IPsec protection of signalling message(s) may use either tunnel or transport mode.

15 The abbreviation RREQ in figure 2 stands for Registration Request while the abbreviation RREP stands for Registration Reply. These are preferably the Mobile IP Registration Request and Registration Reply messages, used in conjunction with IPsec in the invention, but other registration formats may be used. It is also within the
 20 scope of the invention to only use a Registration Request message (not necessarily using the exact Mobile IP format), but not using a Registration Reply message.

25 The invention also covers both the case wherein properly authenticated traffic is used as an implicit registration request, and a mobility binding update is performed automatically. As a specific example, an IPsec tunnel mode SA bundle, including an AH used for sending traffic, in which case the addresses of the outermost IP header
 30 are covered by AH authentication, is used between the mobile terminal and the home server. When the mobile terminal moves to a new network, it sends a data packet which may be an empty data packet if there is no data to send that is processed using the IPsec SA bundle and sent to the home server. Once the home server properly authenticates the message, including the outermost IP header, and determines that it
 35 is coming from an address that differs from the current mobility binding, it may update

the mobility binding automatically. Updating the binding results in that all subsequent packets being destined to the mobile terminal, will be sent using the updated mobility binding, i.e. the new address that the client is using. Thus, no explicit mobility binding update signalling is required in this case.

5

The description of the invention above has been simplified for clarity of description. The invention can be extended in several ways without changing the underlying idea. Some extensions are described in what follows.

10 The Mobile IP concept of simultaneous bindings, and associated traffic n-casting from the home server to the mobile terminal can be used. In this case, packets sent towards the mobile terminal would be processed using several IPsec SAs, one for each simultaneous registration, and sent to the different visited networks used by the mobile terminal. The registration message(s) in this case contain fields that indicate
15 how the mobility binding is to be modified, e.g. whether to replace existing bindings, or to add a new binding in addition to the existing ones. The implicit registration based on data packets can also be used, possibly together with registration message(s) to maintain the bindings.

20 When an IPsec SA does not exist between the new care-of address and the home server address, and an IPsec SA is set up e.g. using an automated key exchange protocol, the completion of the SA setup can be used as an implicit registration, removing the additional registration in steps 5 and possibly 6 in figure 2.

25 When in the above "a Security Association SA" or "a bundle of Security Associations SAs" is referred to, this means in practice, an IPsec SA bundle in both cases – one or more IPsec security associations applied in sequence – can be used for each direction of traffic.

30 The invention is not specific to IPv4 or IPv6, and can be used with Mobile IP for IPv4 and Mobile IP for IPv6. The invention is also straightforward to extend to future IPsec versions

CLAIMS

1. Method for ensuring secure forwarding of a message in a telecommunication network, comprising at least one first terminal from which the message is sent and
5 at least one other terminal to which the message is sent,

characterized by

- a) establishing one or more secure connections between different addresses of the first terminal and address of the other terminal, these connections defining at least said addresses of the two terminals,
- 10 b) the first terminal moving from one address to another address,
- c) a secure connection between said other address and the other terminal address is registered to be at least one of the actual connections to be used.

2. Method of claim 1, characterized in that a new secure connection between
15 the other address of the first terminal and the address of the other terminal is formed for the registration in step c) if such a secure connections does not already exist.

3. Method of claim 1, characterized in that, the secure connection is
20 established in step a) and claim 2 by forming one or more Security Associations (SAs) using the IPSec protocols, such as a bundle of SAs.

4. Method of any of claims 1 - 3, characterized in that the message to be
forwarded consists of IP packets.

5. Method of any of claims 1 - 4, characterized in that, after step b), when the
first terminal intend to send a message from the address it has moved to it first checks whether a secure connection between the new address and the other
terminal already exists.

6. Method of claim 5, characterized in that the existence of the new secure
connection is checked by means of a connection table.

7. Method of any of claims 1 - 6, characterized in that, in step c), the actual connection(s) to be used is/are registered by means of a signalling message or signalling message exchange between the mobile terminal and the other terminal.

5 8. Method of any of claims 1 - 6, characterized in that, the new (second) address of the mobile terminal is updated automatically by the other terminal when the first terminal sends a message from its new address.

9. Method of any of claims 1 - 8, characterized in that the a key exchange
10 being a part of the forming of the secure connection in step a) and claim 2 is performed manually.

10. Method of any of claims 1 - 8, characterized in that a key exchange being a
15 part of the forming of the secure connection in step a) and claim 2 is performed with IKE or some other automated key exchange protocol.

11. Method of any of claims 1 - 10, characterized in that the secure connection
between the new address of the first terminal and the other terminal is in step c)
registered for immediate and/or later use.

20

12. Method of claim 11, characterized in that the registration for later use is
made by the other terminal in a connection table.

25

13. Method of any of claims 3 - 12, characterized in that when sending
message through the secure connection IPSec transport mode is used to secure
traffic between the mobile computer and the destination computer.

30

35

14. Method of claim 13, characterized in that a tunnelling protocol is used
together with IPSec to provide a tunnelling capability.

40

45

50

55

15. Method of claim 14, characterized in that where the Layer 2 Tunnelling Protocol (L2TP) tunnelling protocol is used together with IPsec to provide a tunnelling capability.

5 16. Method of any of claims 3 – 15, characterized in that when sending message through the secure connection IPsec tunnel mode is used to secure traffic between the mobile computer and the destination computer.

10 17. System for ensuring secure forwarding of a message in a telecommunication network, comprising at least one first terminal from which the message is sent and at least one other terminal to which the message is sent,
characterized by
means for forming secure connections between the address of the other terminal and different addresses of the first terminal,
15 tables with lists of said secure connections, and
registrations means for forming such lists.

18. System of claim 17, characterized in that it has means for performing the method of any of claims 1 - 16.

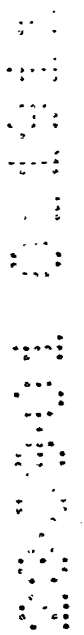
20



ABSTRACT

The invention is concerned with a method for ensuring secure forwarding of a message is performed in a telecommunication network, comprising at least one terminal from which the message is sent and at least one other terminal to which the message is sent. In the method, one or more secure connections are established between different addresses of the first terminal and address of the other terminal, the connections defining at least said addresses of the two terminals. When the first terminal moves from one address to another address, a secure connection, whose endpoints are the new address of the first terminal and the address of the other terminal, is registered to be at least one of the active connections.

FIG. 2



280901 011911

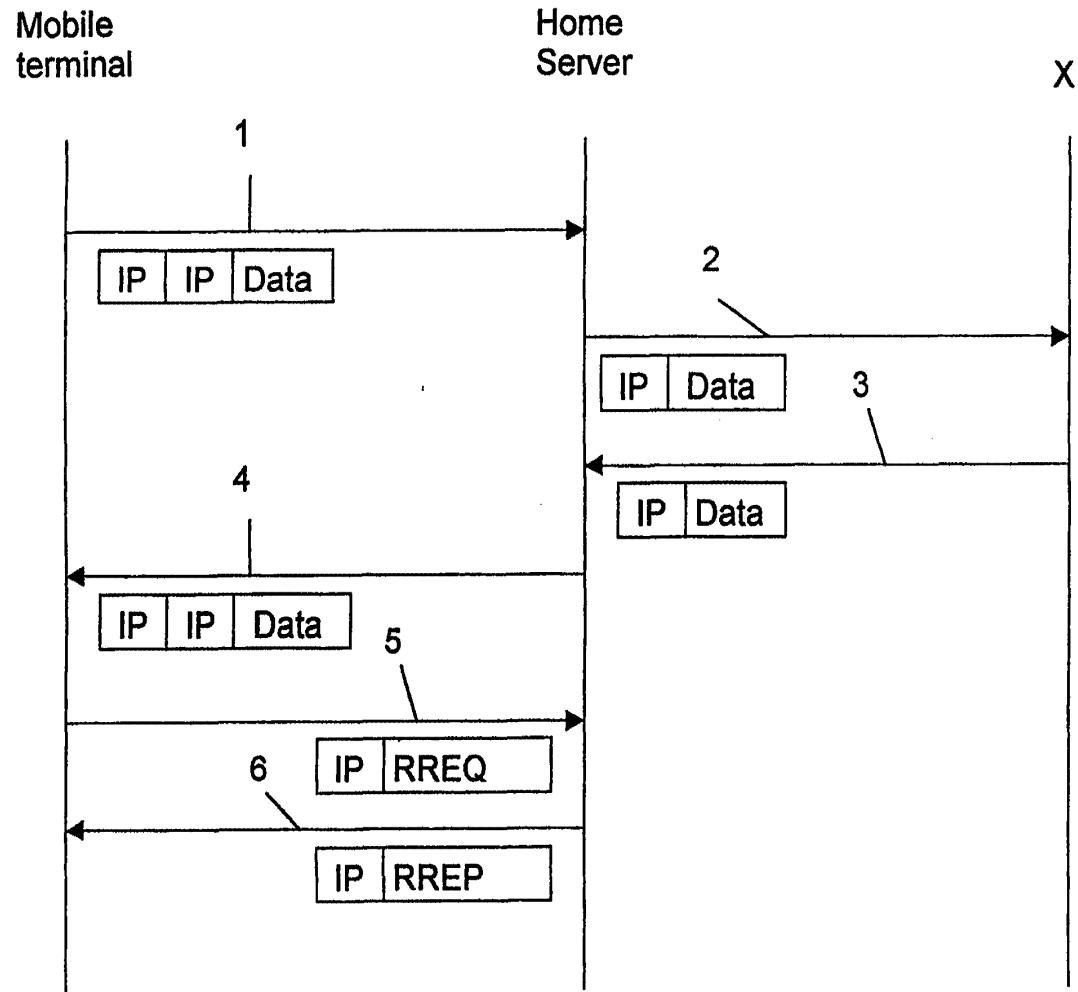


FIG. 1

1/2

26

0070

280901 011911

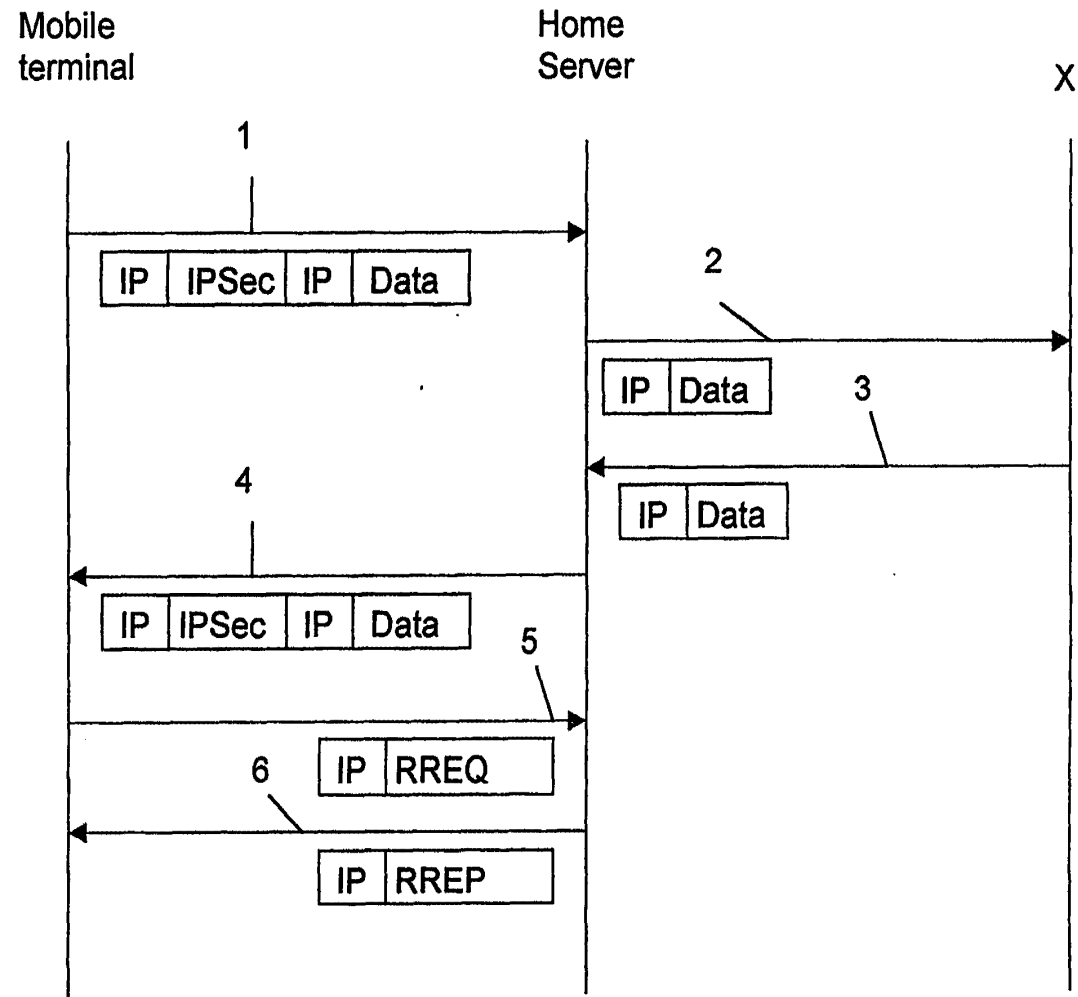


FIG. 2

2/2

26

0071

REC'D 19 SEP 2003

PCT

WIPO PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT
(PCT Article 36 and Rule 70)

26 MAR 2004

Applicant's or agent's file reference S0052PCT	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/PEA/416)	
International application No. PCT/FI02/00771	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 5 sheets, including this cover sheet.

This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 3 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 25.04.2003	Date of completion of this report 17.09.2003
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 

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. **PCT/F102/00771**

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

1-21 as originally filed

Claims, Numbers

1-18 received on 10.07.2003 with letter of 07.07.2003

Drawings, Sheets

1/2-2/2 as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language: , which is:

- the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
 - the language of publication of the international application (under Rule 48.3(b)).
 - the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).
3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:
- contained in the international application in written form.
 - filed together with the international application in computer readable form.
 - furnished subsequently to this Authority in written form.
 - furnished subsequently to this Authority in computer readable form.
 - The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
 - The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.
4. The amendments have resulted in the cancellation of:
- the description, pages:
 - the claims, Nos.:
 - the drawings, sheets:

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. **PCT/FI02/00771**

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	1-18
	No: Claims	
Inventive step (IS)	Yes: Claims	1-18
	No: Claims	
Industrial applicability (IA)	Yes: Claims	1-18
	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. It is considered that independent claims 1 (method) and 17 (apparatus) relate to new and inventive subject-matter (Articles 33 (2) and (3) PCT), since the prior art does not disclose or suggest the specifically claimed method for ensuring secure forwarding of a message in a telecommunication network according to claim 1 and does not disclose or suggest the specifically claimed system for ensuring secure forwarding of a message in a telecommunication network according to claim 17.

Document D2=WO 00/41427 discloses a method for accomplishing handover for a mobile unit from a first stationary unit to a second stationary unit; the Security Association SA in D2 is reused literally when the terminal moves. In D2 the same SA can be transferred and reused because the terminal only moves within one administrative domain. Thus the first stationary unit in the other end has a common IP address as the second stationary unit which now is the end-point. An SA is always defined by its destination address but in D2 the destination address in the SA did not have to be changed as the other terminal always is an access point in the same network domain.

Document D1= WO 01/39538 discloses a method of providing information security when communication with a given mobile terminal is handed-over from a first access point to a second access point; in D1 (as in D2) the SA is also reused literally when the terminal moves. In D1 the SA is maintained when a handover occurs within the network. The SA is there transferred (and not redefined) and there are only one SA that exists between the terminal and the other endpoint that always is an access point in the same network. The same parameters of the SA are transferred.

In the present invention (method claim 1 and corresponding apparatus claim 17) there is established several secure connections, each of which defines different addresses. One or more of them is then registered to be the active(s) one upon moving of the first terminal. Then no renegotiation or reestablishing of any SA is needed when the first terminal moves from one point to another.

In the present invention a different SA defining a different address has to be used when the first terminal moves, and the other terminal can be any other terminal. The question is here, as it is clearly indicated in present claim 1, about using

different secure connections, not reusing them.

In the present invention there is question about different SAs each defining different addresses.

2. Dependent claims 2 to 16 and 18 contain further details of the method of claim 1 and of the system of claim 17 respectively. As they are dependent on claims 1 and 17 respectively, they also satisfy the requirements for novelty and inventive step (Articles 33 (2) and (3) PCT).

CLAIMS

1. Method for ensuring secure forwarding of a message in a telecommunication network, comprising at least one first terminal from which the message is sent and
5 at least one other terminal to which the message is sent,
c h a r a c t e r i z e d b y
 - a) establishing one or more secure connections between different addresses of the first terminal and address of the other terminal, these connections defining at least said addresses of the two terminals,
 - 10 b) the first terminal moving from one address to another address,
 - c) a secure connection between said other address and the other terminal address is registered to be at least one of the actual connections to be used.
2. Method of claim 1, c h a r a c t e r i z e d in that a new secure connection between
15 the other address of the first terminal and the address of the other terminal is formed for the registration in step c) if such a secure connections does not already exist.
3. Method of claim 1, c h a r a c t e r i z e d in that, the secure connection is
20 established in step a) and claim 2 by forming one or more Security Associations (SAs) using the IPSec protocols, such as a bundle of SAs.
4. Method of any of claims 1 - 3, c h a r a c t e r i z e d in that the message to be
25 forwarded consists of IP packets.
5. Method of any of claims 1 - 4, c h a r a c t e r i z e d in that, after step b), when the first terminal intend to send a message from the address it has moved to it first checks whether a secure connection between the new address and the other terminal already exists.
30
6. Method of claim 5, c h a r a c t e r i z e d in that the existence of the new secure connection is checked by means of a connection table.

7. Method of any of claims 1 - 6, characterized in that, in step c), the actual connection(s) to be used is/are registered by means of a signalling message or signalling message exchange between the mobile terminal and the other terminal.
- 5 8. Method of any of claims 1 - 6, characterized in that, the new (second) address of the mobile terminal is updated automatically by the other terminal when the first terminal sends a message from its new address.
9. Method of any of claims 1 - 8, characterized in that the a key exchange
10 being a part of the forming of the secure connection in step a) and claim 2 is performed manually.
10. Method of any of claims 1 - 8, characterized in that a key exchange being a
15 part of the forming of the secure connection in step a) and claim 2 is performed with IKE or some other automated key exchange protocol.
11. Method of any of claims 1 - 10, characterized in that the secure connection
20 between the new address of the first terminal and the other terminal is in step c) registered for immediate and/or later use.
12. Method of claim 11, characterized in that the registration for later use is
made by the other terminal in a connection table.
13. Method of any of claims 3 - 12, characterized in that when sending
25 message through the secure connection IPSec transport mode is used to secure traffic between the mobile computer and the destination computer.
14. Method of claim 13, characterized in that a tunnelling protocol is used
30 together with IPSec to provide a tunnelling capability.

15. Method of claim 14, characterized in that where the Layer 2 Tunnelling Protocol (L2TP) tunnelling protocol is used together with IPSec to provide a tunnelling capability.
- 5 16. Method of any of claims 3 – 15, characterized in that when sending message through the secure connection IPSec tunnel mode is used to secure traffic between the mobile computer and the destination computer.
- 10 17. System for ensuring secure forwarding of a message in a telecommunication network, comprising at least one first terminal from which the message is sent and at least one other terminal to which the message is sent,
characterized by
means for forming secure connections between the address of the other terminal and different addresses of the first terminal,
15 tables with lists of said secure connections, and
registrations means for forming such lists.
18. System of claim 17, characterized in that it has means for performing the
method of any of claims 1 - 16.

490, 933

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

(19) World Intellectual Property Organization
International Bureau



26 MAR 2004



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

PCT

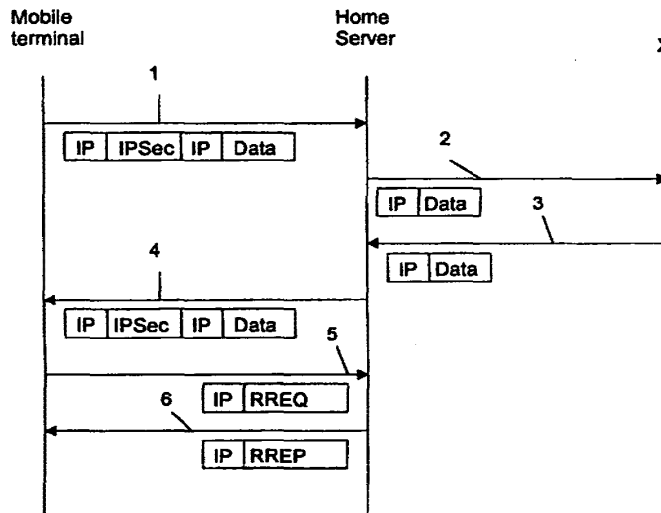
(10) International Publication Number
WO 03/030488 A1

- (51) International Patent Classification?: H04L 29/06, H04Q 7/38
- (74) Agent: INNOPAT LTD; P.O. Box 556, FIN-02151 Espoo (FI).
- (21) International Application Number: PCT/FI02/00771
- (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.
- (22) International Filing Date: 27 September 2002 (27.09.2002)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data: 20011911 28 September 2001 (28.09.2001) FI
- (84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, 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).
- (71) Applicant (for all designated States except US): IN-TRASECURE NETWORKS OY [FI/FI]; P.O. Box 38, FIN-02210 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). PIETIKÄINEN, Panu [FI/FI]; Täysikuu 10 C 103, FIN-02210 Espoo (FI).

Published: — with international search report

[Continued on next page]

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



(57) Abstract: The invention is concerned with a method for ensuring secure forwarding of a message is performed in a telecommunication network, comprising at least one terminal from which the message is sent and at least one other terminal to which the message is sent. In the method, one or more secure connections are established between different addresses of the first terminal and address of the other terminal, the connections defining at least said addresses of the two terminals. When the first terminal moves from one address to another address, a secure connection, whose endpoints are the new address of the first terminal and the address of the other terminal, is registered to be at least one of the active connections.

WO 03/030488 A1

WO 03/030488 A1



For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD AND SYSTEM FOR ENSURING SECURE FORWARDING OF MESSAGES**TECHNICAL FIELD**

5

The method and system of the invention are intended to secure connections in telecommunication networks. Especially, the invention is meant to be used in wireless networks as a part of a mobile IP solution or an IPSec solution.

10

TECHNICAL BACKGROUND

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

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

In fixed networks, there exist solutions to fill the need to protect data and resources from disclosure, to guarantee the authenticity of data, and to protect systems from network based attacks. IPSec is one such technology by means of which security is obtained.

The IP security protocols (IPSec) provides the capability to secure communications 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 (as remote access IPSec

use), or to secure communication with other organisations, ensuring authentication and confidentiality and providing a key exchange mechanism. Even if some applications already have built in security protocols, the use of IPSec further enhances the security.

5 IPSec can encrypt and/or authenticate traffic at IP level. Traffic going in to a WAN is typically encrypted and/or authenticated and traffic coming from a WAN is decrypted and/or authenticated. IPSec is defined by certain documents, which contain rules for the IPSec architecture.

10 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). Both AH and ESP are vehicles for access control based on the distribution of cryptographic keys and the management of
15 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-
20 way relationship is needed, then two security associations are required.

The term IPSec connection is used in what follows in place of an IPSec bundle of one or more security associations SAs, or a pair of IPSec bundles – one bundle for each direction – of one or more security associations. This term thus covers both
25 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
30 Security Parameters Index (SPI), is a 32-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.

5

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
10 communication between two hosts. Transport mode may be used in conjunction with a tunnelling protocol (other than IPSec tunnelling).

Tunnel mode provides protection to the entire IP packet and is used for sending messages through more than two components. Tunnel mode is often used when one
15 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 setup by the IPSec software in the firewall or secure router at boundary of
20 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
25 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
30 "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 AH protection. AH also protects parts of the outer header, in addition to the whole inner packet.

5 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 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 involving
10 encapsulation of the packet in an outer IP header. The source IP address of this outer IP packet 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
15 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 and selected fields of the outer IP header.

20

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
25 (IKE) is a newer name for the ISAKMP/Oakley. IKE is based on the Diffie-Hellman key exchange algorithm, and supports RSA signature authentication among other modes. IKE is easily extensible for future and vendor-specific features without breaking backwards compatibility.

30 The IPsec protocol solves the known security problems of the Internet Protocol (IP) in a satisfactory manner. However, it is designed for a static Internet, where the hosts using IPsec are relatively static. Thus, IPsec does not work well with mobile devices.

For instance, if a mobile terminal moves from one network to another, an IPSec connection set up is required, typically using the IKE key exchange protocol. Such a set up is expensive in terms of latency, since IKE may require several seconds to complete. It is also expensive in terms of computation, because the Diffie-Hellman and authentication-related calculations of IKE are extremely time consuming.

Routing means moving information across an internetwork from one source to another. Along the way, usually at least one intermediate node is encountered. Routing involves both the determination of the optimal routing path and the transport of information packets. To aid the routing of information packets, routing algorithms initialise and maintain routing tables, which contain route information. Routers communicate with each other and maintain their routing tables through the transmission of a variety of messages. The routing update message is one such message that generally consists the whole or part of a routing table.

The fundamental problem with IP mobility is the fact that IP routing is based on fixed addresses. The address space has been divided into subnetworks, that reside in practically fixed locations with respect to network topology (the routing can be changed, but that is a slow process, possibly in the order of minutes). When a mobile host moves away from its home network (where its IP address is proper), there is a problem with the routing of the packets to the new location if the IP network in question does not support such movement.

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.

Standard Mobile IP for IPv4 utilises e.g. IP-IP and Generic Routing Encapsulation (GRE) tunnelling to overcome this problem (See more details in figure 1 with accompanying text). There are also other methods of tunnelling, and hence, IP-IP and GRE tunnelling are used only as examples in this text. Mobile IPv4 has two modes of operation. In the co-located care-of address mode the mobile terminal performs IP-IP

encapsulation and decapsulation. This mode requires a borrowed address - the co-located care-of address - from the visited network. The other mode is the foreign agent mode, where the IP-IP or other tunnelling is performed by a special host in the visited network, called the Foreign Agent (FA). The mobile terminal communicates directly
5 with the FA (an IP address is not required for this direct communication), and does not require a borrowed address in this mode.

In IP-IP tunnelling, an IP address (the so called co-located care-of address) is borrowed from a network being visited. This address is topologically correct, i.e.
10 routable from other parts of the network. When a mobile terminal needs to send a packet to a given target computer, it first constructs an IP packet, whose source address is its home address, i.e. the address that is not topologically correct in the new network, and whose destination address is the target computer.

15 Since this packet may not be directly routable, it is encapsulated into another IP packet (by so called IP-IP encapsulation, or IP-IP tunnelling). The source address of this IP packet is the care-of address, and the target address is the so called home server of the mobile terminal. Upon receiving such an encapsulated packet, the home server unwraps the IP-IP tunnel, and proceeds to route the packet, which was inside the
20 encapsulation.

Reverse packets from the target computer to the mobile terminal are handled similarly; the packet is first routed to the home server, then encapsulated in IP-IP and delivered to the current network the mobile terminal is in. The current mobility binding
25 determines which current care-of address matches a given home address. (There may also be so-called simultaneous bindings, in which case the home address matches a set of care-of addresses; the packet is encapsulated and sent to each care-of address separately.)

30 When the mobile terminal moves to a new network, an authenticated signalling message exchange is done between the mobile terminal and the home server. A Registration Request is sent by the mobile terminal to the home server, requesting an

update of the current mobility binding. The server responds using a Registration Reply that may either accept or deny the request. When the Foreign Agent mode of operation is used, the registration messages go through the Foreign Agent.

5 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
10 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.

15 The IPsec protocol solves the known security problems of the Internet Protocol (IP) in a satisfactory manner. However, it is designed for a static Internet, where the hosts using IPsec are relatively static. Thus, IPsec does not work well with mobile devices. For instance, if a mobile terminal moves from one network to another, an IPsec connection set up is required, typically using the IKE key exchange protocol. Such a
20 set up is expensive in terms of latency, since IKE may require several seconds to complete. It is also expensive in terms of computation, because the Diffie-Hellman and authentication-related calculations of IKE are extremely time consuming.

The above description presents the essential ideas of Mobile IP.

25

The mobile IP approach of prior art has some disadvantages and problems.

The standard Mobile IP protocol provides a mobile terminal with a mobile connection, and defines mechanisms for performing efficient handovers from one network to
30 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. In the manual prior art key management, the signalling authentication mechanism requires the mobile host and the home server to share a secret authentication key and the distribution of that key, which is carried out manually, is not very practical. Finally, the current Mobile IP protocol does not define a method for working through Network Address Translation (NAT) devices.

Said problem with Network Address Translation (NAT) devices, even if NAT devices are able to translate addresses of private networks in messages to public IP addresses so that the messages can be sent through internet, is, however, that currently no standard for making Mobile IP work through NAT devices. NAT devices are widely deployed because the use of private addresses requires less public IP addresses than would otherwise be needed.

15

REFERENCES

The following is a list of useful references for understanding the technology behind the invention.

20

IP in general, UDP and TCP:

[RFC768]

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

[RFC791]

30 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.

5 <ftp://ftp.isi.edu/in-notes/rfc793.txt>

[RFC826]

D.C. Plummer, *An Ethernet Address Resolution Protocol*, RFC 826, November 1982.

10 <ftp://ftp.isi.edu/in-notes/rfc826.txt>

[RFC2460]

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

15

Mobile IP; IP-IP; DHCP:

[RFC2002]

C. Perkins, *IP Mobility Support*, RFC 2002, October 1996.

20 <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>

25

[RFC2131]

R. Droms, *Dynamic Host Configuration Protocol*, RFC 2131, March 1997.

<ftp://ftp.isi.edu/in-notes/rfc2131.txt>

30 [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.

5 [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.

10

IPSec standards:

[RFC2401]

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

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

[RFC2402]

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

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

[RFC2403]

25 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.

30

[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>

5

[RFC2407]

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

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

10

[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>

15

[RFC2409]

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

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

20

[RFC2410]

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

25

[RFC2411]

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

30

[RFC2412]

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

NAT:

[RFC2694]

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

[RFC3022]

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

15 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 described above.

20 SUMMARY OF THE INVENTION

25 The method of the invention for ensuring secure forwarding of a message is performed in a telecommunication network, comprising at least one terminal from which the message is sent and at least one other terminal to which the message is sent. In the method, one or more secure connections are established between different addresses of the first terminal and address of the other terminal, the connections defining at least said addresses of the two terminals. When the first terminal moves from one address to another address, a secure connection, whose endpoints are the new address of the first terminal and the address of the other terminal, is registered to be at least one of
30 the active connections.

If there does not already exist such a secure connection between the new address and the other terminal, a new secure connection between the new address and the other terminal address has to be formed.

- 5 The terminals might have several active connections. In the invention, the terminal might in one embodiment also have only one secure active connection at a time, which can be changed in according with the invention to be defined to be between the address the terminal moves to and the address of the other terminal.
- 10 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 invention is moreover concerned with a system, which is able to perform the method of the invention. The characteristics of the system are defined by the system
15 main claim, the subclaim defining the functions that can be performed by the system of the invention.

The secure connections are preferably established by forming Security Associations (SAs) using the IPSec protocols and the message to be forwarded consists of IP
20 packets. The key exchange being a part of the forming of a secure connection is performed manually or automatically with IKE or some other automated key exchange protocol.

When a new secure connection is formed, it is registered for immediate and/or later
25 use. The registration for later use is made using a connection table, which is maintained by both hosts participating in the forming of the secure connection. The connection table is also used e.g. when the first terminal moves, and needs to determine whether a secure tunnel already exists for the new address. The table can be e.g. a Security Association DataBase (SADB), which is the nominal place to store
30 IPSec SAs in the IPSec model.

In the preferred embodiment, IPsec security associations are used as secure connections. The table, through which the existence of a given IPsec SA (in either the first terminal or the other terminal) is determined, is then the IPsec Security Association DataBase (SADB).

5

The actual connection(s) to be used is registered by means of a signalling message or signalling message exchange between the first terminal and the other terminal, for example by means of Registration Request and possibly Registration Reply messages.

10

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.

15

20

The new address of the first terminal can also be updated automatically by the other terminal when the first terminal sends a message from its new address.

25

The active SA is a stored mobility binding that maps a given terminal address to one or more IPsec tunnel mode SAs (or zero such SAs, if the terminal in question is not connected). These mobility bindings are manipulated when Registration Request and Registration Reply messages are processed when sending packets to the first terminal. It is possible to restrict traffic from the first terminal to only the IPsec SAs that are currently registered in the mobility binding, but allowing traffic from all shared SAs is also reasonable.

30

The mobility binding is necessary, since each of the shared IPsec security associations is valid for securing traffic. There has to be some way for the first terminal

to determine which security association(s) to actually use when processing packets. The mobility binding serves this purpose in the invention.

5 The first terminal may use any IPsec tunnel SA it shares with the other terminal. It is possible to restrict traffic from the first terminal to only the IPsec SAs that are currently registered, but this is not an essential feature. Thus, the first terminal may use any IPsec tunnel SA it shares with the other terminal when sending packets. The other terminal may restrict traffic only to IPsec SAs that are currently active in the mobility binding, but allowing traffic from all shared SAs is also reasonable.

10 The invention can be used for direct end-to-end communication, in which case the secure tunnel is established between these end computers. If applied to IPsec, this could correspond to either an IPsec transport mode or tunnel mode SA. The message might also be sent first to an intermediate computer, whereby the outer address of the
15 IPsec tunnel is unwrapped by the intermediate computer and the message is forwarded as plain text to the end destination computer.

20 Thus, in the solution of the invention, an IPsec security association is used instead of the IP-IP tunnelling. The invention can also be used for tunnelling with IPsec transport mode and an external tunnelling mechanism, such as Layer 2 Tunnelling Protocol (L2TP).

The invention provides the following advantages.

25 IPsec key management and strong authentication can be leveraged for this application involving asymmetric (RSA) authentication, the use of the Diffie-Hellman key exchange algorithm, the possibility to use certificates etc.

30 The IPsec symmetric encryption and authentication methods can be used to protect both signalling and data traffic. This provides confidentiality and integrity and any future developments of IPsec can be taken advantage of.

The NAT traversal problem can be solved by using any available NAT traversal mechanisms for IPSec. One is currently being standardised for IPSec, but any other IPSec NAT traversal mechanism may be used.

- 5 The invention can be used in different networks, such as IPv4 and IPv6.

In the following the invention is described more in detail by means of an advantageous embodiment in an example network but is not restricted to the details thereof.

10

FIGURES

Figure 1 describes the mobile IP tunnelling of prior art by means of a signalling diagram

15

Figure 2 describes the method of the invention by means of a signalling diagram

DETAILED DESCRIPTION

20

The data communication in figure 1 takes place from a mobile terminal to a target host X via an intermediate computer, which works as a home server for host X.

25 Packets sent from the home address of the mobile terminal can be directly routed to the target address X by the intermediate computer, since the home address is registered in routing tables by means of which the routing takes place.

30 Figure 1 describes a method of prior art, wherein IP-IP tunnelling is used for routing data packets when the mobile host moves from one address to another, i.e. from the home address to a new address.

Mobile IP also supports the so-called triangular routing mode, where the packets sent by the mobile terminal are routed directly to the recipient of the packet, bypassing the home server, while packets sent to the mobile terminal are first routed to the home server and then IP-IP tunnelled to the mobile terminal. This mode is more efficient, but is incompatible with so-called ingress filtering routers, which do not route IP packets whose source addresses are topologically incorrect, as is the case with a mobile terminal that is away from the home network. The details of this mode are different, but the general idea is the same. The more general case where IP-IP tunnelling is used for traffic between the mobile terminal and the home server in both directions is discussed in the following text.

In figure 1, when a mobile terminal being in a visited network intends to send a packet to a target host X using its current care-of address, which is an address borrowed from the visited network, it first constructs a data packet, whose source address is its home address – which is not a topologically correct address in the current network the mobile terminal is in – and whose destination address is X. Because the source address of the packet is topologically incorrect, i.e., does not belong to the network the mobile terminal is in, some routers, especially the ones that implement the so-called ingress filtering algorithm, will not route the packet properly. To overcome this, the packet is encapsulated into another IP packet; this process is called IP-IP tunnelling or IP-IP encapsulation. The new, outer IP header source address is the care-of address from the visited network – which is a topologically correct address – and the outer IP header destination address is the home server of the mobile terminal. Thus, the inner IP header source address is the home address of the mobile terminal, while the inner IP header destination address is that of the host X. This is indicated in figure 1 with IP | IP | data, which describes a message containing data and the original IP header, which is encapsulated further in an outer IP header for routing purposes. This IP packet is then sent to the home server in step 1 of figure 1.

Upon receiving the encapsulated IP packet, the home server unwraps the IP-IP tunnel, and proceeds in step 2 of figure 2 with routing a packet indicated with IP/Data, which packet was inside the encapsulation (inside the outer IP header). The routing is

performed in accordance with the inner destination address; the packet now, after the unwrapping, having the home address of the mobile terminal as its source address and host X as its destination address.

- 5 Reverse packets from X to the mobile terminal are handled similarly; the packet is first routed to the home server in step 3, then encapsulated in IP-IP and delivered to the current network (in step 4) the mobile terminal is in. The mobility binding determines which care-of address(es) the packet is forwarded to.
- 10 In the method of the invention, an IPSec tunnel mode or transport mode security association is used instead of the IP - IP tunnelling. Figure 2 describes an example of the method of the invention for sending messages when a mobile terminal moves to a new address.
- 15 A secure connection, preferably an IPSec security association (SA) or more specifically one IPsec SA bundle for each direction of communication is established between the care-of-address and the home server address, e.g. the care-of-address of the mobile terminal and the home server address. The SA can also include additional parameters and attributes, possibly relating to standard or non-standard IPSec
- 20 extensions, such as NAT traversal, which are conventionally used in SAs. A message to be sent through this tunnel is marked IP/IPSec/IP/Data in figure 2, illustrating that the message contains a data part with a destination IP address and can be sent through an IPSec tunnel, while encapsulated with an outer IP header.
- 25 Reverse packets from X to the mobile terminal are handled similarly; the packet is first routed to the home server in step 3, then IPSec processed using the IPSec tunnel mode SA, during which an outer IP header is added to the packet and delivered to the current network(s) (in step 4) the mobile terminal is in.
- 30 When IPSec transport mode is used, the mobile terminal may either communicate directly with the home server, or alternatively some external tunnelling protocol (apart from IPSec tunnelling) can be used to allow routing of packets further. For example,

the Layer 2 Tunnelling Protocol (L2TP) can be used with IPsec transport mode to provide functionality similar to IPsec tunnelling.

When the mobile terminal moves to a new network, it first obtains a care-of address
5 from the visited network. The mobile terminal then checks whether an SA (or more
precisely, a pair of SA bundles) SA already exists between the new care-of address
and the home server address.

This check is normally done by inspecting the contents of a Security Association
10 DataBase (SADB), as specified by the IPsec protocol. The actual implementation may
somewhat deviate from the nominal processing. The nominal model and the actual
operations often are in reality somewhat different (for instance, hardware IPsec
implementations have a radically different "SADB" implementation than simple lookup.)
If an IPsec security association (SA) between the mobile terminal and the home server
15 defining the care-of address of the mobile terminal at one end (the new address of the
mobile terminal) and the address of the home server at the other end already exists,
this SA is registered to be the actual SA to be used.

This happens by means of a signalling message or signalling message exchange done
20 between the mobile terminal and the home server, described by steps 5 and 6 in figure
2. The messages are preferably authenticated and/or encrypted by using IPsec, and
preferably by using the same IPsec SA that is used for the ordinary traffic protection.
In some embodiments no reply is used. Step 5 is a registration request from the mobile
host to the home server to register the new address and step 6 is a registration reply
25 back to the mobile terminal.

When a SA does not exist between the new care-of address and the home server, an
SA setup occurs between steps 4 and 5 of figure 2. This SA setup may be manual, or
may involve some automatic key exchange protocol, such as the Internet Key
30 Exchange (IKE).

Upon receiving the IPsec protected packet sent using the new SA, the home server processes the IPsec headers and uncovers the original packet from the IPsec tunnel, and then routes the IP packet to host X. If IPsec transport mode is used, the home server processes the IPsec headers and processes the resulting plaintext packet
5 directly without routing it onwards. However, if an external tunnelling protocol, such as L2TP, is used, the tunnelling protocol may forward the packet after IPsec processing.

In figure 2, the RREQ and RREP messages are shown without IPsec protection. In an IPsec embodiment, the IPsec protected messages would be expressed e.g. as
10 IP|IPsec|IP|RREQ resp. IP|IPsec|IP|RREP instead of IP|RREQ resp. IP|RREP. Thus, RREQ/RREP can be protected and one method of protection would be IPsec. If they are protected using IPsec, one can leverage the existing IPsec SA for that purpose. The IPsec protection of signalling message(s) may use either tunnel or transport mode.

15

The abbreviation RREQ in figure 2 stands for Registration Request while the abbreviation RREP stands for Registration Reply. These are preferably the Mobile IP Registration Request and Registration Reply messages, used in conjunction with IPsec in the invention, but other registration formats may be used. It is also within the
20 scope of the invention to only use a Registration Request message (not necessarily using the exact Mobile IP format), but not using a Registration Reply message.

The invention also covers both the case wherein properly authenticated traffic is used as an implicit registration request, and a mobility binding update is performed
25 automatically. As a specific example, an IPsec tunnel mode SA bundle, including an AH used for sending traffic, in which case the addresses of the outermost IP header are covered by AH authentication, is used between the mobile terminal and the home server. When the mobile terminal moves to a new network, it sends a data packet which may be an empty data packet if there is no data to send that is processed using
30 the IPsec SA bundle and sent to the home server. Once the home server properly authenticates the message, including the outermost IP header, and determines that it is coming from an address that differs from the current mobility binding, it may update

the mobility binding automatically. Updating the binding results in that all subsequent packets being destined to the mobile terminal, will be sent using the updated mobility binding, i.e. the new address that the client is using. Thus, no explicit mobility binding update signalling is required in this case.

5

The description of the invention above has been simplified for clarity of description. The invention can be extended in several ways without changing the underlying idea. Some extensions are described in what follows.

- 10 The Mobile IP concept of simultaneous bindings, and associated traffic n-casting from the home server to the mobile terminal can be used. In this case, packets sent towards the mobile terminal would be processed using several IPsec SAs, one for each simultaneous registration, and sent to the different visited networks used by the mobile terminal. The registration message(s) in this case contain fields that indicate
- 15 how the mobility binding is to be modified, e.g. whether to replace existing bindings, or to add a new binding in addition to the existing ones. The implicit registration based on data packets can also be used, possibly together with registration message(s) to maintain the bindings.
- 20 When an IPsec SA does not exist between the new care-of address and the home server address, and an IPsec SA is set up e.g. using an automated key exchange protocol, the completion of the SA setup can be used as an implicit registration, removing the additional registration in steps 5 and possibly 6 in figure 2.
- 25 When in the above "a Security Association SA" or "a bundle of Security Associations SAs" is referred to, this means in practice, an IPsec SA bundle in both cases – one or more IPsec security associations applied in sequence – can be used for each direction of traffic.
- 30 The invention is not specific to IPv4 or IPv6, and can be used with Mobile IP for IPv4 and Mobile IP for IPv6. The invention is also straightforward to extend to future IPsec versions

CLAIMS

1. Method for ensuring secure forwarding of a message in a telecommunication network, comprising at least one first terminal from which the message is sent and at least one other terminal to which the message is sent,
5 characterized by
 - a) establishing one or more secure connections between different addresses of the first terminal and address of the other terminal, these connections defining at least said addresses of the two terminals,
 - 10 b) the first terminal moving from one address to another address,
 - c) a secure connection between said other address and the other terminal address is registered to be at least one of the actual connections to be used.
2. Method of claim 1, characterized in that a new secure connection between
15 the other address of the first terminal and the address of the other terminal is formed for the registration in step c) if such a secure connections does not already exist.
3. Method of claim 1, characterized in that, the secure connection is
20 established in step a) and claim 2 by forming one or more Security Associations (SAs) using the IPSec protocols, such as a bundle of SAs.
4. Method of any of claims 1 - 3, characterized in that the message to be
25 forwarded consists of IP packets.
5. Method of any of claims 1 - 4, characterized in that, after step b), when the first terminal intend to send a message from the address it has moved to it first checks whether a secure connection between the new address and the other terminal already exists.
30
6. Method of claim 5, characterized in that the existence of the new secure connection is checked by means of a connection table.

7. Method of any of claims 1 - 6, characterized in that, in step c), the actual connection(s) to be used is/are registered by means of a signalling message or signalling message exchange between the mobile terminal and the other terminal.
- 5 8. Method of any of claims 1 - 6, characterized in that, the new (second) address of the mobile terminal is updated automatically by the other terminal when the first terminal sends a message from its new address.
9. Method of any of claims 1 - 8, characterized in that the a key exchange
10 being a part of the forming of the secure connection in step a) and claim 2 is performed manually.
10. Method of any of claims 1 - 8, characterized in that a key exchange being a
15 part of the forming of the secure connection in step a) and claim 2 is performed with IKE or some other automated key exchange protocol.
11. Method of any of claims 1 - 10, characterized in that the secure connection
20 between the new address of the first terminal and the other terminal is in step c) registered for immediate and/or later use.
12. Method of claim 11, characterized in that the registration for later use is
made by the other terminal in a connection table.
13. Method of any of claims 3 - 12, characterized in that when sending
25 message through the secure connection IPSec transport mode is used to secure traffic between the mobile computer and the destination computer.
14. Method of claim 13, characterized in that a tunnelling protocol is used
30 together with IPSec to provide a tunnelling capability.

15. Method of claim 14, characterized in that where the Layer 2 Tunnelling Protocol (L2TP) tunnelling protocol is used together with IPSec to provide a tunnelling capability.
- 5 16. Method of any of claims 3 – 15, characterized in that when sending message through the secure connection IPSec tunnel mode is used to secure traffic between the mobile computer and the destination computer.
- 10 17. System for ensuring secure forwarding of a message in a telecommunication network, comprising at least one first terminal from which the message is sent and at least one other terminal to which the message is sent, characterized by means for forming secure connections between the address of the other terminal and different addresses of the first terminal,
- 15 tables with lists of said secure connections, and registrations means for forming such lists.
18. System of claim 17, characterized in that it has means for performing the method of any of claims 1 - 16.

1/2

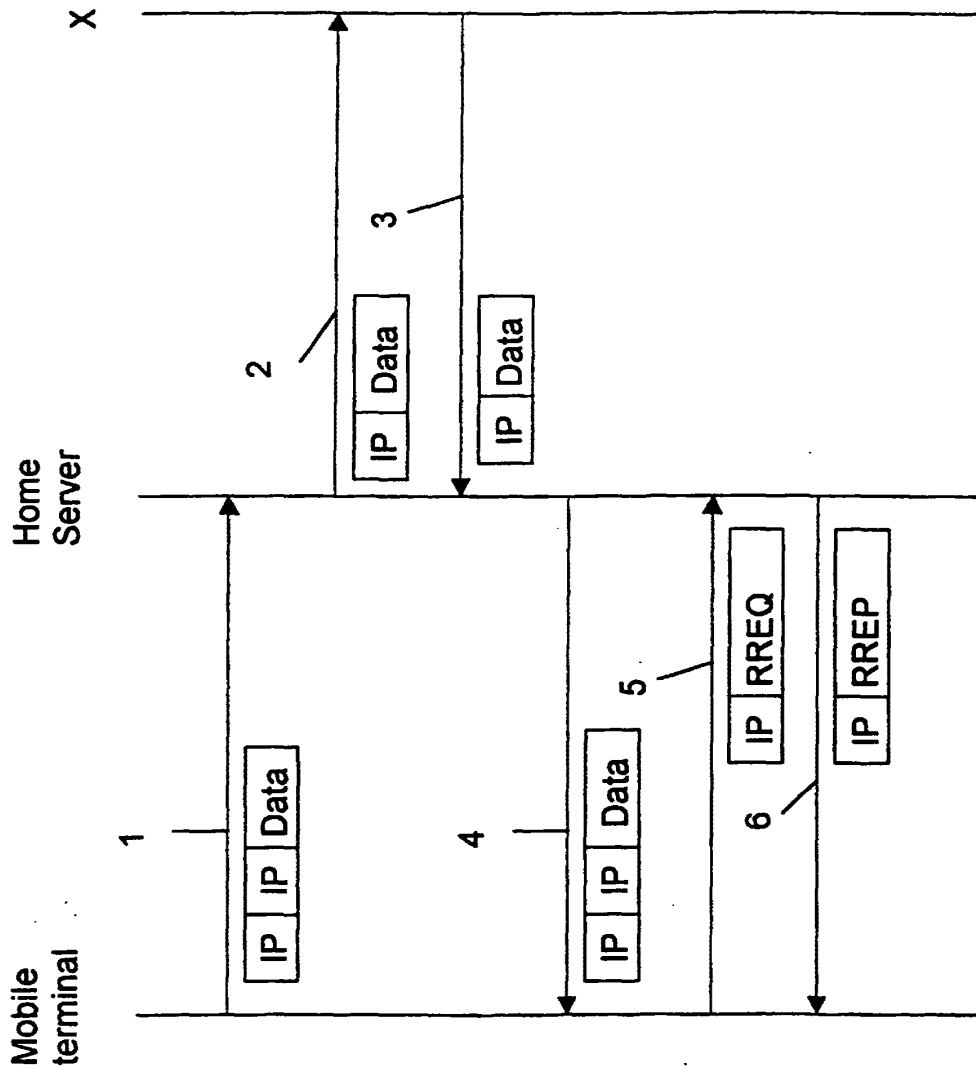


FIG. 1

2 / 2

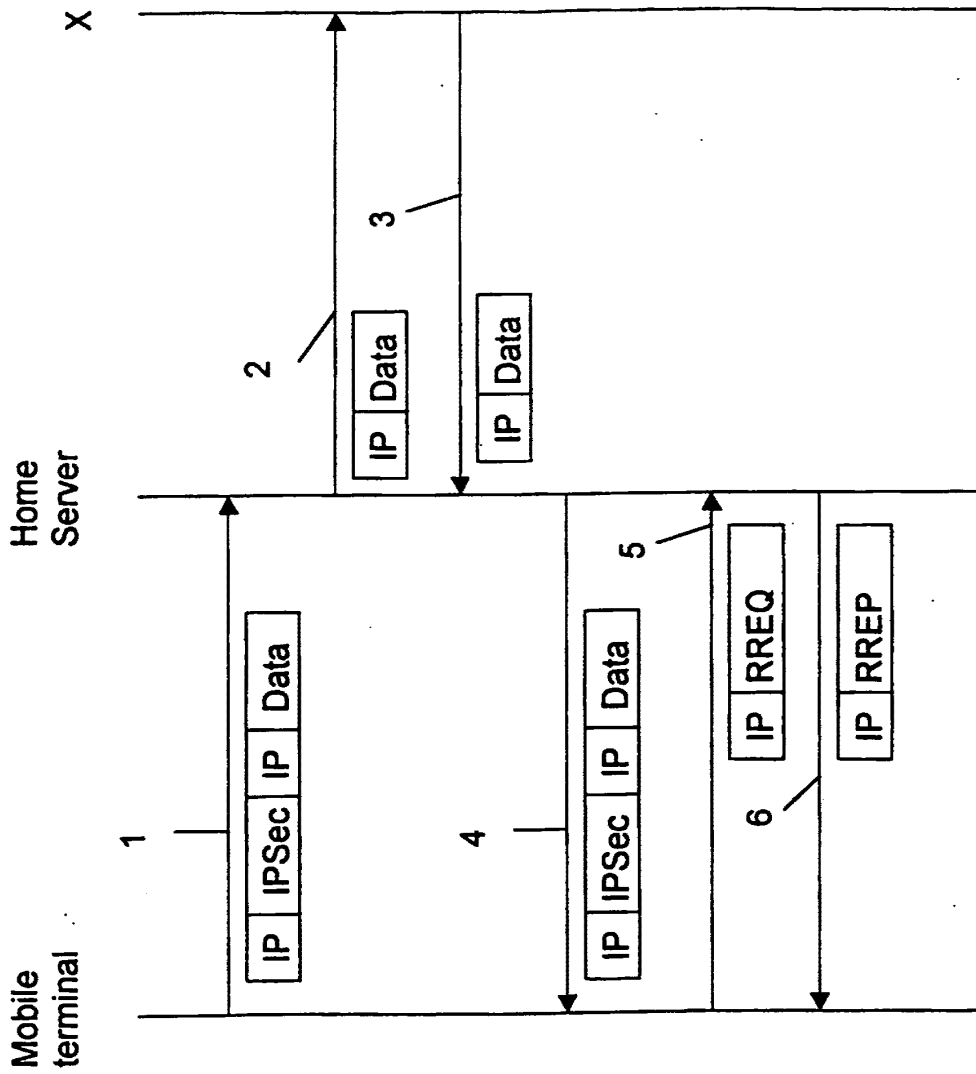


FIG. 2

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FI/00771

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 ---	1-14
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 ---	1-14
A	WO 00 56034 A (3COM CORP) 21 September 2000 (2000-09-21) the whole document ---	1-14
A	WO 01 24560 A (SIMOCO INT LTD ;RAYNE MARK WENTWORTH (GB)) 5 April 2001 (2001-04-05) the whole document ---	1-14
	-/--	

Further documents are listed in the continuation of box C.

Patent family members are listed in annex.

° Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

19 December 2002

Date of mailing of the international search report

20.01.2003

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

MARIANNE ENGDahl/JA A

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FI/00771

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	1-14
A	--- US 2001/009025 A1 (AHONEN PASI MATTI KALEVI) 19 July 2001 (2001-07-19) the whole document -----	1-14

INTERNATIONAL SEARCH REPORT

ormation on patent family members

International Application No
PCT/FI/00771

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 0056034	A	21-09-2000	EP 1159815 A1	05-12-2001
			WO 0056034 A1	21-09-2000

WO 0124560	A	05-04-2001	AU 7534900 A	30-04-2001
			WO 0124560 A1	05-04-2001
			GB 2359464 A	22-08-2001

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

US 2001009025	A1	19-07-2001	GB 2364477 A	23-01-2002
			AU 2895801 A	31-07-2001
			WO 0154379 A1	26-07-2001

PATENT COOPERATION TREATY



PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT
(PCT Article 36 and Rule 70)

REC'D 19 SEP 2003

WIPO PCT

26 MAR 2004

Applicant's or agent's file reference S0052PCT		FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/PEAA16)	
International application No. PCT/FI02/00771	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.			
<p>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.</p> <p>2. This REPORT consists of a total of 5 sheets, including this cover sheet.</p> <p><input checked="" type="checkbox"/> 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).</p> <p>These annexes consist of a total of 3 sheets.</p>			
<p>3. This report contains indications relating to the following items:</p> <p>I <input checked="" type="checkbox"/> Basis of the opinion</p> <p>II <input type="checkbox"/> Priority</p> <p>III <input type="checkbox"/> Non-establishment of opinion with regard to novelty, inventive step and industrial applicability</p> <p>IV <input type="checkbox"/> Lack of unity of invention</p> <p>V <input checked="" type="checkbox"/> Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement</p> <p>VI <input type="checkbox"/> Certain documents cited</p> <p>VII <input type="checkbox"/> Certain defects in the international application</p> <p>VIII <input type="checkbox"/> Certain observations on the international application</p>			
Date of submission of the demand 25.04.2003		Date of completion of this report 17.09.2003	
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 	

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. PCT/FI02/00771

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

1-21 as originally filed

Claims, Numbers

1-18 received on 10.07.2003 with letter of 07.07.2003

Drawings, Sheets

1/2-2/2 as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language: , which is:

- the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
 - the language of publication of the international application (under Rule 48.3(b)).
 - the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).
3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:
- contained in the international application in written form.
 - filed together with the international application in computer readable form.
 - furnished subsequently to this Authority in written form.
 - furnished subsequently to this Authority in computer readable form.
 - The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
 - The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.
4. The amendments have resulted in the cancellation of:
- the description, pages:
 - the claims, Nos.:
 - the drawings, sheets:

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. **PCT/FI02/00771**

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	1-18
	No: Claims	
Inventive step (IS)	Yes: Claims	1-18
	No: Claims	
Industrial applicability (IA)	Yes: Claims	1-18
	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. It is considered that independent claims 1 (method) and 17 (apparatus) relate to new and inventive subject-matter (Articles 33 (2) and (3) PCT), since the prior art does not disclose or suggest the specifically claimed method for ensuring secure forwarding of a message in a telecommunication network according to claim 1 and does not disclose or suggest the specifically claimed system for ensuring secure forwarding of a message in a telecommunication network according to claim 17.

Document D2=WO 00/41427 discloses a method for accomplishing handover for a mobile unit from a first stationary unit to a second stationary unit; the Security Association SA in D2 is reused literally when the terminal moves. In D2 the same SA can be transferred and reused because the terminal only moves within one administrative domain. Thus the first stationary unit in the other end has a common IP address as the second stationary unit which now is the end-point. An SA is always defined by its destination address but in D2 the destination address in the SA did not have to be changed as the other terminal always is an access point in the same network domain.

Document D1= WO 01/39538 discloses a method of providing information security when communication with a given mobile terminal is handed-over from a first access point to a second access point; in D1 (as in D2) the SA is also reused literally when the terminal moves. In D1 the SA is maintained when a handover occurs within the network. The SA is there transferred (and not redefined) and there are only one SA that exists between the terminal and the other endpoint that always is an access point in the same network. The same parameters of the SA are transferred.

In the present invention (method claim 1 and corresponding apparatus claim 17) there is established several secure connections, each of which defines different addresses. One or more of them is then registered to be the active(s) one upon moving of the first terminal. Then no renegotiation or reestablishing of any SA is needed when the first terminal moves from one point to another.

In the present invention a different SA defining a different address has to be used when the first terminal moves, and the other terminal can be any other terminal. The question is here, as it is clearly indicated in present claim 1, about using

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/FI02/00771

different secure connections, not reusing them.

In the present invention there is question about different SAs each defining different addresses.

2. Dependent claims 2 to 16 and 18 contain further details of the method of claim 1 and of the system of claim 17 respectively. As they are dependent on claims 1 and 17 respectively, they also satisfy the requirements for novelty and inventive step (Articles 33 (2) and (3) PCT).

CLAIMS

1. Method for ensuring secure forwarding of a message in a telecommunication network, comprising at least one first terminal from which the message is sent and
5 at least one other terminal to which the message is sent,
c h a r a c t e r i z e d b y
 - a) establishing one or more secure connections between different addresses of the first terminal and address of the other terminal, these connections defining at least said addresses of the two terminals,
 - 10 b) the first terminal moving from one address to another address,
 - c) a secure connection between said other address and the other terminal address is registered to be at least one of the active connections to be used.
2. Method of claim 1, c h a r a c t e r i z e d in that a new secure connection between
15 the other address of the first terminal and the address of the other terminal is formed for the registration in step c) if such a secure connections does not already exist.
3. Method of claim 1, c h a r a c t e r i z e d in that, the secure connection is
20 established in step a) and claim 2 by forming one or more Security Associations (SAs) using the IPsec protocols, such as a bundle of SAs.
4. Method of any of claims 1 - 3, c h a r a c t e r i z e d in that the message to be
25 forwarded consists of IP packets.
5. Method of any of claims 1 - 4, c h a r a c t e r i z e d in that, after step b), when the first terminal intend to send a message from the address it has moved to it first checks whether a secure connection between the new address and the other terminal already exists.
30
6. Method of claim 5, c h a r a c t e r i z e d in that the existence of the new secure connection is checked by means of a connection table.

- 7. Method of any of claims 1 - 6, characterized in that, in step c), the actual connection(s) to be used is/are registered by means of a signalling message or signalling message exchange between the mobile terminal and the other terminal.
- 5 8. Method of any of claims 1 - 6, characterized in that, the new (second) address of the mobile terminal is updated automatically by the other terminal when the first terminal sends a message from its new address.
- 9. Method of any of claims 1 - 8, characterized in that the a key exchange being a part of the forming of the secure connection in step a) and claim 2 is performed manually.
- 10 10. Method of any of claims 1 - 8, characterized in that a key exchange being a part of the forming of the secure connection in step a) and claim 2 is performed with IKE or some other automated key exchange protocol.
- 15 11. Method of any of claims 1 - 10, characterized in that the secure connection between the new address of the first terminal and the other terminal is in step c) registered for immediate and/or later use.
- 20 12. Method of claim 11, characterized in that the registration for later use is made by the other terminal in a connection table.
- 13. Method of any of claims 3 - 12, characterized in that when sending message through the secure connection IPSec transport mode is used to secure traffic between the mobile computer and the destination computer.
- 25 14. Method of claim 13, characterized in that a tunnelling protocol is used together with IPSec to provide a tunnelling capability.

- 15. Method of claim 14, characterized in that where the Layer 2 Tunnelling Protocol (L2TP) tunnelling protocol is used together with IPSec to provide a tunnelling capability.
- 5 16. Method of any of claims 3 – 15, characterized in that when sending message through the secure connection IPSec tunnel mode is used to secure traffic between the mobile computer and the destination computer.
- 10 17. System for ensuring secure forwarding of a message in a telecommunication network, comprising at least one first terminal from which the message is sent and at least one other terminal to which the message is sent, characterized by means for forming secure connections between the address of the other terminal and different addresses of the first terminal,
- 15 tables with lists of said secure connections, and registrations means for forming such lists.
- 18. System of claim 17, characterized in that it has means for performing the method of any of claims 1 - 16.



DT03 Rec'd PCT/PTO 29 JUN 2004
PCT

RP:nr 6/25/04 290.1053USN

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of Art Unit
Sami Vaarala, Antti Nuopponen, Batch No.
Panu Pietikainen

Serial No. 10/490,933

Filed: 26 March 2004

For: METHOD AND system FOR
ENSURING SECURE
FORWARDING OF MESSAGES

Examiner:

Date: 25 June 2004

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 6/25/04 290.1053USN

PATENT

Attorney Matter No. 290.1053USN

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of
Sami Vaarala, Antti Nuopponen,
Panu Pietikainen

Serial No. 10/490,933 Art Unit
Filed: 26 March 2004 Confirmation No.
For: METHOD AND SYSTEM
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


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.
10/490,933	Sami Vaarala	290.1053USN

INTERNATIONAL APPLICATION NO.

PCT/FI02/00771

I.A. FILING DATE	PRIORITY DATE
09/27/2002	09/28/2001

Rolf Fasth
 FASTH LAW OFFICES
 629 East Boca Raton Road
 Phoenix, AZ 85022

CONFIRMATION NO. 2431

371 FORMALITIES LETTER



OC00000014641357

Date Mailed: 12/02/2004

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
- 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.*

SHAKEEL AHMED

Telephone: (703) 305-3659

PART 2 - OFFICE COPY

U.S. APPLICATION NUMBER NO.	INTERNATIONAL APPLICATION NO.	ATTY. DOCKET NO.
10/490,933	PCT/FI02/00771	290.1053USN

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



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. 2431

SERIAL NUMBER 10/490,933	FILING OR 371(c) DATE 04/18/2005 RULE	CLASS 713	GROUP ART UNIT 2131	ATTORNEY DOCKET NO. 290.1053USN	
APPLICANTS Sami Vaarala, Espoo, FINLAND; Antti Nuopponen, Espoo, FINLAND; Panu Pietikainen, Espoo, FINLAND;					
** CONTINUING DATA ***** This application is a 371 of PCT/FI02/00771 09/27/2002					
** FOREIGN APPLICATIONS ***** FINLAND 20011911 09/28/2001					
** SMALL ENTITY **					
Foreign Priority claimed <input type="checkbox"/> yes <input type="checkbox"/> no		STATE OR COUNTRY FINLAND	SHEETS DRAWING 2	TOTAL CLAIMS 17	INDEPENDENT CLAIMS 2
35 USC 119 (a-d) conditions met <input type="checkbox"/> yes <input type="checkbox"/> no <input type="checkbox"/> 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 system for ensuring secure forwarding of messages					
FILING FEE RECEIVED 525	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:		<input type="checkbox"/> All Fees <input type="checkbox"/> 1.16 Fees (Filing) <input type="checkbox"/> 1.17 Fees (Processing Ext. of time) <input type="checkbox"/> 1.18 Fees (Issue) <input type="checkbox"/> Other _____ <input type="checkbox"/> Credit		

JCO3 Rec'd T/PTO 18 APR 2005

3

RF:nr 4/15/05 290.1053USN

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Art Unit

Sami Vaarala, Antti Nuopponen,
Panu Pietikainen

Confirmation No. 2431

Serial No. 10/490,933

CERTIFICATE OF MAILING

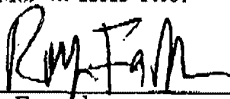
Filed: 26 March 2004

For: METHOD AND SYSTEM FOR
ENSURING SECURE
FORWARDING OF MESSAGES

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 April 15, 2005 AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO: MAIL STOP MISSING PARTS, COMMISSIONER FOR PATENTS, P.O. BOX 1450, ALEXANDRIA, VA 22313-1450.

Examiner:

Date: 15 April 2005



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 2 December 2004
- (X) Request for 3MO EXTENSION in responding to Notification of Missing Requirements dated 2 December 2004
- (X) Signed Oath or Declaration of the inventor(s)
- (X) Check #4135 for \$575.00 (\$510 for 3MO EXTENSION in responding to MP Notification and \$65 to cover surcharge for providing signed oath or declaration later than 30 months from priority date
- (X) The Commissioner is hereby authorized to charge any additional fees which may be required in connection with the filing of this correspondence, or credit over-payment,

04/21/2005 SNAJARRO 00000040 10490933

01 FC:2617

65.00 OP

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

04/21/2005 SNAJARRO 00000040 10490933

02 FC:2253

510.00 OP


UNITED STATES PATENT AND TRADEMARK OFFICE

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

U.S. APPLICATION NUMBER NO. 10/490,933	FIRST NAMED APPLICANT Sami Vaarala	ATTY. DOCKET NO. 290.1053USN
		INTERNATIONAL APPLICATION NO. PCT/FI02/00771
		I.A. FILING DATE 09/27/2002
		PRIORITY DATE 09/28/2001

 Rolf Fasth
 FASTH LAW OFFICES
 629 East Boca Raton Road
 Phoenix, AZ 85022

CONFIRMATION NO. 2431
371 FORMALITIES LETTER


OC000000014641357

Date Mailed: 12/02/2004

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
- 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:

04/21/2005 SNAJARR0 00000040 10490933

01-FC:2617

65.00 DP

- \$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.*

SHAKEEL AHMED

Telephone: (703) 305-3659

PART 1 - ATTORNEY/APPLICANT COPY

U.S. APPLICATION NUMBER NO.	INTERNATIONAL APPLICATION NO.	ATTY. DOCKET NO.
10/490,933	PCT/FI02/00771	290.1053USN

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

JCOB Rec'd PCT/PTO 18 APR 2005

RF 5/26/04 286.10305M

**COMBINED DECLARATION AND POWER OF ATTORNEY
FOR PATENT APPLICATION**

As a below named inventor, I hereby declare that:

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

I believe I an original, first and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled METHOD AND SYSTEM FOR ENSURING SECURE FORWARDING OF MESSAGES, the specification of which was filed as International Patent Application No. PCT/FI02/00771, 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
<u>20011911</u> (Number)	<u>Finland</u> (Country)	<u>28 Sept. 2001</u> (Day/Month/Year)	[X] [] Yes No

RF 3/26/04 290-103305N

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

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

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

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

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

Address all correspondence to:

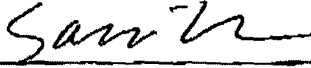
Rolf Fasth
FASTH LAW OFFICES
629 E. Boca Raton
Phoenix, AZ 85022

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

RF 3/26/04 295.1057USN

1 - ∞

Full name of first joint inventor: Sami Vaarala

Inventor's signature  Date _____


Residence: Helsinki, Finland

Citizenship: Finland

Post Office address: SÄTERINKINNE 8B37
02600 ESPOO FIX
~~Neljas Linja 22 A 24~~
~~FIN-00530 Helsinki, Finland~~

2 - ∞

Full name of second joint inventor: Antti Nuopponen

Inventor's signature  Date 10.5.2004

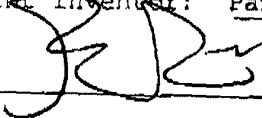
Residence: Espoo, Finland FIX

Citizenship: Finland

Post Office address: Kaksoiskiventie 7-9 A 1
FIN-02760 Espoo, Finland

3 - ∞

Full name of third joint inventor: Panu Pietikainen

Inventor's signature  Date 12.5.2004

Residence: Espoo, Finland FIX

Citizenship: Finland

Post Office address: Westendintie 93F39
~~Taysikuu 10 C 103~~ 02160 Espoo
~~FIN-02210 Espoo, Finland~~ 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

U.S. APPLICATION NUMBER NO.	FIRST NAMED APPLICANT	ATTY. DOCKET NO.
10/490,933	Sami Vaarala	290.1053USN

INTERNATIONAL APPLICATION NO.

PCT/FI02/00771

IA. FILING DATE	PRIORITY DATE
09/27/2002	09/28/2001

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

CONFIRMATION NO. 2431
371 ACCEPTANCE LETTER


OC000000015857988

Date Mailed: 04/26/2005

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:

<u>04/18/2005</u>	<u>04/18/2005</u>
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
- Preliminary Amendments filed on 03/26/2004
- Oath or Declaration filed on 04/18/2005
- 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
- Power of Attorney filed on 04/18/2005

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

SHAKEEL AHMED

Telephone: (703) 308-9140 EXT 208

PART 3 - OFFICE COPY

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



[Handwritten signature]


PTO/SB/122 (04-05)

Approved for use through 07/31/2006. OMB 0851-0035
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	10/490,933
	Filing Date	26 MARCH 2004
	First Named Inventor	SAMI VAARALA
	Art Unit	
	Examiner Name	
	Attorney Docket Number	290.1053USN

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

The address associated with Customer Number: 33369 

33369
PATENT TRADEMARK OFFICE

OR

Firm or Individual Name

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/06).

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 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.



JFW


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.

<p align="center">CHANGE OF CORRESPONDENCE ADDRESS Application</p> <p>Address to: Commissioner for Patents P.O. Box 1450 Alexandria, VA 22313-1450</p>	Application Number	10/490,933
	Filing Date	26 MARCH 2004
	First Named Inventor	SAMI VAARALA
	Art Unit	
	Examiner Name	
	Attorney Docket Number	290.1053USN

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

The address associated with Customer Number: 33369 

33369
PATENT TRADEMARK OFFICE

OR

Firm or Individual Name

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 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

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
10490933

APPLICATION AS FILED - PART I

(Column 1)		(Column 2)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)		RATE (\$)	FEE (\$)
BASIC FEE (37 CFR 1.16(a), (b), or (c))							
SEARCH FEE (37 CFR 1.16(a), (f), or (m))							
EXAMINATION FEE (37 CFR 1.16(e), (g), or (h))							
TOTAL CLAIMS (37 CFR 1.16(i))		minus 20 =	X	=	OR	X	=
INDEPENDENT CLAIMS (37 CFR 1.16(b))		minus 3 =	X	=		X	=
APPLICATION SIZE FEE (37 CFR 1.16(e))	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(e).						
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

		(Column 1)	(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)		RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	17	Minus ** 20	= 0	X	=	OR	X	=
	Independent (37 CFR 1.16(i))	2	Minus *** 3	= 0	X	=	OR	X	=
		Application Size Fee (37 CFR 1.16(e))							
		FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
		TOTAL ADD'L FEE						TOTAL ADD'L FEE	

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

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.
10/490,933	04/18/2005	Sami Vaarala	290.1053USN	2431

33369 7590 10/15/2008
FASTH LAW OFFICES (ROLF FASTH)
26 PINECREST PLAZA, SUITE 2
SOUTHERN PINES, NC 28387-4301

EXAMINER

ALMEIDA, DEVIN E

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

2432

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

10/15/2008

PAPER

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

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

Office Action Summary	Application No. 10/490,933	Applicant(s) VAARALA ET AL.	
	Examiner DEVIN ALMEIDA	Art Unit 2432	

-- 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 26 March 2004.
- 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) 1-17 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) 1-17 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

This action is in response to the papers filed 3/26/2004.

Priority

Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d). The certified copy has been received.

Information Disclosure Statement

The information disclosure statement (IDS) submitted on 6/29/2004 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Objections

Claims 7 and 8 are objected to because of the following informalities:
Claim 7 recites the limitation "the mobile terminal" in line 5 of claim 7. There is insufficient antecedent basis for this limitation in the claim. Claim 8 recites the limitation "the mobile terminal" in line 3 of claim 8. There is insufficient antecedent basis for this limitation in the claim.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

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

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

Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. It is unclear what the limitation "said

Art Unit: 2432

other address" refers to. For purposes of examination "said other address" is interpreted as the new address of the first terminal.

Claim Rejections - 35 USC § 102

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

Office action:

A person shall be entitled to a patent unless –

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

Claims 1-8, 10-14, 16 and 17 rejected under 35 U.S.C. 102(e) as being anticipated by Ala-Laurila (U.S. 6,587,680).

With respect to claim 1 a method for ensuring secure forwarding of a message in a telecommunication network (see abstract i.e. radio communications system), comprising at least one first terminal from which the message is sent and at least one other terminal to which the message is sent (see abstract), the method comprising: a) establishing one or more secure connections between different addresses of the first terminal (mobile terminal) and address of the other terminal (access points), these connections defining at least said addresses of the two terminals (see column 6 lines 25-50), b) the first terminal (mobile terminal address with old access point) moving from one address to another address (mobile terminal address new access point) (see column 7 line 46 – column 8 line 41), and c) registering a secure connection

Art Unit: 2432

between said other address and the other terminal address to be at least one of the active connections to be used (see column 7 line 46 – column 8 line 41).

With respect to claim 2, characterized in that a new secure connection between the other address of the first terminal and the address of the other terminal is formed for the registration in step c) if such a secure connections does not already exist (see column 7 line 46 – column 8 line 16).

With respect to claim 3, characterized in that, the secure connection is established in step a) and by forming one or more Security Associations (SAs) using the IPSec protocols (see column 9 lines 17-21).

With respect to claim 4, characterized in that the message to be forwarded consists of IP packets (see column 8 lines 1-16).

With respect to claim 5, characterized in that, after step b), when the first terminal intend to send a message from the address it has moved to it first checks whether a secure connection between the new address and the other terminal already exists (see column 8 lines 49-61).

With respect to claim 6, characterized in that the existence of the new secure connection is checked by means of a connection table (see column 7 line 56-67 i.e. available access point list).

With respect to claim 7, characterized in that, in step c), the actual connection(s) to be used is/are registered by means of a signaling message or signaling message exchange between the mobile terminal and the other terminal (see figure 2 and 3).

With respect to claim 8, characterized in that, the new (second) address of the mobile terminal is updated automatically by the other terminal when the first terminal sends a message from its new address (see column 7 line 46 – column 8 line 41).

With respect to claim 10, characterized in that a key exchange being a part of the forming of the secure connection in step a) and claim 2 is performed with IKE or some other automated key exchange protocol (see column 8 lines 17-22).

With respect to claim 11, characterized in that the secure connection between the new address of the first terminal and the other terminal is in step c) registered for immediate and/or later use (see column 7 line 46 – column 8 line 41).

With respect to claim 12, characterized in that the registration for later use is made by the other terminal in a connection table (see column 7 line 56-67 i.e. available access point list).

With respect to claim 13, characterized in that when sending message through the secure connection IPSec transport mode is used to secure traffic between the mobile computer and the destination computer (see column 9 lines 17-21).

With respect to claim 14, characterized in that a tunneling protocol is used together with IPSec to provide a tunneling capability (see figure 2, 3 and column 9 lines 17-21).

With respect to claim 16, characterized in that when sending message through the secure connection IPSec tunnel mode is used to secure traffic between the mobile computer and the destination computer (see figure 2, 3 and column 9 lines 17-21).

With respect to claim 17 a system for ensuring secure forwarding of a message in a telecommunication network, comprising at least one first terminal from which the message is sent and at least one other terminal to which the message is sent (see abstract), characterized by means for forming secure connections between the address of the other terminal and different addresses of the first terminal (see abstract), tables with lists of said secure connections, and registrations means for forming such lists (see column 7 line 56-67 i.e. available access point list).

Claim Rejections - 35 USC § 103

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

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

Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ala-Laurila (U.S. 6,587,680) in view of Takagi et al (U.S. 7,143,282).

Ala-Laurila does not teach that the a key exchange being a part of the forming of the secure connection in step a) and is performed manually. Takagi

Art Unit: 2432

teaches a key exchange being a part of the forming of the secure connection in step a) and is performed manually (see Takagi column 8 lines 29-34).

It 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 to have the Security Associations of Ala-Laurila to be set up manually as taught in Takagi by Internet Key Exchange to increase the compatibility of the system (see Takagi column 8 lines 29-34). Therefore one would have been motivated to have Security Associations be able to be set up manually by Internet Key Exchange.

Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ala-Laurila (U.S. 6,587,680) in view of Jorgensen (U.S. 6,452,915).

Ala-Laurila does not teach with respect to claim 15 where the Layer 2 Tunneling Protocol (L2TP) tunneling protocol is used together with IPsec to provide a tunneling capability. Jorgensen teaches Layer 2 Tunneling Protocol (L2TP) tunneling protocol is used together with IPsec to provide a tunneling capability (see Jorgensen column 44 lines 8-17). It 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 to have used L2TP over IPsec because L2TP can carry multiple protocols. L2TP also offers transmission capability over non-IP networks (see Jorgensen column 44 lines 8-17). Therefore one would have been motivated to have used L2TP over IPsec.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Devin Almeida whose telephone number is 571-270-1018. The examiner can normally be reached on Monday-Thursday from 7:30 A.M. to 5:00 P.M. The examiner can also be reached on alternate Fridays from 7:30 A.M. to 4:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on 571-272-3799. 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).

/Devin Almeida/
Examiner, Art Unit 2432
10/8/2008

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2432

Notice of References Cited	Application/Control No. 10/490,933	Applicant(s)/Patent Under Reexamination VAARALA ET AL.	
	Examiner DEVIN ALMEIDA	Art Unit 2432	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-7,143,282	11-2006	Takagi et al.	713/153
*	C US-6,452,915	09-2002	Jorgensen, Jacob W.	370/338
	D US-			
	E US-			
	F US-			
	G US-			
	H US-			
	I US-			
	J US-			
	K US-			
	L US-			
	M US-			


FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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

<i>Index of Claims</i> 	Application/Control No. 10490933	Applicant(s)/Patent Under Reexamination VAARALA ET AL.
	Examiner DEVIN ALMEIDA	Art Unit 2432

✓	Rejected
=	Allowed


-	Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

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

CLAIM		DATE									
Final	Original	10/08/2008									
	1	✓									
	2	✓									
	3	✓									
	4	✓									
	5	✓									
	6	✓									
	7	✓									
	8	✓									
	9	✓									
	10	✓									
	11	✓									
	12	✓									
	13	✓									
	14	✓									
	15	✓									
	16	✓									
	17	✓									
	18	-									

Search Notes 	Application/Control No. 10490933	Applicant(s)/Patent Under Reexamination VAARALA ET AL.
	Examiner DEVIN ALMEIDA	Art Unit 2432

SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
See east printout	10/8/2008	DA

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

/DEVIN ALMEIDA/ Examiner.Art Unit 2432	
---	--

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L12	421	tunnel\$ with l2tp same ipsec	US- PGPUB; USPAT; EPO	OR	ON	2008/10/08 12:17
L13	220	tunnel\$ with l2tp same ipsec and mobile	US- PGPUB; USPAT; EPO	OR	ON	2008/10/08 12:18
L14	17	tunnel\$ with l2tp same ipsec and mobile adj terminal	US- PGPUB; USPAT; EPO	OR	ON	2008/10/08 12:18
L15	268	tunnel\$ with l2tp same ipsec same security	US- PGPUB; USPAT; EPO	OR	ON	2008/10/08 12:21
S10	1	10/490933	US- PGPUB; USPAT	OR	ON	2008/10/07 15:04
S17	18	"6587680"	US- PGPUB; USPAT; EPO	OR	ON	2008/10/07 15:11
S18	6	"6418130"	US- PGPUB; USPAT; EPO	OR	ON	2008/10/07 15:12

10/ 8/ 2008 12:38:06 PM

C:\ Documents and Settings\ dalmeida\ My Documents\ EAST\ Workspaces
\ 10490933.wsp



UNITED STATES PATENT AND TRADEMARK OFFICE

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

BIB DATA SHEET

CONFIRMATION NO. 2431

SERIAL NUMBER 10/490,933	FILING or 371(c) DATE 04/18/2005 RULE	CLASS 713	GROUP ART UNIT 2432	ATTORNEY DOCKET NO. 290.1053USN	
APPLICANTS Sami Vaarala, Espoo, FINLAND; Antti Nuopponen, Espoo, FINLAND; Panu Pietikainen, Espoo, FINLAND; ** CONTINUING DATA ***** This application is a 371 of PCT/FI02/00771 09/27/2002 ** FOREIGN APPLICATIONS ***** FINLAND 20011911 09/28/2001 ** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** ** SMALL ENTITY **					
Foreign Priority claimed <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No 35 USC 119(a-d) conditions met <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Verified and Acknowledged <u>/DEVIN E ALMEIDA/</u> Examiner's Signature	<input type="checkbox"/> Met after Allowance Initials	STATE OR COUNTRY FINLAND	SHEETS DRAWINGS 2	TOTAL CLAIMS 17	INDEPENDENT CLAIMS 2
ADDRESS FASTH LAW OFFICES (ROLF FASTH) 26 PINECREST PLAZA, SUITE 2 SOUTHERN PINES, NC 28387-4301 UNITED STATES					
TITLE Method and system for ensuring secure forwarding of messages					
FILING FEE RECEIVED 525	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:		<input type="checkbox"/> All Fees <input type="checkbox"/> 1.16 Fees (Filing) <input type="checkbox"/> 1.17 Fees (Processing Ext. of time) <input type="checkbox"/> 1.18 Fees (Issue) <input type="checkbox"/> Other _____ <input type="checkbox"/> Credit		

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of Art Unit 2432

5 Sami Vaarala, Antti Nuopponen, Panu Pietikainen

Serial No. 10/490,933

10 Filed: 18 April 2005

For: METHOD AND NETWORK FOR ENSURING SECURE FORWARDING OF
MESSAGES

15 Examiner: Devin E. Almeida

Date: 8 January 2009

Attorney Docket Number: 290.1053USN

20

AMENDMENT

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

This is in response to the Office action of 15
October 2008. Please amend the above-identified patent
application as follows:

30

In the Claims:

Amend the claims as follows:

5

1. (Currently amended) A method for ensuring secure forwarding of a message in a telecommunication network, comprising: providing at least one a first terminal from which the message is sent and a at least one other second terminal to which the message is sent, ~~the method comprising:~~

10

a) establishing ~~one or more a secure connection connections~~ between ~~different a first~~ addresses of the first terminal and an original address of the ~~other second~~ terminal, ~~these connections the secure connection~~ defining the first and original ~~at least said~~ addresses of the ~~two first and second~~ terminals,

15

b) the first terminal ~~moving~~ changing from ~~one the first~~ address to a new another address, and

20

c) registering a secure connection between ~~said other the new~~ address and the original address of the second other terminal address to be ~~at least one of the active connections~~ the secure connection to be used.

25

2. (Currently amended) The method of claim 1, characterized in that a new secure connection between the ~~other new~~ address of the first terminal and the address of the ~~other second~~ terminal is formed for the registration in step c) if such a secure connections does not already exist.

30

3. (Previously presented) The method of claim 1, characterized in that, the secure connection is established in step a) and by forming one or more Security Associations (SAs) using the IPsec protocols.

35

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

in that the message to be forwarded consists of IP packets.

5. (Currently amended) The method of claim 1, characterized in that, after step b), when the first terminal intend to send a message from the address it has moved to it first checks whether a secure connection between the new address and the ~~other~~ second terminal already exists.

6. (Previously presented) The method of claim 5, characterized in that the existence of the new secure connection is checked by means of a connection table.

7. (Currently amended) The method of claim 1, characterized in that, in step c), the actual connection(s) to be used is/are registered by means of a signaling message or signaling message exchange between the ~~mobile~~ first terminal and the ~~other~~ second terminal.

8. (Currently amended) The method of claim 1, characterized in that, the new (second) address of the ~~mobile~~ first terminal is updated automatically by the ~~other~~ second terminal when the first terminal sends a message from ~~its~~ the new address.

9. (Previously presented) The method of claim 1, characterized in that the a key exchange being a part of the forming of the secure connection in step a) and is performed manually.

10. (Currently amended) The method of claim 2 ~~4~~, characterized in that a key exchange being a part of the forming of the secure connection ~~in step a) and claim 2~~ is performed with IKE or some other automated key exchange protocol.

11. (Previously presented) The method of claim 1, characterized in that the secure connection between the new address of the first terminal and the ~~other~~ second terminal is

in step c) registered for immediate and/or later use.

12. (Currently amended) The method of claim 11, characterized
in that the registration for later use is made by the ~~other~~
5 second terminal in a connection table.

13. (Currently amended) The method of claim 3, characterized
in that when sending message through the secure connection
IPSec transport mode is used to secure traffic between the
10 mobile computer and ~~the~~ a destination computer.

14. (Previously presented) The method of claim 13,
characterized in that a tunneling protocol is used together
with IPSec to provide a tunneling capability.
15

15. (Currently amended) The method of claim 14, characterized
in that where the Layer 2 Tunneling Protocol (L2TP) tunneling
protocol is used together with IPSec to provide a tunneling
capability.
20

16. (Currently amended) The method of claim 3, characterized
in that when sending message through the secure connection
IPSec tunnel mode is used to secure traffic between the mobile
computer and ~~the~~ a destination computer.
25

17. (Canceled)

18. (Canceled)_

REMARKS

Reconsideration of the application is respectfully requested.
5 Claims 1-16 are pending in the current application. Claim 17
was canceled in this amendment to facilitate the prosecution
of this application. Claim 18 was previously canceled. No
new matter has been added to the application. Applicants
noticed that the first page of the Office action has 18 April
10 2005 as the filing date. This is incorrect. The correct
filing date is 26 March 2004. Appropriate correction is
respectfully requested.

1. Objections to Claims 7-8

15

Claims 7 and 8 were objected to. Claims 7 and 8 have now been
amended and should be in full conformance.

2. Rejection of Claim 1 As Being Indefinite Under §112

20

Claim 1 was rejected under §112 as being indefinite because it
is unclear what the statement "said other address" refers to.
Claim 1 has now been amended and should fully conform to the
requirements of §112. Claims 2, 5, 10-13 and 16 have also
25 been amended for consistency.

3. Rejection of Claims 1-8, 10-14 and 16-17 Under §102

Claims 1-8, 10-14 and 16-17 were rejected under §102 as being
30 anticipated by Ala-Laurila (US 6,587,680). This rejection is
respectfully traversed. No new matter has been added to this
application.

Claim 1 has been amended to clarify that it is only the first
35 terminal that switches from the first address to the new

address while the original address of the second terminal remains the same in the secure connection so that the secure connection is registered between the new address of the first terminal and the original address of the second terminal.

5

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 first terminal changing from the first address to a new address and registering a secure connection between the new address of the first terminal and the original address of the second terminal to be the secure connection to be used. Such steps are not taught or suggested in the cited references.

15

The Examiner states at the bottom of page 3 and at the top of page 4 of the Office action that Ala teaches "registering a secure connection between said other address and the other terminal address to be at least one of the active connections to be used" by referring to col. 7, line 48 - col. 8, line 41 of the Ala reference. It should be noted that both the original claim 1 and the amended claim 1 require that the same address of the other terminal is used in the secure connection both before and after the mobile terminal has changed from the first address to the new address. For clarity, the amended claim 1 has now been amended to specify that it is only the first terminal that changes from the first address to the new

25

address while the original address of the second terminal remains un-changed in the secure connection so that the secure connection is registered between the new address of the first terminal and the original address of the second terminal.

5

It is submitted that Ala completely fails to teach or suggest these steps. Ala is void any discussion of teaching of a registering a secure connection between the new address of the first terminal and the original address of the second terminal. 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 new address and a new access point is established between the mobile terminal at the new 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. When the mobile terminal moves from a first address to a new address, the access points at the other end are changed also (AP old -> AP new). In other words, when the mobile terminal moves from cell 18 to cell 118 the other end-point of the secure connection changes also i.e. from AP 14 to AP 114.

The transfer of the access point AP 14 to AP 114 (including the transfer of the keys, see e.g. col. 8, lines 35-41) means that a new security connection has to be created and the

original security connection is destroyed from the access
point AP 14. In other words, the new access point AP 114
creates the new security connection (see for example claim 1)
for itself and the mobile terminal updates its security
5 connection to be in accordance to the requirements of access
point 114.

In col. 5, lines 51-58, Ala explains that the new AP requests
the keys and other information that is transferred from the
10 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, Ala fails to teach or suggest
registering a secure connection between the new address of the
first terminal and the original address of the second terminal
15 to be the secure connection to be used, as required by the
amended claim 1.

It is submitted that it would not make sense to registering
the secure connection between the new address of the first
20 terminal and the original address of the second terminal (i.e.
access point) because the new security association has already
been set up between the new AP of the second terminal and the
new address of the first terminal. When the mobile terminal
connects to the new AP, the security association has already
25 been set up for the first terminal so there is no incentive to
register a secure connection between the second address of the

first terminal and the old AP of the second terminal. In fact, the old AP has been disconnected so why register a secure connection thereto.

5 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 steps of the first
10 terminal changing from the first address to a new address and registering a secure connection between the new address and the original address of the second terminal to be the secure connection to be used.

15 In summary, there is no registration of the secure connection between the new address of Ala-Laurila's mobile terminal and the original address of the second terminal (AP), as required by the amended claim 1.

20 Therefore, all of the limitations of the amended claim 1 are not anticipated by Ala-Laurila and the anticipation rejection should be withdrawn.

Claims 2-8, 10-14 and 16 are submitted to be allowable because
25 they depend upon the allowable base claim 1 and because each claim includes limitations that are not taught or suggested in

the cited reference.

Claim 9 was rejected under §103 as being obvious over Ala-
Laurila in view of Takagi. This rejection is respectfully
5 traversed.

Claim 9 is submitted to be allowable because it depends upon
the allowable base claim 1 and because the claim includes
limitations that are not taught or suggested in the cited
10 references.

Claim 15 was rejected under §103 as being obvious over Ala-
Laurila in view of Jorgensen. This rejection is respectfully
traversed.

15
Claim 15 is submitted to be allowable because it depends upon
the allowable base claim 1 and because the claim includes
limitations that are not taught or suggested in the cited
references.

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

5

Respectfully submitted,

FASTH LAW OFFICES

10

/rfasth/

Rolf Fasth

15

Registration No. 36,999

Attorney Docket No. 290.1053USN

20

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

25

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

cc: Lisbeth Soderman, Borenus
(Your ref: S00052US)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Sami Vaarala, et al. Art Unit 2432
Confirmation No. 2431

Serial No. 10/490,933

CERTIFICATE OF MAILING

Filed: 18 April 2005

I HEREBY CERTIFY THAT THIS PAPER AND THE DOCUMENTS
REFERRED TO AS BEING ATTACHED OR ENCLOSED HERewith
ARE BEING SUBMITTED ELECTRONICALLY TO THE UNITED
STATES PATENT AND TRADEMARK OFFICE 10 January 2009.

For: METHOD AND SYSTEM FOR
ENSURING SECURE FORWARDING OF
MESSAGES

/rfasth/

Examiner: Devin E. Almeida

Rolf Fasth

Date: 10 January 2009

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 15 October 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. 290.1053USN

Electronic Acknowledgement Receipt

EFS ID:	4591129
Application Number:	10490933
International Application Number:	
Confirmation Number:	2431
Title of Invention:	Method and system 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:	290.1053USN
Receipt Date:	10-JAN-2009
Filing Date:	18-APR-2005
Time Stamp:	14:42:46
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		AMD.PDF	36511 101ea0fbcd51d6218d58634fb1e6b14ae7a 1afc	yes	11

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	11

Warnings:

Information:

2	Miscellaneous Incoming Letter	TRX.PDF	18249	no	1
			1a8b85ce79f1d7672524160d793729905f3f6bc3		

Warnings:

Information:

Total Files Size (in bytes):		54760
-------------------------------------	--	-------

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

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

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 10/490,933	Filing Date 04/18/2005	<input type="checkbox"/> To be Mailed
---	---	----------------------------------	---------------------------------------

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

APPLICATION AS AMENDED – PART II					OTHER THAN SMALL ENTITY			
	(Column 1)	(Column 2)	(Column 3)	SMALL ENTITY	OR	SMALL ENTITY	OTHER THAN SMALL ENTITY	
AMENDMENT	01/10/2009	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)
	Total <small>(37 CFR 1.16(i))</small>	* 20	Minus	** 20	=	0	OR	X \$ =
	Independent <small>(37 CFR 1.16(h))</small>	* 2	Minus	*** 3	=	0	OR	X \$ =
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>							
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>							
				TOTAL ADD'L FEE		0	OR	TOTAL ADD'L FEE

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

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.
10/490,933	04/18/2005	Sami Vaarala	290.1053USN	2431

33369 7590 03/30/2009
FASTH LAW OFFICES (ROLF FASTH)
26 PINECREST PLAZA, SUITE 2
SOUTHERN PINES, NC 28387-4301

EXAMINER

ALMEIDA, DEVIN E

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

2432

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

03/30/2009

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. 10/490,933	Applicant(s) VAARALA ET AL.	
	Examiner DEVIN ALMEIDA	Art Unit 2432	

-- 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 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) 1-16 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) 1-16 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) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

This action is in response to the papers filed 1/10/2009.

Response to Arguments

Applicant's arguments with respect to the address of the second terminal that does not change have been fully considered but they are not persuasive. According to column 7 line 46 – column 8 line 41 only the given position of mobile terminal 12 changes from cell 18 to cell 118 during a given communication session. The first mobile terminal during the communication session switches cell but the communication session is still maintained with the end device (second device) therefor minimizing any interruption of real-time services such as Voice over IP (VOIP) and video distribution. The access point is just an intermediary for the secure session not the second device that the session is with.

Claim Rejections - 35 USC § 102

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

A person shall be entitled to a patent unless –

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

Claims 1-8, 10-14, 16 and 17 rejected under 35 U.S.C. 102(e) as being anticipated by Ala-Laurila (U.S. 6,587,680).

With respect to claim 1 a method for ensuring secure forwarding of a message in a telecommunication network (see abstract i.e. radio communications system), comprising: providing a first terminal from which the message is sent and a second terminal to which the message is sent (see abstract):

a) establishing a secure connection between a first address of the first terminal (mobile terminal) and an original address of the second terminal (another of the plurality of mobile terminals of the wireless communication network), the secure connection defining the first and original addresses of the first and second terminals (see column 6 lines 25-50),

b) the first terminal (mobile terminal address with old access point) changing from the first address to a new address (mobile terminal address new access point) (see column 7 line 46 – column 8 line 41), and

c) registering a secure connection between the new address and the original address of the second terminal to be the secure connection to be used (see column 7 line 46 – column 8 line 41).

With respect to claim 2, characterized in that a new secure connection between the new address of the first terminal and the address of the second terminal is formed for the registration in step c) if such a secure connections does not already exist (see column 7 line 46 – column 8 line 16).

With respect to claim 3, characterized in that, the secure connection is established in step a) and by forming one or more Security Associations (SAs) using the IPSec protocols (see column 9 lines 17-21).

With respect to claim 4, characterized in that the message to be forwarded consists of IP packets (see column 8 lines 1-16).

With respect to claim 5, characterized in that, after step b), when the first terminal intend to send a message from the address it has moved to it first checks whether a secure connection between the new address and the other terminal already exists (see column 8 lines 49-61).

With respect to claim 6, characterized in that the existence of the new secure connection is checked by means of a connection table (see column 7 line 56-67 i.e. available access point list).

With respect to claim 7, characterized in that, in step c), the actual connection(s) to be used is/are registered by means of a signaling message or signaling message exchange between the first terminal and the second terminal (see figure 2 and 3).

With respect to claim 8, characterized in that, the new (second) address of the first terminal is updated automatically by the second terminal when the first terminal sends a message from the new address (see column 7 line 46 – column 8 line 41).

With respect to claim 10, characterized in that a key exchange being a part of the forming of the secure connection is performed with IKE or some other automated key exchange protocol (see column 8 lines 17-22).

With respect to claim 11, characterized in that the secure connection between the new address of the first terminal and the second terminal is in step c) registered for immediate and/or later use (see column 7 line 46 – column 8 line 41).

With respect to claim 12, characterized in that the registration for later use is made by the second terminal in a connection table (see column 7 line 56-67 i.e. available access point list).

With respect to claim 13, characterized in that when sending message through the secure connection IPSec transport mode is used to secure traffic between the mobile computer and a destination computer (see column 9 lines 17-21).

With respect to claim 14, characterized in that a tunneling protocol is used together with IPSec to provide a tunneling capability (see figure 2, 3 and column 9 lines 17-21).

With respect to claim 16, characterized in that when sending message through the secure connection IPSec tunnel mode is used to secure traffic between the mobile computer and a destination computer (see figure 2, 3 and column 9 lines 17-21).

Claim Rejections - 35 USC § 103

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

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

Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ala-Laurila (U.S. 6,587,680) in view of Takagi et al (U.S. 7,143,282).

Ala-Laurila does not teach that the a key exchange being a part of the forming of the secure connection in step a) and is performed manually. Takagi teaches a key exchange being a part of the forming of the secure connection in step a) and is performed manually (see Takagi column 8 lines 29-34).

It 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 to have the Security Associations of Ala-Laurila to be set up manually as taught in Takagi by Internet Key Exchange to increase the compatibility of the system (see Takagi column 8 lines 29-34). Therefore one would have been motivated to have Security Associations be able to be set up manually by Internet Key Exchange.

Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ala-Laurila (U.S. 6,587,680) in view of Jorgensen (U.S. 6,452,915).

Ala-Laurila does not teach with respect to claim 15 where the Layer 2 Tunneling Protocol (L2TP) tunneling protocol is used together with IPsec to provide a tunneling capability. Jorgensen teaches Layer 2 Tunneling Protocol (L2TP) tunneling protocol is used together with IPsec to provide a tunneling capability (see Jorgensen column 44 lines 8-17). It 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 to have used L2TP over IPsec because L2TP can carry multiple protocols. L2TP also offers transmission

capability over non-IP networks (see Jorgensen column 44 lines 8-17). Therefore one would have been motivated to have used L2TP over IPsec.

Conclusion

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

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


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Devin Almeida whose telephone number is 571-270-1018. The examiner can normally be reached on Monday-Thursday from 7:30 A.M. to 5:00 P.M. The examiner can also be reached on alternate Fridays from 7:30 A.M. to 4:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on 571-272-3799. 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).

/Devin Almeida/
Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432

Index of Claims 	Application/Control No. 10490933	Applicant(s)/Patent Under Reexamination VAARALA ET AL.
	Examiner DEVIN ALMEIDA	Art Unit 2432

✓	Rejected
=	Allowed

-	Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

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

CLAIM		DATE							
Final	Original	10/08/2008	03/18/2009						
	1	✓	✓						
	2	✓	✓						
	3	✓	✓						
	4	✓	✓						
	5	✓	✓						
	6	✓	✓						
	7	✓	✓						
	8	✓	✓						
	9	✓	✓						
	10	✓	✓						
	11	✓	✓						
	12	✓	✓						
	13	✓	✓						
	14	✓	✓						
	15	✓	✓						
	16	✓	✓						
	17	✓	-						
	18	-	-						

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

Application Number	10490933	Filing Date	2005-04-18	Docket Number (if applicable)	290.1053USN	Art Unit	2432
First Named Inventor	Sami Vaarala			Examiner Name	Devin E. Almeida		

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

Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

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

Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

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

Other _____

Enclosed

Amendment/Reply

Information Disclosure Statement (IDS)

Affidavit(s)/ Declaration(s)

Other _____

MISCELLANEOUS

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

Other _____

FEES

The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to
Deposit Account No 060243

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Patent Practitioner Signature

Applicant Signature

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

Signature of Registered U.S. Patent Practitioner			
Signature	/rfasth/	Date (YYYY-MM-DD)	2009-05-22
Name	Rolf Fasth	Registration Number	36999

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

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

Privacy Act Statement

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

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

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

RF:ss 5/22/09

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
 In re application of **EXPEDITED PROCEDURE UNDER 37**
CFR 1.114
 Sami Vaarala, Antti Art Unit 2432
 Nuopponen, Panu Pietikainen Confirmation No. 2431

Serial No. 10/490,933

CERTIFICATE OF MAILING

Filed: 18 April 2005
 For: METHOD AND SYSTEM FOR
 ENSURING SECURE
 FORWARDING OF MESSAGES

I HEREBY CERTIFY THAT THIS PAPER AND THE DOCUMENTS
 REFERRED TO AS BEING ATTACHED OR ENCLOSED HERewith
 ARE BEING SUBMITTED ELECTRONICALLY TO THE UNITED
 STATES PATENT AND TRADEMARK OFFICE ON 22 May 2009.

Examiner: Devin E. Almeida /rfasth/

Date: 22 May 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 30 March 2009.
- (X) Request for Continued Examination (RCE)
- (X) The Commissioner is hereby authorized to charge any fees which may be required in connection with the filing of this correspondence, or credit over-payment, to Account No. 06-0243.

Respectfully submitted,

FASTH LAW OFFICES

/rfasth/

 Rolf Fasth
 Registration No. 36,999

Attorney Docket No. 290.1053USN

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:	10490933			
Filing Date:	18-Apr-2005			
Title of Invention:	Method and system for ensuring secure forwarding of messages			
First Named Inventor/Applicant Name:	Sami Vaarala			
Filer:	Rolf Fasth/Sloan Smith			
Attorney Docket Number:	290.1053USN			
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:	5382585
Application Number:	10490933
International Application Number:	
Confirmation Number:	2431
Title of Invention:	Method and system 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:	290.1053USN
Receipt Date:	22-MAY-2009
Filing Date:	18-APR-2005
Time Stamp:	11:28:25
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	6826
Deposit Account	060243
Authorized User	
<p>The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:</p> <ul style="list-style-type: none"> Charge any Additional Fees required under 37 C.F.R. 1.492 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees) 	

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

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

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		AMD.PDF	37955 09c2f09f019f3312a019e817fb5fcd450302c777	yes	13
Multipart Description/PDF files in .zip description					
	Document Description		Start		End
	Amendment Submitted/Entered with Filing of CPA/RCE		1		1
	Claims		2		4
	Applicant Arguments/Remarks Made in an Amendment		5		13
Warnings:					
Information:					
2	Request for Continued Examination (RCE)	RCE.PDF	36006 ab7a868cfaf04cc983303cd39aede106e507f6fa	no	3
Warnings:					
This is not a USPTO supplied RCE SB30 form.					
Information:					
3	Miscellaneous Incoming Letter	TRX.PDF	18565 e23b2380c222996c78de5f6924ec482a43e7a61b	no	1
Warnings:					
Information:					
4	Fee Worksheet (PTO-875)	fee-info.pdf	29916 061a03823f46b299904f2b53f313ec3ce86b8c23	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			122442		

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 2432

5 Sami Vaarala, Antti Nuopponen, Panu Pietikainen

Serial No. 10/490,933

10 Filed: 18 April 2005

For: METHOD AND NETWORK FOR ENSURING SECURE FORWARDING OF
MESSAGES

15 Examiner: Devin E. Almeida

Date: 22 May 2009

Attorney Docket Number: 290.1053USN

20

AMENDMENT

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

This is in response to the Office action of 30 March
2009. Please amend the above-identified patent application as
follows:

30

In the Claims:

Amend the claims as follows:

- 5
1. (Currently amended) A method for ensuring secure forwarding of a message in a telecommunication network, comprising: providing a first terminal from which the message is sent and a second terminal to which the message is sent,
- 10 a) establishing a first secure connection between a first address of the first terminal and an original address of the second terminal, the first secure connection extending between ~~defining~~ the first address of the first terminal and the original addresses of the ~~first and~~ second terminals,
- 15 b) the first terminal changing from the first address to a new address, ~~and~~
- c) registering a second secure connection extending between the new address of the first terminal and the original address of the second terminal, ~~to be the secure connection to be~~
- 20 ~~used.~~ and
using the second secure connection extending between the new address of the first terminal and the original address of the second terminal.
- 25 2. (Currently amended) The method of claim 1, ~~characterized in that~~ wherein a new secure connection between the new address of the first terminal and the address of the second terminal is formed for the registration in step c) if such a secure connections does not already exist.
- 30 3. (Currently amended) The method of claim 1, ~~characterized in that,~~ wherein the secure connection is established in step a) and by forming one or more Security Associations (SAs) using the IPsec protocols.

35

4. (Currently amended) The method of claim 1, ~~characterized in that~~ wherein the message to be forwarded consists of IP packets.

5 5. (Currently amended) The method of claim 1, ~~characterized in that~~ wherein, after step b), when the first terminal ~~intend to~~ sends a message from the address ~~it~~ the first terminal has moved to, the first terminal ~~it~~ first checks whether a secure connection between the new address and the second terminal
10 already exists.

6. (Currently amended) The method of claim 5, ~~characterized in that~~ wherein ~~the~~ an existence of the ~~new~~ second secure connection is checked by means of a connection table.

15 7. (Currently amended) The method of claim 1, ~~characterized in that,~~ wherein in step c), the actual connection(s) to be used is/are registered by means of a signaling message or signaling message exchange between the first terminal and the second
20 terminal.

8. (Currently amended) The method of claim 1, ~~characterized in that,~~ wherein the new ~~(second)~~ address of the first terminal is updated automatically by the second terminal when the first
25 terminal sends a message from the new address.

9. (Currently amended) The method of claim 1, ~~characterized in that the~~ wherein a key exchange is ~~being~~ a part of ~~the~~ forming of the first secure connection in step a) and is performed
30 manually.

10. (Currently amended) The method of claim 2, ~~characterized in that~~ wherein a key exchange ~~being~~ is a part of ~~the~~ forming of the secure connection ~~is~~ performed with IKE ~~or some other~~ automated key exchange protocol.
35

11. (Currently amended) The method of claim 1, ~~characterized in that~~ wherein the second secure connection between the new address of the first terminal and the second terminal is in
5 step c) registered for immediate and/or later use.

12. (Currently amended) The method of claim 11, ~~characterized in that~~ wherein the registration for later use is made by the second terminal in a connection table.
10

13. (Currently amended) The method of claim 3, ~~characterized in that~~ wherein when sending message through the secure connection, IPSec transport mode is used to secure traffic between ~~the~~ a mobile computer and a destination computer.
15

14. (Currently amended) The method of claim 13, ~~characterized in that~~ wherein a tunneling protocol is used together with IPSec to provide a tunneling capability.

15. (Currently amended) The method of claim 14, ~~characterized in that~~ wherein where ~~the~~ a Layer 2 Tunneling Protocol (L2TP) tunneling protocol is used together with IPSec to provide a tunneling capability.
20

16. (Currently amended) The method of claim 3, ~~characterized in that~~ wherein when sending message through the secure connection, an IPSec tunnel mode is used to secure traffic between ~~the~~ a mobile computer and a destination computer.
25

30 17. (Canceled)

18. (Canceled)

REMARKS

Reconsideration of the application is respectfully requested.
5 Claims 1-16 are pending in the current application. No new
matter has been added to the application. Figs. 1-2 show that
the first secure connection extends between the first address
of the first terminal and the original address of the second
terminal and that the second secure connection extends between
10 the new address of the first terminal and the same original
address of the second terminal. These features are also
described on pages 16-21 in the priority document WO
03/030488.

15 1. Incorrect filing date on Office action

Applicants pointed out in the previous response that the first
Office action of 15 October 2008 had "18 April 2005" as the
filing date and that the correct filing date is 26 March 2004.
20 Applicants noticed that the second Office action still has 18
April 2005 as the filing date. PTO has not corrected the
filing date despite the request. Applicants again request
that the filing date is corrected to 26 March 2004.

25 2. Examiner's "Response to Arguments"

On page 2 of the Office action the Examiner states that only
"the mobile terminal 12 changes from cell 18 to cell 118
during a given communication session" and that the
30 "communication session is still maintained with the end device
(second device)." The Examiner either seems to infer that the
second device must physically move also or the Examiner has
missed the express statement in col. 7, line 46 - col. 8, line
41 that the end address of the security association at the end
35 device (second device) switches from AP 14 to AP 114. More

particularly, col. 8, lines 6-9 states: "In accordance with the invention, this established and shared security association is transferred from old-AP 14 to new-AP 114 in a secure fashion, as mobile terminal moves from cell 18 to cell 118." Additionally, col. 8, lines 23-29 states: "Later, when mobile terminal 12 moves from cell 18 and its AP 14 to cell 118 and its AP 114, authentication during the handover process is achieved by the invention's simple challenge/response procedure. Also, security associations are transferred between old-AP 14 and new-AP 114, thus avoiding the need for a new key exchange during a handover from old-AP 14 to new-AP 114." It is submitted that the above cited text sections clearly describe a hand-over process in which the address of the security association at the end device changes from old-AP 14 to new-AP 114.

The Examiner states that the "access point is just an intermediary for the secure session not the second device that the session is with." It should be understood that the amended claim 1 requires that the first secure connection extends between the first address of the first terminal and the original address of the second terminal and that the second secure connection extends between the new address of the first terminal and the original address of the second terminal. This is to clarify that the original address of the second terminal refers to the end point of the security connection and not to the physical location of the second terminal.

Col. 6, lines 41-49 of Ala-Laurila, explain that the APs 14, 114 are base stations or remote antenna devices (RADs) and that the term access point is used to identify devices that form points of access to the network infrastructure of communication system 10. This means AP14 and AP 114 are the end address of the two security associations. As pointed out

above, the amended claim 1 requires that the first secure connection has the same original address at the second terminal as the second secure connection. This means the end point of the first secure connection is the same as the end point of the second secure connection. This is equivalent to the security association of Ala-Laurila that extends between the mobile terminal 12 when in cell 18 and the access point 14 of the base station. The first security association of Ala-Laurila thus extends between the mobile terminal 12 when in cell 18 and the access point 14 of the base station. However, the second security association extends between the mobile terminal 12 when in cell 118 and the access point 114 (not the access point 14) of the base station. In other words, the address AP114 of the second security association at the base station is clearly different from the address AP 14 of the first security association.

3. Rejection of Claims 1-8, 10-14 and 16-17 Under §102

Claims 1-8, 10-14 and 16-17 were rejected under §102 as being anticipated by Ala-Laurila (US 6,587,680). This rejection is respectfully traversed. No new matter has been added to this application.

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

Claim 1 has been amended to clarify that the first secure connection extends between the first address of the first terminal and the original address of the second terminal and that the second secure connection extends between the second address of the first terminal and the same original address of the second terminal. This is to clarify that the original address of the second terminal refers to the end point of the

secure connections and not to the physical location of the second terminal.

5 It is submitted that Ala-Laurila fails, among other things, to teach or suggest the step of registering a second secure connection extending between the new address of the first terminal and the original address of the second terminal. In contrast, Ala-Laurila teaches registering the address AP 114
10 of the second security association that is different from the original address AP 14 of the first security association. Ala-Laurila also fails to teach the step of using the second secure connection extending between the new address of the first terminal and the same original address of the second
15 terminal.

As explained above, Ala-Laurila teaches, in contrast, the step of changing the address of the second security association from AP 14 to AP 114 at the base station during the hand-over
20 process. In col. 8, lines 57-61, Ala-Laurila teaches that the mobile terminal 12 is even disconnected from old-AP 14 and connected new-AP 114 where the new security association 35 has already been established. It is submitted that the security association 35 is equivalent to the second secure connection
25 of the amended claim 1. However, one important difference compared to the present invention is that the security association 35 of Ala-Laurila has both a new address (cell

118) at the mobile terminal 12 and the new-AP 114 address at the base station (second terminal).

It is submitted that Ala-Laurila completely fails to teach or
5 suggest the required steps of the amended claim 1. Ala-Laurila is void any discussion of teaching of a registering a second secure connection extending between the new address of the first terminal and the original address of the second terminal. As indicated above, Ala-Laurila merely discloses a
10 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 new address and a new access point is established between the mobile terminal at the new address that belongs to a new coverage area of the new
15 access point. Ala-Laurila's system requires a change of the location of both the mobile terminal and the access points. When the mobile terminal moves from a first address to a new address, the access points at the other end of the security associations are changed also (AP old -> AP new). In other
20 words, when the mobile terminal moves from cell 18 to cell 118 the other end-point of the secure connection changes also i.e. from AP 14 to AP 114.

The transfer of the access point AP 14 to AP 114 (including
25 the transfer of the keys, see e.g. col. 8, lines 35-41) means that a new security connection has to be created and the original security connection is destroyed from the access

point AP 14. In other words, the new access point AP 114 creates the new security connection (see for example claim 1) for itself and the mobile terminal updates its security connection to be in accordance to the requirements of access
5 point 114.

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
10 is between the two APs and not between the old AP and the mobile terminal). More importantly, Ala-Laurila fails to teach or suggest using the second secure connection extending between the new address of the first terminal and the original address of the second terminal, as required by the amended
15 claim 1.

It is submitted that it would not make sense to use the first secure connection between the new address of the first terminal and the original address of the second terminal (i.e.
20 access point) because the new security association 35 has already been set up between the new AP of the second terminal and the new address of the first terminal. When the mobile terminal connects to the new AP, the security association 35 has already been set up for the first terminal so there is no
25 incentive to register a secure connection between the second address of the first terminal and the old AP of the second

terminal. In fact, the old AP has been disconnected so why register a secure connection thereto.

Applicants fails to see why a person of ordinary skill in the art would look to Ala-Laurila 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 steps of the first terminal changing from the first address to a new address and using the second secure connection extending between the new address and the original address of the second terminal.

In summary, there is no step of using the second secure connection extending between the new address of Ala-Laurila's mobile terminal and the original address of the second terminal (AP), as required by the amended claim 1.

Therefore, all of the limitations of the amended claim 1 are not anticipated by Ala-Laurila and the anticipation rejection should be withdrawn.

Claims 2-8, 10-14 and 16 are submitted to be allowable because they depend upon the allowable base claim 1 and because each claim includes limitations that are not taught or suggested in the cited reference.

Claim 9 was rejected under §103 as being obvious over Alalaurila in view of Takagi. This rejection is respectfully traversed.

5

Claim 9 is submitted to be allowable because it depends upon the allowable base claim 1 and because the claim includes limitations that are not taught or suggested in the cited references.

10

Claim 15 was rejected under §103 as being obvious over Alalaurila in view of Jorgensen. This rejection is respectfully traversed.

15

Claim 15 is submitted to be allowable because it depends upon the allowable base claim 1 and because the claim includes limitations that are not taught or suggested in the cited references.

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

5

Respectfully submitted,

FASTH LAW OFFICES

10

/rfasth/

Rolf Fasth

15

Registration No. 36,999

Attorney Docket No. 290.1053USN

20

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

25

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

cc: Lisbeth Soderman, Borenien
(Your ref: S00052US)

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

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 10/490,933	Filing Date 04/18/2005	<input type="checkbox"/> To be Mailed
---	---	----------------------------------	---------------------------------------

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

APPLICATION AS AMENDED – PART II					OTHER THAN SMALL ENTITY			
	(Column 1)	(Column 2)	(Column 3)	SMALL ENTITY	OR	SMALL ENTITY	OTHER THAN SMALL ENTITY	
AMENDMENT	05/22/2009	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)
	Total <small>(37 CFR 1.16(i))</small>	* 16	Minus	** 20	=	0	X \$ =	X \$ =
	Independent <small>(37 CFR 1.16(h))</small>	* 1	Minus	*** 3	=	0	X \$ =	X \$ =
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>							
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>							
					TOTAL ADD'L FEE	0	TOTAL ADD'L FEE	

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

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

Legal Instrument Examiner:
/BRENDA WEBB/

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



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.
10/490,933	04/18/2005	Sami Vaarala	290.1053USN	2431

33369 7590 06/12/2009
FASTH LAW OFFICES (ROLF FASTH)
26 PINECREST PLAZA, SUITE 2
SOUTHERN PINES, NC 28387-4301

EXAMINER

ALMEIDA, DEVIN E

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

2432

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

06/12/2009

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. 10/490,933	Applicant(s) VAARALA ET AL.	
	Examiner DEVIN ALMEIDA	Art Unit 2432	

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

Period for Reply

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

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

Status

- 1) Responsive to communication(s) filed on 22 May 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) 1-16 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) 1-16 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

This action is in response to the papers filed 5/22/2009.

Response to Arguments

Applicant's arguments with respect to the address of the second terminal that does not change have been fully considered but they are not persuasive. According to column 7 line 46 – column 8 line 41 only the given position of mobile terminal 12 changes from cell 18 to cell 118 during a given communication session. The first mobile terminal during the communication session switches cell but the communication session is still maintained with the end device (second device) therefore minimizing any interruption of real-time services such as Voice over IP (VOIP) and video distribution. **The access point is just an intermediary for the secure session not the second device that the session is with.**

Applicant's arguments have been fully considered but they are not persuasive. Applicant is arguing the claim not the way they are mapped out in the rejection below. The second device is not the access point that the mobile terminal uses but the end device that the mobile terminal is receiving real-time services such as Voice over IP (VOIP) and video distribution from as taught in column 7 line 46 – column 8 line 41.

Claim Rejections - 35 USC § 102

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

A person shall be entitled to a patent unless –

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

Claims 1-8, 10-14, 16 and 17 rejected under 35 U.S.C. 102(e) as being anticipated by Ala-Laurila (U.S. 6,587,680).

With respect to claim 1 a method for ensuring secure forwarding of a message in a telecommunication network (see abstract i.e. radio communications system), comprising: providing a first terminal from which the message is sent and a second terminal (end device) to which the message is sent (see abstract):

a) establishing a first secure connection between a first address of the first terminal (mobile terminal) and an original address of the second terminal (another of the plurality of mobile terminals of the wireless communication network), the first secure connection extending between the first address of the first terminal and the original address of the second terminal (see column 6 lines 25-50),

b) the first terminal (mobile terminal address with old access point) changing from the first address to a new address (mobile terminal address new access point) (see column 7 line 46 – column 8 line 41),

c) registering a second secure connection extending between the new address of the first terminal and the original address of the second terminal (see column 7 line 46 – column 8 line 41) and using the second secure connection extending between the new

address of the first terminal and the original address of the second terminal (see column 7 line 46 – column 8 line 41).

With respect to claim 2, wherein a new secure connection between the new address of the first terminal and the address of the second terminal is formed for the registration in step c) if such a secure connections does not already exist (see column 7 line 46 – column 8 line 16).

With respect to claim 3, characterized in that, the secure connection is established in step a) and by forming one or more Security Associations (SAs) using the IPSec protocols (see column 9 lines 17-21).

With respect to claim 4, wherein the message to be forwarded consists of IP packets (see column 8 lines 1-16).

With respect to claim 5, wherein, after step b), when the first terminal intend to send a message from the address it has moved to it first checks whether a secure connection between the new address and the other terminal already exists (see column 8 lines 49-61).

With respect to claim 6, wherein the existence of the new secure connection is checked by means of a connection table (see column 7 line 56-67 i.e. available access point list).

With respect to claim 7, wherein, in step c), the actual connection(s) to be used is/are registered by means of a signaling message or signaling message exchange between the first terminal and the second terminal (see figure 2 and 3).

With respect to claim 8, wherein the new (second) address of the first terminal is updated automatically by the second terminal when the first terminal sends a message from the new address (see column 7 line 46 – column 8 line 41).

With respect to claim 10, wherein a key exchange being a part of the forming of the secure connection is performed with IKE or some other automated key exchange protocol (see column 8 lines 17-22).

With respect to claim 11, wherein the secure connection between the new address of the first terminal and the second terminal is in step c) registered for immediate and/or later use (see column 7 line 46 – column 8 line 41).

With respect to claim 12, wherein the registration for later use is made by the second terminal in a connection table (see column 7 line 56-67 i.e. available access point list).

With respect to claim 13, wherein when sending message through the secure connection IPSec transport mode is used to secure traffic between the mobile computer and a destination computer (see column 9 lines 17-21).

With respect to claim 14, wherein a tunneling protocol is used together with IPSec to provide a tunneling capability (see figure 2, 3 and column 9 lines 17-21).

With respect to claim 16, wherein when sending message through the secure connection IPSec tunnel mode is used to secure traffic between the mobile computer and a destination computer (see figure 2, 3 and column 9 lines 17-21).

Claim Rejections - 35 USC § 103

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

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

Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ala-Laurila (U.S. 6,587,680) in view of Takagi et al (U.S. 7,143,282).

Ala-Laurila does not teach that the a key exchange being a part of the forming of the secure connection in step a) and is performed manually. Takagi teaches a key exchange being a part of the forming of the secure connection in step a) and is performed manually (see Takagi column 8 lines 29-34).

It 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 to have the Security Associations of Ala-Laurila to be set up manually as taught in Takagi by Internet Key Exchange to increase the compatibility of the system (see Takagi column 8 lines 29-34). Therefore one would have been motivated to have Security Associations be able to be set up manually by Internet Key Exchange.

Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ala-Laurila (U.S. 6,587,680) in view of Jorgensen (U.S. 6,452,915).

Ala-Laurila does not teach with respect to claim 15 where the Layer 2 Tunneling Protocol (L2TP) tunneling protocol is used together with IPSec to provide a tunneling capability. Jorgensen teaches Layer 2 Tunneling Protocol (L2TP) tunneling protocol is

used together with IPsec to provide a tunneling capability (see Jorgensen column 44 lines 8-17). It 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 to have used L2TP over IPsec because L2TP can carry multiple protocols. L2TP also offers transmission capability over non-IP networks (see Jorgensen column 44 lines 8-17). Therefore one would have been motivated to have used L2TP over IPsec.

Conclusion


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Devin Almeida whose telephone number is 571-270-1018. The examiner can normally be reached on Monday-Thursday from 7:30 A.M. to 5:00 P.M. The examiner can also be reached on alternate Fridays from 7:30 A.M. to 4:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on 571-272-3799. 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.

/Devin Almeida/
Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432

Index of Claims 	Application/Control No. 10490933	Applicant(s)/Patent Under Reexamination VAARALA ET AL.
	Examiner DEVIN ALMEIDA	Art Unit 2432

✓	Rejected
=	Allowed

-	Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

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

CLAIM		DATE							
Final	Original	10/08/2008	03/18/2009	06/08/2009					
	1	✓	✓	✓					
	2	✓	✓	✓					
	3	✓	✓	✓					
	4	✓	✓	✓					
	5	✓	✓	✓					
	6	✓	✓	✓					
	7	✓	✓	✓					
	8	✓	✓	✓					
	9	✓	✓	✓					
	10	✓	✓	✓					
	11	✓	✓	✓					
	12	✓	✓	✓					
	13	✓	✓	✓					
	14	✓	✓	✓					
	15	✓	✓	✓					
	16	✓	✓	✓					
	17	✓	-	-					
	18	-	-	-					

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of Art Unit 2432

5 Sami Vaarala, Antti Nuopponen, Panu Pietikainen

Serial No. 10/490,933

10 Filed: 26 March 2004

For: METHOD AND NETWORK FOR ENSURING SECURE FORWARDING OF
MESSAGES

15 Examiner: Devin E. Almeida

Date: 23 July 2009

Attorney Docket Number: 290.1053USN

20

AMENDMENT

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

This is in response to the Office action of 12 June
2009. Please amend the above-identified patent application as
follows:

In the specification:

Please change the paragraph starting on page 17, line 30 as shown below:

5

Upon receiving the encapsulated IP packet, the home server unwraps the IP-IP tunnel, and proceeds in step 2 of figure 1 ~~2~~ with routing a packet indicated with IP/Data, which packet was inside the encapsulation (inside the outer IP header). The routing is performed in accordance with the inner destination address, the packet now, after the unwrapping, having the home address of the mobile terminal as its source address and host X as its destination address.

10

15

In the Claims:

Amend the claims as follows:

- 5
1. (Currently amended) A method for ensuring secure forwarding of a message in a telecommunication network, comprising: providing a first terminal from which the message is sent and a second terminal to which the message is sent,
- 10 a) establishing a first secure connection extending between a first end-point at ~~address of~~ the first terminal and an original end-point at ~~address of~~ the second terminal, ~~the first secure connection extending between the first address of the first terminal and the original address of the second~~
- 15 ~~terminal,~~
- b) the first terminal changing from ~~the~~ a first address to a new address,
- c) registering a second secure connection extending between ~~the new address of the first terminal~~ a new end-point and the
- 20 original end-point of the first secure connection ~~address of~~ ~~the second terminal,~~ and
- using the second secure connection extending between the new ~~address of the first terminal~~ end-point and the original end-point of the first secure connection ~~address of the second~~
- 25 ~~terminal.~~
2. (Previously presented) The method of claim 1, wherein a new secure connection between the new address of the first terminal and the address of the second terminal is formed for
- 30 the registration in step c) if such a secure connections does not already exist.
3. (Previously presented) The method of claim 1, wherein the secure connection is established in step a) and by forming one
- 35 or more Security Associations (SAs) using the IPsec protocols.

4. (Previously presented) The method of claim 1, wherein the message to be forwarded consists of IP packets.

5 5. (Previously presented) The method of claim 1, wherein, after step b), when the first terminal sends a message from the address the first terminal has moved to, the first terminal first checks whether a secure connection between the new address and the second terminal already exists.

10

6. (Previously presented) The method of claim 5, wherein an existence of the second secure connection is checked by means of a connection table.

15

7. (Previously presented) The method of claim 1, wherein in step c), the actual connection(s) to be used is/are registered by means of a signaling message or signaling message exchange between the first terminal and the second terminal.

20

8. (Previously presented) The method of claim 1, wherein the new address of the first terminal is updated automatically by the second terminal when the first terminal sends a message from the new address.

25

9. (Previously presented) The method of claim 1, wherein a key exchange is a part of forming of the first secure connection in step a) and is performed manually.

30

10. (Previously presented) The method of claim 2, wherein a key exchange is a part of forming of the secure connection performed with IKE.

35

11. (Previously presented) The method of claim 1, wherein the second secure connection between the new address of the first terminal and the second terminal is in step c) registered for

immediate and/or later use.

12. (Previously presented) The method of claim 11, wherein the registration for later use is made by the second terminal in a connection table.
5

13. (Previously presented) The method of claim 3, wherein when sending message through the secure connection, IPSec transport mode is used to secure traffic between a mobile computer and a destination computer.
10

14. (Previously presented) The method of claim 13, wherein a tunneling protocol is used together with IPSec to provide a tunneling capability.
15

15. (Previously presented) The method of claim 14, wherein where a Layer 2 Tunneling Protocol (L2TP) tunneling protocol is used together with IPSec to provide a tunneling capability.

16. (Previously presented) The method of claim 3, wherein when sending message through the secure connection, an IPSec tunnel mode is used to secure traffic between a mobile computer and a destination computer.
20

17. (Canceled)
25

18. (Canceled)

REMARKS

Reconsideration of the application is respectfully requested.
5 Claims 1-16 are pending in the current application. No new
matter has been added to the application. Claim 1 has now
been amended to clarify that it is not the physical address of
the first and second terminal that is important but the end-
points of the secure connections. More particularly, the end-
10 points of the second secure connection are the new end-point
and the original end-point of the first secure connection.
Support may be found in the abstract and in paragraphs [0010,
0013, 0108, 0122 and 0143-0144] that explain that the secure
connections extend between the end-points of the secure
15 connections and that the end-points define the secure
connections.

1. Incorrect filing date on Office action

20 Applicants pointed out in the previous response that the first
Office action of 15 October 2008 had "18 April 2005" as the
filing date and that the correct filing date is 26 March 2004.
Applicants noticed that the second Office action still has 18
April 2005 as the filing date. PTO has not corrected the
25 filing date despite the request. The Examiner did not seem to
have corrected this error. **Applicants make a THIRD request to
have the filing date corrected to 26 March 2004. Applicants
respectfully request that the Examiner responds to this issue
in the next communication from USPTO.**

30

2. Examiner's "Response to Arguments"

On page 2 of the Office action the Examiner states that only
"the mobile terminal 12 changes from cell 18 to cell 118
35 during a given communication session" and that the

"communication session is still maintained with the end device (second device)." The Examiner refers to col. 7, line 46 - col. 8, line 41 of Ala-Laurila that expressly states that the end address of the security association at the end device
5 (second device) switches from AP 14 to AP 114. More particularly, col. 8, lines 6-9 states: "In accordance with the invention, this established and shared security association is transferred from old-AP 14 to new-AP 114 in a secure fashion, as mobile terminal moves from cell 18 to cell
10 118." Additionally, col. 8, lines 23-29 states: "Later, when mobile terminal 12 moves from cell 18 and its AP 14 to cell 118 and its AP 114, authentication during the handover process is achieved by the invention's simple challenge/response procedure. Also, security associations are transferred
15 between old-AP 14 and new-AP 114, thus avoiding the need for a new key exchange during a handover from old-AP 14 to new-AP 114." It is submitted that the above cited text sections clearly describe a hand-over process in which the end-points of the security associations at the end device changes from
20 old-AP 14 to new-AP 114.

More particularly, the mobile terminal in Ala-Laurila communicates by e.g. Voice Over IP with another device via the access point, but this whole path can not be a secure
25 connection. The payload traffic mentioned in col. 8, lines 13-16 and all the Figs. 2 -7 is between the mobile terminal and the access point. Actually, there is in Ala-Laurila nothing said about the communication between the access points and the VoIP at all. Especially, there is no teaching or
30 suggestion about this being a secure connection. Additionally, it should be noted that virtual private network channels are not necessarily secured, they are just controlled. Per definition, a virtual private network (VPN) does not need to have explicit security features such as
35 authentication or content encryption. For example, VPNs can

also be used to separate the traffic of different user communities over an underlying network with strong security features, or to provide access to a network via customized or private routing mechanisms.

5

It is submitted that Ala-Laurila clearly fails to teach or suggest the steps of registering and using a second secure connection that extends between the new end-point and the original end-point of the first secure connection, as required
10 by the amended claim 1. As explained above, Ala-Laurila expressly requires a transfer from the old-AP 14 to the new-AP 114 and there is no secure connection between the old-AP 14 and the cell 118. More particularly, in col. 6, lines 41-49 of Ala-Laurila explains that the APs 14, 114 are base stations
15 or remote antenna devices (RADs) and that the term access point is used to identify devices that form points of access to the network infrastructure of communication system 10. This means AP14 and AP 114 are the end points of the two security associations. As pointed out above, the amended
20 claim 1 now requires that the second secure connection has the original end-point as the first secure connection. This means the end point of the first secure connection is the same as the end point of the second secure connection. In contrast Ala-Laurila's second security association extends between the
25 mobile terminal 12 when in cell 118 and the access point 114 (not the access point 14) of the base station. In other words, the end point AP114 of the second security association at the base station is clearly different from the end-point AP 14 of the first security association.

30

3. Rejection of Claims 1-8, 10-14 and 16-17 Under §102

Claims 1-8, 10-14 and 16-17 were rejected under §102 as being anticipated by Ala-Laurila (US 6,587,680). This rejection is

respectfully traversed. No new matter has been added to this application.

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

Claim 1 has been amended to clarify that the first secure connection extends between a first end-point at the first terminal and an original end-point at the second terminal and
10 that the second secure connection extends between a new end-point and the same original end-point of the first secure connection. This is to clarify that the original end-point of the first secure connection is the same as the end-point of the second secure connection.

15

It is submitted that Ala-Laurila fails, among other things, to teach or suggest the step of registering a second secure connection extending between the new end-point and the
20 original end-point of the first secure connection. In contrast, Ala-Laurila teaches registering the end-point AP 114 of the second security association that is different from the original address AP 14 of the first security association. Ala-Laurila also fails to teach the step of using the second
25 secure connection extending between the new end-point and the same original end-point of the first secure connection.

As explained above, Ala-Laurila teaches, in contrast, the step of changing the end-point of the second security association
30 from AP 14 to AP 114 at the base station during the hand-over

process. In col. 8, lines 57-61, Ala-Laurila teaches that the mobile terminal 12 is even disconnected from old-AP 14 and connected new-AP 114 when the new (second) security association 35 is established. It is submitted that the security association 35 is equivalent to the second secure connection of the amended claim 1. However, one important difference compared to the present invention is that the security association 35 of Ala-Laurila changes both end-points (cell 118) at the mobile terminal 12 and the new-AP 114 end-point at the base station (second terminal).

It is submitted that Ala-Laurila completely fails to teach or suggest the required steps of the amended claim 1. Ala-Laurila is void any discussion of teaching of a registering a second secure connection extending between the new end-point and the original end-point of the first secure connection. As indicated above, Ala-Laurila merely discloses a conventional system for transferring a security association during a mobile terminal handover. This is not surprising since in the standardized IPSsec protocol the end points are fixed and if one of the end-points changes (for example when one terminal moves) then the secure connection must be re-defined by repeating all the key exchange messages and parameter definitions. This means when Ala-Laurila's mobile terminal is moved from a first address to a new address and a new access point is established between the mobile terminal at the new

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 end-points. When the mobile terminal moves from a first address to a new
5 address, the end-points at the other end of the security associations are changed also (AP old -> AP new). In other words, when the mobile terminal moves from cell 18 to cell 118 the other end-point of the secure connection changes also i.e. from AP 14 to AP 114.

10 The transfer of the access point AP 14 to AP 114 (including the transfer of the keys, see e.g. col. 8, lines 35-41) means that a new security connection (i.e. security connection 35) has to be created and the original security connection is
15 destroyed from the access point AP 14. In other words, the new access point AP 114 creates the new security connection 35 (see for example claim 1 of Ala-Laurila) for itself and the mobile terminal updates its security connection to be in accordance to the requirements of access point 114.

20 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
25 mobile terminal). More importantly, Ala-Laurila fails to teach or suggest using the second secure connection extending between the new end-point and the original end-point of the

first secure connection, as required by the amended claim 1.

It is submitted that it would not make sense to use a secure connection of Ala-Laurila between the new end-point and the original end-point (i.e. access point) because the new security association 35 has already been set up between the new AP (new end-point) and the new end-point at the first terminal. When the mobile terminal connects to the new AP, the security association 35, with the new two end-points, has already been set up for the first terminal so there is no incentive to register a secure connection between the new end-point and the old AP (end-point) particularly since the old AP has been disconnected.

Applicants fails to see why a person of ordinary skill in the art would look to Ala-Laurila 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 steps of the registering and using the second secure connection that extends between the new end-point and the original end-point of the first secure connection when the first terminal has changed from the first address to the new address.

In summary, the cited references fails to teach or suggest the steps of registering and using the second secure connection

extending between the new end-point of Ala-Laurila's mobile terminal and the original end-point of the first secure connection, as required by the amended claim 1.

5 Therefore, all of the limitations of the amended claim 1 are not anticipated by Ala-Laurila and the anticipation rejection should be withdrawn.

Claims 2-8, 10-14 and 16 are submitted to be allowable because
10 they depend upon the allowable base claim 1 and because each claim includes limitations that are not taught or suggested in the cited reference.

Claim 9 was rejected under §103 as being obvious over Ala-
15 Laurila in view of Takagi. This rejection is respectfully traversed.

Claim 9 is submitted to be allowable because it depends upon the allowable base claim 1 and because the claim includes
20 limitations that are not taught or suggested in the cited references.

Claim 15 was rejected under §103 as being obvious over Ala-Laurila in view of Jorgensen. This rejection is respectfully
25 traversed.

Claim 15 is submitted to be allowable because it depends upon the allowable base claim 1 and because the claim includes limitations that are not taught or suggested in the cited references.

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

5

Respectfully submitted,

FASTH LAW OFFICES

10

/rfasth/

15

Rolf Fasth
Registration No. 36,999

Attorney Docket No. 290.1053USN

20

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

25

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

cc: Lisbeth Soderman, Borenien
(Your ref: S00052US)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Sami Vaarala, et al. Art Unit 2432
Confirmation No. 2431

Serial No. 10/490,933

CERTIFICATE OF MAILING

Filed: 18 April 2005

I HEREBY CERTIFY THAT THIS PAPER AND THE DOCUMENTS
REFERRED TO AS BEING ATTACHED OR ENCLOSED HERewith
ARE BEING SUBMITTED ELECTRONICALLY TO THE UNITED
STATES PATENT AND TRADEMARK OFFICE ON 23 July 2009.

For: METHOD AND SYSTEM FOR
ENSURING SECURE FORWARDING OF
MESSAGES

/rfasth/

Examiner: Devin E. Almeida

Rolf Fasth

Date: 23 July 2009

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 June 2009.
- (X) The Commissioner is hereby authorized to charge any fees which may be required in connection with the filing of this correspondence, or credit over-payment, to Account No. 06-0243.

Respectfully submitted,

FASTH LAW OFFICES

/rfasth/

Rolf Fasth
Registration No. 36,999

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

Attorney Docket No. 290.1053USN

Electronic Acknowledgement Receipt

EFS ID:	5758073
Application Number:	10490933
International Application Number:	
Confirmation Number:	2431
Title of Invention:	Method and system 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:	290.1053USN
Receipt Date:	23-JUL-2009
Filing Date:	18-APR-2005
Time Stamp:	15:29:22
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	41129 5bee20ff2d0f5ba43db308a4c3530c2a93d6e43e	yes	15

Multipart Description/PDF files in .zip description			
Document Description	Start	End	
Amendment/Req. Reconsideration-After Non-Final Reject	1	1	
Specification	2	2	
Claims	3	5	
Applicant Arguments/Remarks Made in an Amendment	6	15	

Warnings:

Information:

2	Miscellaneous Incoming Letter	TRX.PDF	18427	no	1
			0762233e95b8ed2f3b7f16e13472a3ff918310f9		

Warnings:

Information:

Total Files Size (in bytes):	59556
-------------------------------------	-------

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

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

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 10/490,933	Filing Date 04/18/2005	<input type="checkbox"/> To be Mailed
---	---	----------------------------------	---------------------------------------

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

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

APPLICATION AS AMENDED – PART II					OTHER THAN SMALL ENTITY			
	(Column 1)	(Column 2)	(Column 3)	SMALL ENTITY	OR	SMALL ENTITY	OTHER THAN SMALL ENTITY	
				RATE (\$)		ADDITIONAL FEE (\$)		
AMENDMENT	07/23/2009	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA				
	Total <small>(37 CFR 1.16(i))</small>	* 16	Minus	** 20	=	0		
	Independent <small>(37 CFR 1.16(h))</small>	* 1	Minus	*** 3	=	0		
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>							
<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>								
					TOTAL ADD'L FEE	0	TOTAL ADD'L FEE	

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

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

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
10/490,933 04/18/2005 Sami Vaarala 290.1053USN 2431

33369 7590 11/19/2009
FASTH LAW OFFICES (ROLF FASTH)
26 PINECREST PLAZA, SUITE 2
SOUTHERN PINES, NC 28387-4301

Table with 1 column: EXAMINER
ALMEDA, DEVIN E

Table with 2 columns: ART UNIT, PAPER NUMBER
2432

Table with 2 columns: NOTIFICATION DATE, DELIVERY MODE
11/19/2009 ELECTRONIC

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

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

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

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

Office Action Summary	Application No. 10/490,933	Applicant(s) VAARALA ET AL.	
	Examiner DEVIN ALMEIDA	Art Unit 2432	

-- 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 23 July 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) 1-16 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) 1-16 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) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

This action is in response to the papers filed 5/22/2009.

Response to Arguments

Applicant's arguments with respect to the filing date. Palm has the effective filling date as 26 March 2004.

Applicant's arguments with respect to registering a second secure connection extending between a new end-point (mobile terminal address on new access point) and the original end-point of the first secure connection (the device that is sending the voice over IP) are have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

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

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

Claims 1-8, 10-14, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ala-Laurila (U.S. 6,587,680) in view of Herle (U.S. 7,165,173).

With respect to claim 1 a method for ensuring secure forwarding of a message in a telecommunication network (see abstract i.e. radio communications system),

Art Unit: 2432

comprising: providing a first terminal from which the message is sent and a second terminal (end device) to which the message is sent (see abstract):

a) establishing a first connection extending between a first end-point at the first terminal (mobile terminal) and an original end-point at the second terminal (another of the plurality of mobile terminals of the wireless communication network) (see column 6 lines 25-50),

b) the first terminal (mobile terminal address with old access point) changing from the first address to a new address (mobile terminal address on new access point) (see column 7 line 46 – column 8 line 41),

c) registering a secure connection extending between a new end-point (mobile terminal address on new access point) and the original end-point of the first secure connection (see column 7 line 46 – column 8 line 41 the device that is sending the voice over IP) and using the second secure connection extending between the new end-point and the original end-point of the first secure connection (see column 7 line 46 – column 8 line 41).

Ala-Laurila does not teach that the connections are secure connection. Herle teaches that the connections are secure connection from end point to end point through the access point (see figure 2 and column 8 lines 41-63). It 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 to have secure path between the mobile station and provisioning server to increase security of the path. Therefore one would have been motivated to have a secure path between the mobile station and provisioning server.

With respect to claim 2, wherein a new secure connection between the new address of the first terminal and the address of the second terminal is formed for the registration in step c) if such a secure connections does not already exist (see column 7 line 46 – column 8 line 16).

With respect to claim 3, characterized in that, the secure connection is established in step a) and by forming one or more Security Associations (SAs) using the IPSec protocols (see column 9 lines 17-21).

With respect to claim 4, wherein the message to be forwarded consists of IP packets (see column 8 lines 1-16).

With respect to claim 5, wherein, after step b), when the first terminal intend to send a message from the address it has moved to it first checks whether a secure connection between the new address and the other terminal already exists (see column 8 lines 49-61).

With respect to claim 6, wherein the existence of the new secure connection is checked by means of a connection table (see column 7 line 56-67 i.e. available access point list).

With respect to claim 7, wherein, in step c), the actual connection(s) to be used is/are registered by means of a signaling message or signaling message exchange between the first terminal and the second terminal (see figure 2 and 3).

With respect to claim 8, wherein the new (second) address of the first terminal is updated automatically by the second terminal when the first terminal sends a message from the new address (see column 7 line 46 – column 8 line 41).

With respect to claim 10, wherein a key exchange being a part of the forming of the secure connection is performed with IKE or some other automated key exchange protocol (see column 8 lines 17-22).

With respect to claim 11, wherein the secure connection between the new address of the first terminal and the second terminal is in step c) registered for immediate and/or later use (see column 7 line 46 – column 8 line 41).

With respect to claim 12, wherein the registration for later use is made by the second terminal in a connection table (see column 7 line 56-67 i.e. available access point list).

With respect to claim 13, wherein when sending message through the secure connection IPSec transport mode is used to secure traffic between the mobile computer and a destination computer (see column 9 lines 17-21).

With respect to claim 14, wherein a tunneling protocol is used together with IPSec to provide a tunneling capability (see figure 2, 3 and column 9 lines 17-21).

With respect to claim 16, wherein when sending message through the secure connection IPSec tunnel mode is used to secure traffic between the mobile computer and a destination computer (see figure 2, 3 and column 9 lines 17-21).

Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ala-Laurila (U.S. 6,587,680) in view of Herle (U.S. 7,165,173) in view of Takagi et al (U.S. 7,143,282).

Ala-Laurila does not teach that the a key exchange being a part of the forming of the secure connection in step a) and is performed manually. Takagi teaches a key exchange being a part of the forming of the secure connection in step a) and is performed manually (see Takagi column 8 lines 29-34).

It 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 to have the Security Associations of Ala-Laurila to be set up manually as taught in Takagi by Internet Key Exchange to increase the compatibility of the system (see Takagi column 8 lines 29-34). Therefore one would have been motivated to have Security Associations be able to be set up manually by Internet Key Exchange.

Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ala-Laurila (U.S. 6,587,680) in view of Herle (U.S. 7,165,173) in view of Jorgensen (U.S. 6,452,915).

Ala-Laurila does not teach with respect to claim 15 where the Layer 2 Tunneling Protocol (L2TP) tunneling protocol is used together with IPsec to provide a tunneling capability. Jorgensen teaches Layer 2 Tunneling Protocol (L2TP) tunneling protocol is used together with IPsec to provide a tunneling capability (see Jorgensen column 44 lines 8-17). It 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 to have used L2TP over IPsec because L2TP can carry multiple protocols. L2TP also offers transmission

capability over non-IP networks (see Jorgensen column 44 lines 8-17). Therefore one would have been motivated to have used L2TP over IPsec.

Conclusion

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

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

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Devin Almeida whose telephone number is 571-270-1018. The examiner can normally be reached on Monday-Thursday from 7:30 A.M. to 5:00 P.M. The examiner can also be reached on alternate Fridays from 7:30 A.M. to 4:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.


Application/Control Number: 10/490,933
Art Unit: 2432

Page 8

Information regarding the status of an application may be obtained from the
Patent Application Information Retrieval (PAIR) system.

/Devin Almeida/
Examiner, Art Unit 2432

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432

Index of Claims 	Application/Control No. 10490933	Applicant(s)/Patent Under Reexamination VAARALA ET AL.
	Examiner DEVIN ALMEIDA	Art Unit 2432

✓	Rejected
=	Allowed

-	Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

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

CLAIM		DATE							
Final	Original	10/08/2008	03/18/2009	06/08/2009	10/28/2009				
	1	✓	✓	✓	✓				
	2	✓	✓	✓	✓				
	3	✓	✓	✓	✓				
	4	✓	✓	✓	✓				
	5	✓	✓	✓	✓				
	6	✓	✓	✓	✓				
	7	✓	✓	✓	✓				
	8	✓	✓	✓	✓				
	9	✓	✓	✓	✓				
	10	✓	✓	✓	✓				
	11	✓	✓	✓	✓				
	12	✓	✓	✓	✓				
	13	✓	✓	✓	✓				
	14	✓	✓	✓	✓				
	15	✓	✓	✓	✓				
	16	✓	✓	✓	✓				
	17	✓	-	-	-				
	18	-	-	-	-				

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

Application Number	10490933	Filing Date	2004-03-26	Docket Number (if applicable)	290.1053USN	Art Unit	2432
First Named Inventor	Sami Vaarala			Examiner Name	Devin E. Almeida		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

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

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

MISCELLANEOUS

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

FEES

- The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to
Deposit Account No 060243

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

- Patent Practitioner Signature
- Applicant Signature

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

Signature of Registered U.S. Patent Practitioner			
Signature	/rfasth/	Date (YYYY-MM-DD)	2009-12-28
Name	Rolf Fasth	Registration Number	36999

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

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

Privacy Act Statement

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

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

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

RF:ss 12/29/09

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
 In re application of **EXPEDITED PROCEDURE UNDER 37**
CFR 1.114
 Sami Vaarala, et al. Art Unit 2432
 Confirmation No. 2431
 Serial No. 10/490,933

Filed: 26 March 2004

CERTIFICATE OF MAILING

For: METHOD AND SYSTEM FOR
ENSURING SECURE FORWARDING OF
MESSAGES

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 December**
2009.

Examiner: Devin E. Almeida

Date: 29 December 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 Final Office Action dated 19 November 2009.
- (X) Request for Continued Examination (RCE)
- (X) The Commissioner is hereby authorized to charge any fees which may be required in connection with the filing of this correspondence, or credit over-payment, to Account No. 06-0243.

Respectfully submitted,

FASTH LAW OFFICES

/rfasth/

Rolf Fasth
Registration No. 36,999

Attorney Docket No. 290.1053USN

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:	10490933			
Filing Date:	18-Apr-2005			
Title of Invention:	Method and system for ensuring secure forwarding of messages			
First Named Inventor/Applicant Name:	Sami Vaarala			
Filer:	Rolf Fasth/Sloan Smith			
Attorney Docket Number:	290.1053USN			
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:	6717191
Application Number:	10490933
International Application Number:	
Confirmation Number:	2431
Title of Invention:	Method and system 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:	290.1053USN
Receipt Date:	29-DEC-2009
Filing Date:	18-APR-2005
Time Stamp:	06:55:31
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	6478
Deposit Account	060243
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. 1.492 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

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

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

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment Submitted/Entered with Filing of CPA/RCE	AMD.PDF	42813 a9610a7793e041013720ae5374701c507160dc87	no	13
Warnings:					
Information:					
2	Request for Continued Examination (RCE)	RCE.PDF	718147 e6c71ecf0e137b32d51bc25e0d71cb1fa0577823	no	3
Warnings:					
Information:					
3	Miscellaneous Incoming Letter	TRX.PDF	18797 686b958a131c3c03200c6089cfe15189a01b5a61	no	1
Warnings:					
Information:					
4	Fee Worksheet (PTO-875)	fee-info.pdf	29915 c9bffc273bbefcf908b2d52e063f1029f1a09d83	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			809672		

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 2432

5 Sami Vaarala, Antti Nuopponen, Panu Pietikainen

Serial No. 10/490,933

10 Filed: 26 March 2004

For: METHOD AND NETWORK FOR ENSURING SECURE FORWARDING OF
MESSAGES

15 Examiner: Devin E. Almeida

Date: 28 December 2009

Attorney Docket Number: 290.1053USN

20

AMENDMENT

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

This is in response to the Office action of 19
November 2009. Please amend the above-identified patent
application as follows:

In the Claims:

Amend the claims as follows:

5

1. (Currently amended) A method for ensuring secure forwarding of a message in a telecommunication network, comprising:

providing a first terminal from which the message is sent and a second terminal to which the message is sent,

10 a) establishing a first secure connection extending between a first ~~end-point at~~ network address of the first terminal and an original ~~end-point at~~ network address of the second terminal,

15 b) the first terminal changing from ~~a~~ the first network address to a new network address, and

c) registering a second secure connection extending between the ~~a new end-point~~ network address and the original ~~end-point~~ network address of the first secure connection. ~~, and using the second secure connection extending between the new~~
20 ~~end-point and the original end-point of the first secure connection.~~

2. (Currently amended) The method of claim 1, wherein the
method further comprises establishing the second secure
25 connection ~~a new secure connection between the new address of~~
~~the first terminal and the address of the second terminal is~~

~~formed for the registration in step e) if such a~~ when the
second secure connection~~s~~ does not already exist.

3. (Currently amended) The method of claim 1, wherein the
5 method further comprises establishing the first secure
connection ~~is established in step a) and by forming one or~~
~~more Security Associations (SAs) by~~ using the IPsec protocols.

4. (Currently amended) The method of claim 1, wherein the
10 method further comprises providing the message ~~to be forwarded~~
~~consists of~~ with IP packets.

5. (Currently amended) The method of claim 1, wherein, ~~after~~
~~step b), when the first terminal sends a message from the~~
15 ~~address the first terminal has moved to, the first terminal~~
~~first checks~~ the method further comprises checking whether a
secure connection between the new network address and the
second terminal already exists.

20 6. (Currently amended) The method of claim 5, wherein the
method further comprises checking by using ~~an existence of the~~
~~second secure connection is checked by means of a connection~~
table.

25 7. (Currently amended) The method of claim 1, wherein ~~in step~~
~~e), the actual connection(s) to be used is/are registered by~~

~~means of~~ the method further comprises using a signaling message or signaling message exchange between the first terminal and the second terminal.

5 8. (Currently amended) The method of claim 1, wherein the method further comprises automatically updating the new network address of the first terminal ~~is updated automatically~~ by the second terminal when the first terminal sends a message from the new network address.

10

9. (Currently amended) The method of claim 1, wherein the method further comprises using a key exchange ~~is a part of forming of~~ when establishing the first secure connection ~~in step a)~~ and ~~is performed manually~~.

15

10. (Currently amended) The method of claim 2, wherein the method further comprises using a key exchange ~~is a part of forming of the secure connection~~ performed with Internet Key Exchange (IKE).

20

11. (Currently amended) The method of claim 1, wherein ~~the second secure connection between the new address of the first terminal and the second terminal is in step c)~~ registered the second secure connection is registered for immediate and/or
25 later use.

12. (Previously presented) The method of claim 11, wherein the registration for later use is made by the second terminal in a connection table.

5 13. (Currently amended) The method of claim 3, wherein the method further comprises sending the message ~~when sending message through the secure connection, IPSec transport mode is used~~ to secure traffic between a mobile computer and a destination computer.

10

14. (Currently amended) The method of claim 13, wherein the method further comprises using a tunneling protocol ~~is used~~ together with IPSec to provide a tunneling capability.

15 15. (Currently amended) The method of claim 14, wherein the method further comprises using ~~where~~ a Layer 2 Tunneling Protocol (L2TP) tunneling protocol ~~is used~~ together with IPSec to provide a tunneling capability.

20 16. (Currently amended) The method of claim 3, wherein the method further comprises using ~~when sending message through the secure connection,~~ an IPSec tunnel mode ~~is used~~ to secure traffic between a mobile computer and a destination computer.

25 17-18. (Canceled)

REMARKS

Reconsideration of the application is respectfully requested.

5 Claim 1 has been clarified to require that the first terminal changes from the first network address to a new network address. No new matter has been added. The fact that the method of the present invention relates to network addresses and not physical addresses of the mobile terminal is clear

10 from the detailed description. Support for the change of the network may be found on, for example, page 5, lines 16-26; page 6, lines 8-14; page 13, line 10-11; and page 16, line 28 - page 17, line 28.

15 Applicants would like to respectfully assert that the cited Ala-Laurila does not show a mobile terminal changing its network address. When a mobile terminal changes access point, as described in Ala-Laurila, it simply means that the mobile terminal is going to be served by a new base station (such as

20 when switching from AP 14 to AP 114 as illustrated in Ala-Laurila). The mobile terminal does not change the network address itself even if the mobile terminal physically moves to a new place (such as moving from cell 18, served by AP 14, to cell 118 served by AP 114). In other words, the new base

25 station AP 114 is merely another terminal that the mobile terminal 12 communicates with when the mobile terminal has

moved to a new cell/area so that it first communicates with the first base station AP 14 and after the hand-over it communicates with the new base station AP 114. It should be made clear that the mobile terminal does not change its
5 network address just because it moves to a new geographic area or cell (such as when moving from geographic area 18 to area 118 as described in Ala-Laurila).

It is therefore submitted that Ala-Laurila does not teach or
10 suggest step b) of the amended claim 1, i.e. the step of "the first terminal changing from the first network address to a new network address." In contrast, Ala-Laurila's mobile terminal merely moves from the geographical area 18 to the new geographical area 118 but maintains the same network address.
15 Before the hand-over, the mobile terminal 12 communicates with AP 14 and after the hand-over the mobile terminal 12 communicates with AP 114 but the mobile terminal 12 never changes its network address. This means the mobile terminal 12 has the same network address even after it has moved to
20 cell 118 and after the handover to AP 114.

In the present invention, it is thus not necessary for the mobile terminal to physically move. The mobile terminal can remain in the same physical place while the mobile terminal
25 changes from one network address to another network address (see, for example, page 5, lines 24-26).

It is submitted that Ala-Laurila fails to teach or suggest the step of the first terminal changing from the first network address to a new network address, as required by step b) of the amended claim 1. Consequently, Ala-Laurila also fails to teach or suggest the step of registering a second secure connection extending between the new network address and the original network address of the first secure connection, as required by the amended step c) of claim 1.

10

Herle does not cure these deficiencies. Herle was cited to show that the connections are secure connections from end-point to end-point through the access point. Herle merely teaches a mobile station 112 that is capable of securely communicating with a plurality of base stations. It is submitted that Herle alone or in combination with Ala-Laurila completely fails to teach or suggest the steps of the mobile station 112 changing from the first network address to a new network address, and registering a second secure connection extending between the new network address and the original network address of the first secure connection, as required by the amended claim 1. Similar to Ala-Laurila, Herle merely teaches the mobile terminal switching between different base stations to find a stronger signal. As explained above, this is quite different from changing the network address of the mobile terminal to another network address.

In summary, the proposed combination of Ala-Laurila and Herle completely fails to teach or suggest the amended steps b) and c) of the amended claim 1. The cited references would require
5 extensive modifications to arrive at the limitations of the amended claim 1. Applicants fail to see why a person of ordinary skill in the art would look to Ala-Laurila and Herle to learn about the limitations of step b) and step c) when such limitations are completely missing from the cited
10 references.

Even assuming *arguendo* that the requisite method steps of claim 1 are shown by the combination of Ala-Laurila and Herle, (although this is disputed by Applicants) *prima facie* support
15 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)
20 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
25 with some rational underpinning to support the legal conclusion of obviousness." *In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006). Furthermore, the Examiner

must make "explicit" this rationale of "the apparent reason to combine the known elements in the fashion claimed," including a detailed explanation of "the effects of demands known to the design community or present in the marketplace" and "the
5 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,
10 which merely asserts it would have been obvious to modify the teaching method of Herle with Ala-Laurila in order to "increase security of the path." (emphasis added). Thus, one benefit, or advantage of the modification is the only rationale provided in the Office Action in support of the
15 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
20 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
25 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
5 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*
10 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
15 additional remaining claims to the extent they may depend therefrom.

Most importantly and as explained above, Applicants respectfully request the rejection of claim 1 is withdrawn
20 because the proposed combination of Ala-Laurila and Herle complete fails to teach or suggest all the limitations of the amended claim 1.

Claims 2-8, 10-14 and 16 are submitted to be allowable because
25 they depend upon the allowable base claim 1 and because each claim includes limitations that are not taught or suggested in

the cited reference.

Claim 9 was rejected under §103 as being obvious over Ala-
Laurila in view of Herle. This rejection is respectfully
5 traversed.

Claim 9 is submitted to be allowable because it depends upon
the allowable base claim 1 and because the claim includes
limitations that are not taught or suggested in the cited
10 references.

Claim 15 was rejected under §103 as being obvious over Ala-
Laurila in view of Herle. This rejection is respectfully
traversed.

15

Claim 15 is submitted to be allowable because it depends upon
the allowable base claim 1 and because the claim includes
limitations that are not taught or suggested in the cited
references.

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

5

Respectfully submitted,

FASTH LAW OFFICES

10

/rfasth/

Rolf Fasth

15

Registration No. 36,999

Attorney Docket No. 290.1053USN

20

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

25

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

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

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 10/490,933	Filing Date 04/18/2005	<input type="checkbox"/> To be Mailed
---	---	----------------------------------	---------------------------------------

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

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

APPLICATION AS AMENDED – PART II					OTHER THAN SMALL ENTITY			
	(Column 1)	(Column 2)	(Column 3)	SMALL ENTITY	OR	SMALL ENTITY	OTHER THAN SMALL ENTITY	
	12/29/2009	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)
AMENDMENT	Total <small>(37 CFR 1.16(i))</small>	* 16	Minus	** 20	=	0	X \$ =	
	Independent <small>(37 CFR 1.16(h))</small>	* 1	Minus	*** 3	=	0	X \$ =	
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>							
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>							
					TOTAL ADD'L FEE	0	TOTAL ADD'L FEE	

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

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

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
10/490,933 04/18/2005 Sami Vaarala 290.1053USN 2431

33369 7590 01/19/2010
FASTH LAW OFFICES (ROLF FASTH)
26 PINECREST PLAZA, SUITE 2
SOUTHERN PINES, NC 28387-4301

Table with 1 column: EXAMINER
ALMEDA, DEVIN E

Table with 2 columns: ART UNIT, PAPER NUMBER
2432

Table with 2 columns: NOTIFICATION DATE, DELIVERY MODE
01/19/2010 ELECTRONIC

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

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

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

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

Office Action Summary	Application No. 10/490,933	Applicant(s) VAARALA ET AL.	
	Examiner DEVIN ALMEIDA	Art Unit 2432	

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

Period for Reply

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

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

Status

- 1) Responsive to communication(s) filed on 29 December 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) 1-16 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) 1-16 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) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

This action is in response to the papers filed 12/29/2009.

Response to Arguments

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

Claim Rejections - 35 USC § 103

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

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

Claims 1-8, 10-14, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sturniolo et al (U.S. 6,091,951) in view of Herle (U.S. 7,165,173).

With respect to claim 1, Sturniolo discloses a method for ensuring secure forwarding of a message in a telecommunication network (see abstract i.e. radio communications system), comprising: providing a first terminal from which the message is sent and a second terminal (end device) to which the message is sent (see abstract):

a) establishing a first connection extending between a first network address of the first terminal (mobile terminal at AP1) and an original network address of the second terminal (see abstract i.e. device on the network backbone),

b) the first terminal (mobile terminal) changing from the first network address to a new network address (see column 10 line 8-55) and

c) registering a second connection extending between the new network address (mobile terminal address on new access point) and the original network address of the first secure connection (see column 10 line 8-55).

Sturniolo does not teach that the connections are secure connection.

Herle teaches that the connections are secure connection from end point to end point through the access point (see figure 2 and column 8 lines 41-63). It 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 to have secure path between the mobile station and provisioning server to increase security of the path. Therefore one would have been motivated to have a secure path between the mobile station and provisioning server.

With respect to claim 2, wherein the method further comprises establishing the second secure connection when the second secure connections does not already exist (see column 10 line 8-55).

With respect to claim 3, wherein the method further comprises establishing the first secure connection by using the IPSec protocols (see Herle column 9 lines 4-22).

With respect to claim 4, wherein the method further comprises providing the message with IP packets (see column 9 lines 21-38).

With respect to claim 5, checking whether a secure connection between the new network address and the other terminal already exists (see figure 2 and column 10 line 8-55).

With respect to claim 6, checking by using a connection table (see figure 5a and 5b).

With respect to claim 7, a signaling message or signaling message exchange between the first terminal and the second terminal (see figure 2 and column 10 line 8-55).

With respect to claim 8, automatically updating the new network address of the first terminal by the second terminal when the first terminal sends a message from the new network address (see figure 2 and column 10 line 8-55).

With respect to claim 10, using a key exchange performed with Internet key exchange IKE (see Herle figure 2, 3 and column 9 lines 5-22).

With respect to claim 11, the second secure connection is registered for immediate and/or later use (see figure 2 and column 10 line 8-55).

With respect to claim 12, wherein the registration for later use is made by the second terminal in a connection table (see figure 2 and column 10 line 8-55).

With respect to claim 13, to secure traffic between the mobile computer and a destination computer (see figure 2 and column 10 line 8-55).

With respect to claim 14, using a tunneling protocol together with IPSec to provide a tunneling capability (see Herle figure 2, 3 and column 9 lines 5-22).

With respect to claim 16, an IPSec tunnel mode is used to secure traffic between the mobile computer and a destination computer (see Herle figure 2, 3 and column 9 lines 5-22).

Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sturniolo et al (U.S. 6,091,951) in view of Herle (U.S. 7,165,173) in view of Takagi et al (U.S. 7,143,282).

Sturniolo does not teach that a key exchange when establishing the secure connection. Takagi teaches a key exchange when establishing the secure connection (see Takagi column 8 lines 29-34). It 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 to have the Security Associations of Ala-Laurila to be set up manually as taught in Takagi by Internet Key Exchange to increase the compatibility of the system (see Takagi column 8 lines 29-34). Therefore one would have been motivated to have Security Associations be able to be set up manually by Internet Key Exchange.

Claims 14 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sturniolo et al (U.S. 6,091,951) in view of Herle (U.S. 7,165,173) in view of Jorgensen (U.S. 6,452,915).

Sturniolo does not teach with respect to claim 14, using a tunneling protocol together with IPSec to provide a tunneling capability. Jorgensen using a tunneling protocol together with IPSec to provide a tunneling capability (see Jorgensen column 44 lines 8-17). It 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 to have used L2TP over IPsec because L2TP can carry multiple protocols. L2TP also offers transmission

capability over non-IP networks (see Jorgensen column 44 lines 8-17). Therefore one would have been motivated to have used L2TP over IPsec.

With respect to claim 15 where the Layer 2 Tunneling Protocol (L2TP) tunneling protocol together with IPsec to provide a tunneling capability (see Jorgensen column 44 lines 8-17).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Devin Almeida whose telephone number is 571-270-1018. The examiner can normally be reached on Monday-Thursday from 7:30 A.M. to 5:00 P.M. The examiner can also be reached on alternate Fridays from 7:30 A.M. to 4:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on 571-272-3799. 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.

/Devin Almeida/
Examiner, Art Unit 2432

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432

Notice of References Cited	Application/Control No. 10/490,933	Applicant(s)/Patent Under Reexamination VAARALA ET AL.	
	Examiner DEVIN ALMEIDA	Art Unit 2432	Page 1 of 1

U.S. PATENT DOCUMENTS

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A US-6,091,951	07-2000	Sturniolo et al.	455/432.2
B	US-			
C	US-			
D	US-			
E	US-			
F	US-			
G	US-			
H	US-			
I	US-			
J	US-			
K	US-			
L	US-			
M	US-			


FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

*	Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
U	
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. 10490933	Applicant(s)/Patent Under Reexamination VAARALA ET AL.
	Examiner DEVIN ALMEIDA	Art Unit 2432

✓	Rejected
=	Allowed


-	Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

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

CLAIM		DATE										
Final	Original	10/08/2008	03/18/2009	06/08/2009	10/28/2009	01/05/2010						
	1	✓	✓	✓	✓	✓						
	2	✓	✓	✓	✓	✓						
	3	✓	✓	✓	✓	✓						
	4	✓	✓	✓	✓	✓						
	5	✓	✓	✓	✓	✓						
	6	✓	✓	✓	✓	✓						
	7	✓	✓	✓	✓	✓						
	8	✓	✓	✓	✓	✓						
	9	✓	✓	✓	✓	✓						
	10	✓	✓	✓	✓	✓						
	11	✓	✓	✓	✓	✓						
	12	✓	✓	✓	✓	✓						
	13	✓	✓	✓	✓	✓						
	14	✓	✓	✓	✓	✓						
	15	✓	✓	✓	✓	✓						
	16	✓	✓	✓	✓	✓						
	17	✓	-	-	-	-						
	18	-	-	-	-	-						

Search Notes 	Application/Control No. 10490933	Applicant(s)/Patent Under Reexamination VAARALA ET AL.
	Examiner DEVIN ALMEIDA	Art Unit 2432

SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
See east printout	10/8/2008	DA
See east printout	1/5/2010	DA

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

/DEVIN ALMEIDA/ Examiner.Art Unit 2432	
---	--

EAST Search History**EAST Search History (Prior Art)**

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	36	"6587680"	US- PGPUB; USPAT	OR	ON	2010/01/05 12:26
L2	1559	network adj address with change	US- PGPUB; USPAT	OR	ON	2010/01/05 12:30
L3	323	change adj network adj address	US- PGPUB; USPAT	OR	ON	2010/01/05 12:30
L5	32	change adj network adj address with access adj point	US- PGPUB; USPAT	OR	ON	2010/01/05 12:33
L6	5	"7,165,173"	US- PGPUB; USPAT	OR	ON	2010/01/05 13:54

EAST Search History (Interference)

< This search history is empty >

1 / 5 / 2010 2:03:39 PM

UNITED STATES PATENT AND TRADEMARK OFFICE
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA VA 22313-1451

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

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



**Courtesy Reminder for
Application Serial No: 10/490,933**

Attorney Docket No: 290.1053USN

Customer Number: 33369

Date of Electronic Notification: 01/19/2010

This is a courtesy reminder that new correspondence is available for this application. The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

An email notification regarding the correspondence was sent to the following email address(es) associated with your customer number:

sloan.smith@fasthlaw.com

nan_russell@fasthlaw.com

Please verify that these email addresses are correct.

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of Art Unit 2432

5 Sami Vaarala, Antti Nuopponen, Panu Pietikainen

Serial No. 10/490,933

10 Filed: 26 March 2004

For: METHOD AND NETWORK FOR ENSURING SECURE FORWARDING OF
MESSAGES

15 Examiner: Devin E. Almeida

Date: 11 February 2010

Attorney Docket Number: 290.1053USN

20

AMENDMENT

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

This is in response to the Office action of 19
January 2010. Please amend the above-identified patent
application as follows:

In the Claims:

Amend the claims as follows:

5

1. (Currently amended) A method for ensuring secure forwarding of a message in a telecommunication network, comprising:

providing a first terminal from which the message is sent and a second terminal to which the message is sent,

10

a) establishing a first secure connection as being an active connection and extending between a first network address of

the first terminal and an original network address of the second terminal, establishing a second secure connection

15

extending between a second network address of the first terminal and the original network address of the second terminal,

b) the first terminal changing from the first network address to ~~a new~~ the second network address, ~~and~~

20

the first terminal checking whether the second secure connection already exists, and

c) when the second secure connection already exists, registering a the already established second secure connection as being the active connection ~~extending between the new~~

25

~~network address and the original network address of the first secure connection~~ without having to reestablish the second secure connection.

2. (Previously presented) The method of claim 1, wherein the method further comprises establishing the second secure connection when the second secure connections does not already
5 exist.

3. (Previously presented) The method of claim 1, wherein the method further comprises establishing the first secure connection by using IPsec protocols.
10

4. (Previously presented) The method of claim 1, wherein the method further comprises providing the message with IP packets.

15 5. (Previously presented) The method of claim 1, wherein the method further comprises checking whether a secure connection between the new network address and the second terminal already exists.

20 6. (Previously presented) The method of claim 5, wherein the method further comprises checking by using a connection table.

7. (Previously presented) The method of claim 1, wherein the method further comprises using a signaling message or
25 signaling message exchange between the first terminal and the second terminal.

8. (Previously presented) The method of claim 1, wherein the method further comprises automatically updating the new network address of the first terminal by the second terminal when the first terminal sends a message from the new network address.

9. (Previously presented) The method of claim 1, wherein the method further comprises using a key exchange when establishing the first secure connection.

10. (Previously presented) The method of claim 2, wherein the method further comprises using a key exchange performed with Internet Key Exchange (IKE).

11. (Previously presented) The method of claim 1, wherein the second secure connection is registered for immediate and/or later use.

12. (Previously presented) The method of claim 11, wherein the registration for later use is made by the second terminal in a connection table.

13. (Previously presented) The method of claim 3, wherein the method further comprises sending the message to secure traffic between a mobile computer and a destination computer.

14. (Previously presented) The method of claim 13, wherein the method further comprises using a tunneling protocol together with IPsec to provide a tunneling capability.

5

15. (Previously presented) The method of claim 14, wherein the method further comprises using a Layer 2 Tunneling Protocol (L2TP) tunneling protocol together with IPsec to provide a tunneling capability.

10

16. (Previously presented) The method of claim 3, wherein the method further comprises using an IPsec tunnel mode to secure traffic between a mobile computer and a destination computer.

15 17-18. (Canceled)

REMARKS

5 Reconsideration of the application is respectfully
requested. Claims 1-8, 10-14 and 16 were rejected under
Section 103 as being obvious over Sturniolo in view of Herle.
This rejection is respectfully traversed.

10 On page 2 of the current Office action, the Examiner
states that Sturniolo "discloses a method for ensuring secure
forwarding of a message..." Applicants strongly disagree.

15 There is absolute nothing in Sturniolo about secure
forwarding or the use of secure connections. The Examiner
refers to the abstract of Sturniolo and despite the relatively
long abstract there is no mentioning whatsoever about "secure
forwarding" or the use of secure connections. The Examiner
then confirms on page 3 of the Office action that Sturniolo
does not teach connections that are secure connections.

20 The use of secure connections is a critical aspect
of the present invention so that the mobile terminal may
switch from a first secure connection to an already
established second secure connection while maintaining the
original network address of the second terminal but without
having to reestablish the second secure connection since it
has already been established. More particularly, the amended
25 claim 1 has been clarified to require that the second secure
connection is established prior to the first terminal changing

from the first network address to the second network address. Claim 1 has also been amended to require that the first secure connection is established as the active connection and after the change of the first terminal from the first network
5 address to the second network address, the first terminal checks whether the second secure connection already exists and when it already exists the second secure connection is established as the active connection without having to reestablish the second secure connection. No new matter has
10 been added to the application. The amended claim 1 is, for example, supported in the original claim 1; page 4, lines 30-32; page 5, lines 1-5; page 12, lines 22-30; page 13, line 25 - page 14, line 4; page 14, line 24; page 15, line 2; page 19, lines 4-18 and 25-30; page 20, line 23 - page 21, line 4 of
15 the corresponding WO publication.

It is submitted that Sturniolo completely fails to teach or suggest the method steps of the amended claim 1. As indicated above, the main reason for this is that Sturniolo fails to teach the establishment and use of the critical
20 secure connections.

Herle does not cure these deficiencies. Herle was merely cited to show a secure connection from one end point to another end point. Herle merely teaches a mobile station 112 that is capable of securely communicating with a plurality of
25 base stations. Additionally, Herle merely teaches the mobile terminal switching between different base stations to find a

stronger signal. As explained earlier, this is quite different from changing the network address of the mobile terminal to another network address. Herle fails to teach or suggest the steps of establishing a first secure connection as the active connection and establishing a second secure connection before the first terminal changes from the first network address to the second network address. Herle also fails to teach or suggest the first terminal checking whether the second secure connection already exists prior to registering the second secure connection as the active connection without having to reestablish the second secure connection (since it has already been established). In contrast, the network address of the first terminal in Herle does not change.

Applicants cannot see why a person of ordinary skill in the art would look to Sturniolo, Herle or the combination thereof to learn about the features of the amended claim 1 when those features are completely missing in the cited references. It is submitted that the cited references would require extensive modifications, that are not taught or suggested, to arrive at all of the method steps of the amended claim 1.

Even assuming *arguendo* that the requisite method steps of claim 1 are shown by the combination of Sturniolo and Herle, (although this is disputed by Applicants) *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
5 (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
10 conclusion of obviousness.” *In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006). Furthermore, the Examiner must make “explicit” this rationale of “the apparent reason to combine the known elements in the fashion claimed,” including a detailed explanation of “the effects of demands known to the
15 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 in the middle of page 3 of the Office
20 action, which merely asserts it would have been obvious to modify the teaching method of Herle with Sturniolo in order to “increase security of the path.” (emphasis added). Thus, one benefit, or advantage of the modification is the only rationale provided in the Office Action in support of the
25 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

5 "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

10 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*

15 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

20 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

25 therefrom.

Most importantly and as explained above, Applicants

respectfully request the rejection of claim 1 is withdrawn because the proposed combination of Sturniolo and Herle complete fails to teach or suggest all the limitations of the amended claim 1.

5 Claims 2-8, 10-14 and 16 are submitted to be allowable because they depend upon the allowable base claim 1 and because each claim includes limitations that are not taught or suggested in the cited reference.

10 Claim 9 was rejected under §103 as being obvious over Sturniolo in view of Herle and Takagi. This rejection is respectfully traversed.

15 Claim 9 is submitted to be allowable because it depends upon the allowable base claim 1 and because the claim includes limitations that are not taught or suggested in the cited references.

 Claims 14-15 were rejected under §103 as being obvious over Sturniolo in view of Herle and Jorgensen. This rejection is respectfully traversed.

20 Claims 14-15 are submitted to be allowable because they depend upon the allowable base claim 1 and because the claims include limitations that are not taught or suggested in the cited references.

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

5 Respectfully submitted,

FASTH LAW OFFICES

10

/rfasth/
Rolf Fasth
Registration No. 36,999

15

Attorney Docket No. 290.1053USN

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

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Sami Vaarala, et al. Art Unit 2432
Confirmation No. 2431

Serial No. 10/490,933

CERTIFICATE OF MAILING

Filed: 26 March 2004

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 **11 February**
2010.

For: METHOD AND SYSTEM FOR
ENSURING SECURE FORWARDING OF
MESSAGES

Examiner: Devin E. Almeida

/rfasth/

Date: 11 February 2010

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 19 January 2010.
- (X) The Commissioner is hereby authorized to charge any fees which may be required in connection with the filing of this correspondence, or credit over-payment, to Account No. 06-0243.

Respectfully submitted,

FASTH LAW OFFICES

/rfasth/

Rolf Fasth
Registration No. 36,999

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

Attorney Docket No. 290.1053USN

Electronic Acknowledgement Receipt

EFS ID:	6992205
Application Number:	10490933
International Application Number:	
Confirmation Number:	2431
Title of Invention:	Method and system 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:	290.1053USN
Receipt Date:	11-FEB-2010
Filing Date:	18-APR-2005
Time Stamp:	14:32:22
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	AMD.PDF	38654 <small>7e330223645f86027ae73a490533125ea7879604</small>	no	12

Warnings:

Information:

2	Miscellaneous Incoming Letter	TRX.PDF	18645 <small>file762cf00484345cd818f122dc1597dfce0a4a</small>	no	1
Warnings:					
Information:					
Total Files Size (in bytes):			57299		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

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

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 10/490,933	Filing Date 04/18/2005	<input checked="" type="checkbox"/> To be Mailed
---	---	----------------------------------	--

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

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

APPLICATION AS AMENDED – PART II					OTHER THAN SMALL ENTITY					
	(Column 1)	(Column 2)	(Column 3)		SMALL ENTITY		OTHER THAN SMALL ENTITY			
AMENDMENT	02/11/2010	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)		RATE (\$)	ADDITIONAL FEE (\$)	
		* 16	Minus	** 20	=	0	OR	X \$ =		
		* 1	Minus	*** 3	=	0	OR	X \$ =		
		<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))								
		<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								
					TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE		

	(Column 1)	(Column 2)	(Column 3)		SMALL ENTITY		OTHER THAN SMALL ENTITY			
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)		RATE (\$)	ADDITIONAL FEE (\$)	
		*	Minus	**	=		OR	X \$ =		
		*	Minus	***	=		OR	X \$ =		
		<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))								
		<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								
					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:
/NICHELE PETERSON/

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

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
10/490,933 04/18/2005 Sami Vaarala 290.1053USN 2431

33369 7590 04/20/2010
FASTH LAW OFFICES (ROLF FASTH)
26 PINECREST PLAZA, SUITE 2
SOUTHERN PINES, NC 28387-4301

Table with 1 column: EXAMINER
ALMEDA, DEVIN E

Table with 2 columns: ART UNIT, PAPER NUMBER
2432

Table with 2 columns: NOTIFICATION DATE, DELIVERY MODE
04/20/2010 ELECTRONIC

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

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

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

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

Office Action Summary	Application No. 10/490,933	Applicant(s) VAARALA ET AL.	
	Examiner DEVIN ALMEIDA	Art Unit 2432	

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

Disposition of Claims

- 4) Claim(s) 1-16 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) 1-16 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) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

This action is in response to the papers filed 2/11/2010.

Response to Arguments

Applicant's arguments with respect to Sturniolo not teaching secure forwarding of messages have been fully considered but they are not persuasive. Sturniolo in view of Herle teach the claimed invention. Sturniolo does not teach that the connections are secure connection. Herle teaches that the connections are secure connection from end point to end point through the access point (see figure 2 and column 8 lines 41-63). It 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 to have secure path between the mobile station and provisioning server to increase security of the path. Therefore one would have been motivated to have a secure path between the mobile station and provisioning server.

Applicant's arguments with respect to Sturniolo not teaching the second secure connection is established prior to the first terminal changing from the first network address to the second network address. Sturniolo teaches "Nevertheless, the virtual circuit, session, and socket connection information previously obtained via the GATEWAY1 is still valid despite the mobile terminal 36 receiving a new network address in step 76. Thus, packets delivered to the GATEWAY1 for routing to the mobile terminal 36 still may be routed to the mobile terminal 36 by the GATEWAY1." Therefore there is still the first connection when the second connection is being established.

In response to applicant's argument that there is no teaching, suggestion, or motivation to combine the references, the examiner recognizes that obviousness may be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988), *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992), and *KSR International Co. v. Teleflex, Inc.*, 550 U.S. 398, 82 USPQ2d 1385 (2007). In this case, It 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 to have secure path between the mobile station and provisioning server to increase security of the path (see column 3 lines 37-46).

Claim Rejections - 35 USC § 103

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

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

Claims 1-8, 10-14, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sturniolo et al (U.S. 6,091,951) in view of Herle (U.S. 7,165,173).

With respect to claim 1, Sturniolo discloses a method for ensuring secure forwarding of a message in a telecommunication network (see abstract i.e. radio

communications system), comprising: providing a first terminal from which the message is sent and a second terminal (end device) to which the message is sent (see abstract):

a) establishing a first connection as being an active connection and extending between a first network address of the first terminal (mobile terminal at AP1) and an original network address of the second terminal (see abstract i.e. device on the network backbone), establishing a second connection extending between a second network address of the first terminal and the original network address of the second terminal (see column 10 line 8-55),

b) the first terminal (mobile terminal) changing from the first network address to the second network address (see column 10 line 8-55), the first terminal checking whether the second connection already exists, and

c) when the second connection already exists registering the already established second connection as being the active connection without having to reestablish the second connection (see column 10 line 8-55).

Sturniolo does not teach that the connections are secure connection.

Herle teaches that the connections are secure connection from end point to end point through the access point (see figure 2 and column 8 lines 41-63). It 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 to have secure path between the mobile station and provisioning server to increase security of the path (see column 3 lines 37-46). Therefore one would have been motivated to have a secure path between the mobile station and provisioning server.

With respect to claim 2, wherein the method further comprises establishing the second secure connection when the second secure connections does not already exist (see column 10 line 8-55).

With respect to claim 3, wherein the method further comprises establishing the first secure connection by using the IPSec protocols (see Herle column 9 lines 4-22).

With respect to claim 4, wherein the method further comprises providing the message with IP packets (see column 9 lines 21-38).

With respect to claim 5, checking whether a secure connection between the new network address and the other terminal already exists (see figure 2 and column 10 line 8-55).

With respect to claim 6, checking by using a connection table (see figure 5a and 5b).

With respect to claim 7, a signaling message or signaling message exchange between the first terminal and the second terminal (see figure 2 and column 10 line 8-55).

With respect to claim 8, automatically updating the new network address of the first terminal by the second terminal when the first terminal sends a message from the new network address (see figure 2 and column 10 line 8-55).

With respect to claim 10, using a key exchange performed with Internet key exchange IKE (see Herle figure 2, 3 and column 9 lines 5-22).

With respect to claim 11, the second secure connection is registered for immediate and/or later use (see figure 2 and column 10 line 8-55).

With respect to claim 12, wherein the registration for later use is made by the second terminal in a connection table (see figure 2 and column 10 line 8-55).

With respect to claim 13, to secure traffic between the mobile computer and a destination computer (see figure 2 and column 10 line 8-55).

With respect to claim 14, using a tunneling protocol together with IPSec to provide a tunneling capability (see Herle figure 2, 3 and column 9 lines 5-22).

With respect to claim 16, an IPSec tunnel mode is used to secure traffic between the mobile computer and a destination computer (see Herle figure 2, 3 and column 9 lines 5-22).

Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sturniolo et al (U.S. 6,091,951)in view of Herle (U.S. 7,165,173)in view of Takagi et al (U.S. 7,143,282).

Sturniolo does not teach that a key exchange when establishing the secure connection. Takagi teaches a key exchange when establishing the secure connection (see Takagi column 8 lines 29-34). It 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 to have the Security Associations of Ala-Laurila to be set up manually as taught in Takagi by Internet Key Exchange to increase the compatibility of the system (see Takagi column 8 lines 29-34). Therefore one would have been motivated to have Security Associations be able to be set up manually by Internet Key Exchange.

Claims 14 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sturniolo et al (U.S. 6,091,951) in view of Herle (U.S. 7,165,173) in view of Jorgensen (U.S. 6,452,915).

Sturniolo does not teach with respect to claim 14, using a tunneling protocol together with IPsec to provide a tunneling capability. Jorgensen using a tunneling protocol together with IPsec to provide a tunneling capability (see Jorgensen column 44 lines 8-17). It 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 to have used L2TP over IPsec because L2TP can carry multiple protocols. L2TP also offers transmission capability over non-IP networks (see Jorgensen column 44 lines 8-17). Therefore one would have been motivated to have used L2TP over IPsec.

With respect to claim 15 where the Layer 2 Tunneling Protocol (L2TP) tunneling protocol together with IPsec to provide a tunneling capability (see Jorgensen column 44 lines 8-17).

Conclusion

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

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

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


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Devin Almeida whose telephone number is 571-270-1018. The examiner can normally be reached on Monday-Thursday from 7:30 A.M. to 5:00 P.M. The examiner can also be reached on alternate Fridays from 7:30 A.M. to 4:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on 571-272-3799. 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.

/Devin Almeida/
Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432

Index of Claims 	Application/Control No. 10490933	Applicant(s)/Patent Under Reexamination VAARALA ET AL.
	Examiner DEVIN ALMEIDA	Art Unit 2432

✓	Rejected
=	Allowed

-	Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

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

CLAIM		DATE							
Final	Original	10/08/2008	03/18/2009	06/08/2009	10/28/2009	01/05/2010	04/13/2010		
	1	✓	✓	✓	✓	✓	✓		
	2	✓	✓	✓	✓	✓	✓		
	3	✓	✓	✓	✓	✓	✓		
	4	✓	✓	✓	✓	✓	✓		
	5	✓	✓	✓	✓	✓	✓		
	6	✓	✓	✓	✓	✓	✓		
	7	✓	✓	✓	✓	✓	✓		
	8	✓	✓	✓	✓	✓	✓		
	9	✓	✓	✓	✓	✓	✓		
	10	✓	✓	✓	✓	✓	✓		
	11	✓	✓	✓	✓	✓	✓		
	12	✓	✓	✓	✓	✓	✓		
	13	✓	✓	✓	✓	✓	✓		
	14	✓	✓	✓	✓	✓	✓		
	15	✓	✓	✓	✓	✓	✓		
	16	✓	✓	✓	✓	✓	✓		
	17	✓	-	-	-	-	-		
	18	-	-	-	-	-	-		

UNITED STATES PATENT AND TRADEMARK OFFICE
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA VA 22313-1451

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

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



**Courtesy Reminder for
Application Serial No: 10/490,933**

Attorney Docket No: 290.1053USN

Customer Number: 33369

Date of Electronic Notification: 04/20/2010

This is a courtesy reminder that new correspondence is available for this application. The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

An email notification regarding the correspondence was sent to the following email address(es) associated with your customer number:

sloan.smith@fasthlaw.com

nan_russell@fasthlaw.com

Please verify that these email addresses are correct.

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of Art Unit 2432

5 Sami Vaarala, Antti Nuopponen, Panu Pietikainen

Serial No. 10/490,933

10 Filed: 26 March 2004

For: METHOD AND NETWORK FOR ENSURING SECURE FORWARDING OF
MESSAGES

15 Examiner: Devin E. Almeida

Date: 14 July 2010

Attorney Docket Number: 290.1053USN

20

AMENDMENT

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

This is in response to the Office action of 20 April
2010. Please amend the above-identified patent application as
follows:

In the Claims:

Amend the claims as follows:

5

1. (Currently amended) A method for ensuring secure forwarding of a message in a telecommunication network, comprising:

providing a first terminal from which the message is sent and a second terminal to which the message is sent,

10

a) establishing a first secure connection as being an active connection and extending between a first network address of the first terminal and an original network address of the second terminal, establishing a second secure connection extending between a second network address of the first terminal and the original network address of the second terminal,

15

b) the first terminal changing from the first network address to the second network address,

20

the first terminal checking whether the second secure connection already exists, and

c) when the second secure connection already exists, the second terminal registering the already established second secure connection as being the active connection without having to reestablish the second secure connection.

25

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

method further comprises establishing the second secure connection when the second secure connection does not already exist.

5 3. (Previously presented) The method of claim 1, wherein the method further comprises establishing the first secure connection by using IPSec protocols.

10 4. (Previously presented) The method of claim 1, wherein the method further comprises providing the message with IP packets.

15 5. (Previously presented) The method of claim 1, wherein the method further comprises checking whether a secure connection between the new network address and the second terminal already exists.

20 6. (Previously presented) The method of claim 5, wherein the method further comprises checking by using a connection table.

25 7. (Previously presented) The method of claim 1, wherein the method further comprises using a signaling message or signaling message exchange between the first terminal and the second terminal.

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

method further comprises automatically updating the new network address of the first terminal by the second terminal when the first terminal sends a message from the new network address.

5

9. (Previously presented) The method of claim 1, wherein the method further comprises using a key exchange when establishing the first secure connection.

10 10. (Previously presented) The method of claim 2, wherein the method further comprises using a key exchange performed with Internet Key Exchange (IKE).

15 11. (Previously presented) The method of claim 1, wherein the second secure connection is registered for immediate and/or later use.

20 12. (Previously presented) The method of claim 11, wherein the registration for later use is made by the second terminal in a connection table.

25 13. (Previously presented) The method of claim 3, wherein the method further comprises sending the message to secure traffic between a mobile computer and a destination computer.

14. (Previously presented) The method of claim 13, wherein the

method further comprises using a tunneling protocol together with IPSec to provide a tunneling capability.

15. (Previously presented) The method of claim 14, wherein the
5 method further comprises using a Layer 2 Tunneling Protocol (L2TP) tunneling protocol together with IPSec to provide a tunneling capability.

16. (Previously presented) The method of claim 3, wherein the
10 method further comprises using an IPSec tunnel mode to secure traffic between a mobile computer and a destination computer.

17-18. (Canceled)

REMARKS

Reconsideration of the application is respectfully
5 requested. Claims 1-8, 10-14 and 16 were rejected under
Section 103 as being obvious over Sturniolo in view of Herle.
This rejection is respectfully traversed.

No new matter has been added. Support may, for
example, be found on page 14, lines 20-22. The original
10 claims 7-8 also provide some support for the amended claim 1.
One important aspect of the present invention is that the
method ensures secure forwarding even when the first terminal,
such as a mobile phone, changes from a first address to a
second address. The problem of the prior art solutions is
15 that when the mobile terminal changes to the second address
the already established first secure connection does not work
because it was only defined for the first address of the
mobile terminal. A second secure connection must then be
established by using a rather cumbersome key exchange
20 protocol.

In Sturniolo, the "second terminal" (i.e. the
device) that communicates with the first terminal uses the
same address both before and after the move of the first
terminal. On page 2, lines 45-52, Sturniolo explains that the
25 actual network addresses of the mobile terminal becomes
transparent to the device so that even if the mobile terminal

roams from one LAN to another communication between the mobile terminal and the device is not interrupted so as to provide seamless roaming. This means the device is using the same address before and after the mobile terminal roams. At the

5 end of the abstract Sturniolo explains that "the device is able to maintain communications with the mobile terminal without requiring knowledge of a change in the network address of the mobile terminal." This means Sturniolo's device would not be able to know when to register an already established

10 second secure connection as being the active connection since it does not even know about the change of address of the mobile terminal. The lack of knowledge of the device is further explained in col. 7, lines 21-29 where Sturniolo states that the device remains "unaware that the mobile

15 terminal 36 has received a new network address." An important point is that Sturniolo's device ("the second terminal") does not know or need to know that the first terminal has changed address since Sturniolo has arranged a gateway (intermediate computer) to take care of the change. It is submitted that

20 Sturniolo never had the problem of the security connection not working after an address change of the mobile terminal since there is no secure connection established in Sturniolo, as agreed by the Examiner on page 4 of the Office action. Sturniolo merely uses an un-secure connection.

25 Herle does not cure these deficiencies either. It is submitted that Herle also fails to address the issue of how

to handle the change of address of the mobile terminal when using secure connections. The Examiner is respectfully requested to point out where Herle addresses this issue. It is submitted that the address of the mobile terminal does not even change in Herle. Herle uses a SSH tunnel over a TCP/IP connection, as shown in Fig. 3 of Herle, so that the IP addresses cannot change. Herle is merely cited as showing a secure connection defined from one end point to another end point.

10 An important distinction over the cited patents is thus that it is the second terminal that registers the already established second secure connection as being the active connection. As pointed out above, Sturniolo's device ("second terminal") is not even aware of the address change of the mobile terminal ("first terminal") and would thus not know when to register an already established second secure connection as being the active connection as required by the amended claim 1. Therefore, it is submitted that it would not make sense and it would not be obvious to modify Sturniolo so that the device registers an already established second secure connection as being the active connection, as required by the amended claim 1. As indicated above, Herle teaches nothing about how to handle the change of secure connections as a result of the first terminal changing network address.

25 Applicants cannot see why a person of ordinary skill in the art would look to Sturniolo, Herle or the combination

thereof to learn about the features of the amended claim 1
when those features are completely missing in the cited
references. If a secure connection is set up in Sturniolo a
key exchange is first required and there can only be one
5 secure connection setup i.e. for one address only for the
device which never changes since Sturniolo's device is not
even aware of or affected by any change of the addresses of
the mobile terminal. It is submitted that the cited
references would require extensive modifications that are not
10 taught or suggested, to arrive at all of the method steps of
the amended claim 1.

In view of the amended claim 1, Applicants
respectfully request the rejection of claim 1 is withdrawn
because the proposed combination of Sturniolo and Herle fails
15 to teach or suggest all the limitations of the amended claim
1.

Claims 2-8, 10-14 and 16 are submitted to be
allowable because they depend upon the allowable base claim 1
and because each claim includes limitations that are not
20 taught or suggested in the cited reference.

Claim 9 was rejected under §103 as being obvious
over Sturniolo in view of Herle and Takagi. This rejection is
respectfully traversed.

Claim 9 is submitted to be allowable because it
25 depends upon the allowable base claim 1 and because the claim
includes limitations that are not taught or suggested in the

cited references.

Claims 14-15 were rejected under §103 as being obvious over Sturniolo in view of Herle and Jorgensen. This rejection is respectfully traversed.

5 Claims 14-15 are submitted to be allowable because they depend upon the allowable base claim 1 and because the claims include limitations that are not taught or suggested in the cited references.

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

5 Respectfully submitted,

FASTH LAW OFFICES

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

15 **Attorney Docket No. 290.1053USN**

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

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Sami Vaarala, Antti Nuopponen,
Panu PietikainenArt Unit 2432
Confirmation No. 2431

Serial No. 10/490,933

CERTIFICATE OF MAILING

Filed: 26 March 2004

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 **14 July 2010**.For: METHOD AND SYSTEM FOR
ENSURING SECURE
FORWARDING OF MESSAGES

/rfasth/

Examiner: Devin E. Almeida

Rolf Fasth
Attorney for Applicant

Date: 14 July 2010

TRANSMITTAL LETTER**ELECTRONIC SUBMISSION**COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450Enclosed for filing in the above-referenced application are the
following:

- (X) Response to Office Action dated 20 April 2010.
- (X) The Commissioner is hereby authorized to charge any fees
which may be required in connection with the filing of this
correspondence, or credit over-payment, to Account
No. 06-0243.

Respectfully submitted,

FASTH LAW OFFICES

/rfasth/

Rolf Fasth
Registration No. 36,999FASTH LAW OFFICES
26 Pinecrest Plaza, Suite 2
Southern Pines, North Carolina 28387-4301Telephone: 910-687-0001
Facsimile: 910-295-2152**Attorney Ref. No. 290.1053USN**

Electronic Acknowledgement Receipt

EFS ID:	8011984
Application Number:	10490933
International Application Number:	
Confirmation Number:	2431
Title of Invention:	Method and system 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:	290.1053USN
Receipt Date:	14-JUL-2010
Filing Date:	18-APR-2005
Time Stamp:	12:48:00
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	AMD.PDF	31623 <small>f310cba5e012e39469d5fb807022ed55180 317d6</small>	no	11

Warnings:

Information:

2	Miscellaneous Incoming Letter	TRX.PDF	18202 <small>9a1fc448982a76cea4e0a794a482a7238cd 7523</small>	no	1
Warnings:					
Information:					
Total Files Size (in bytes):			49825		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

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

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 10/490,933	Filing Date 04/18/2005	<input type="checkbox"/> To be Mailed
---	---	----------------------------------	---------------------------------------

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

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

APPLICATION AS AMENDED – PART II					OTHER THAN SMALL ENTITY				
	(Column 1)	(Column 2)	(Column 3)		SMALL ENTITY	OR	OTHER THAN SMALL ENTITY		
AMENDMENT	07/14/2010	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)		
		Total <small>(37 CFR 1.16(i))</small>	* 16	Minus	** 20	=	0	X \$ =	
		Independent <small>(37 CFR 1.16(h))</small>	* 1	Minus	*** 3	=	0	X \$ =	
		<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>							
		<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>							
					TOTAL ADD'L FEE		0	OR	TOTAL ADD'L FEE

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

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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of Art Unit 2432

5 Sami Vaarala, Antti Nuopponen, Panu Pietikainen

Serial No. 10/490,933

10 Filed: 26 March 2004

For: METHOD AND NETWORK FOR ENSURING SECURE FORWARDING OF
MESSAGES

15 Examiner: Devin E. Almeida

Date: 14 July 2010

Attorney Docket Number: 290.1053USN

20

AMENDMENT

Do Not Enter
/DA/
8/10/2010

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

This is in response to the Office action of 20 April
2010. Please amend the above-identified patent application as
follows:



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.
10/490,933	04/18/2005	Sami Vaarala	290.1053USN	2431

33369 7590 08/13/2010
FASTH LAW OFFICES (ROLF FASTH)
26 PINECREST PLAZA, SUITE 2
SOUTHERN PINES, NC 28387-4301

EXAMINER

ALMEIDA, DEVIN E

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

2432

NOTIFICATION DATE	DELIVERY MODE
-------------------	---------------

08/13/2010

ELECTRONIC

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

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

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

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

**Advisory Action
Before the Filing of an Appeal Brief**

Application No.

10/490,933

Applicant(s)

VAARALA ET AL.

Examiner

DEVIN ALMEIDA

Art Unit

2432

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

THE REPLY FILED 14 July 2010 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:

a) The period for reply expires 3 months from the mailing date of the final rejection.

b) The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because

(a) They raise new issues that would require further consideration and/or search (see NOTE below);

(b) They raise the issue of new matter (see NOTE below);

(c) They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or

(d) They present additional claims without canceling a corresponding number of finally rejected claims.

NOTE: The Amendment to claims would require further consideration of the cited prior art as well as an updated search. (See 37 CFR 1.116 and 41.33(a)).

4. The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).

5. Applicant's reply has overcome the following rejection(s): _____.

6. Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).

7. For purposes of appeal, the proposed amendment(s): a) will not be entered, or b) will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.

The status of the claim(s) is (or will be) as follows:

Claim(s) allowed: _____.

Claim(s) objected to: _____.

Claim(s) rejected: _____.

Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).

9. The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).

10. The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. The request for reconsideration has been considered but does NOT place the application in condition for allowance because: _____.

12. Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____

13. Other: _____.

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432

/Devin Almeida/
Examiner, Art Unit 2432

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

Application Number	10/490,933	Filing Date	2004-03-26	Docket Number (if applicable)	290.1053USN	Art Unit	2431
First Named Inventor	Sami Vaarala			Examiner Name	Devin Almeida		

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 2010-08-14

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

Doc code: RCEX

Doc description: Request for Continued Examination (RCE)

PTO/SB/30EFS (07-09)

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

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

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

Signature of Registered U.S. Patent Practitioner			
Signature	/rfasth/	Date (YYYY-MM-DD)	2010-09-17
Name	Rolf Fasth	Registration Number	36999

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

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

Privacy Act Statement

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

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

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Sami Vaarala, Antti Nuopponen,
Panu PietikainenArt Unit 2432
Confirmation No. 2431

Serial No. 10/490,933

CERTIFICATE OF MAILING

Filed: 26 March 2004

For: METHOD AND SYSTEM FOR
ENSURING SECURE
FORWARDING OF MESSAGESI HEREBY CERTIFY THAT THIS PAPER AND THE DOCUMENTS
REFERRED TO AS BEING ATTACHED OR ENCLOSED HERewith
ARE BEING SUBMITTED ELECTRONICALLY TO THE UNITED
STATES PATENT AND TRADEMARK OFFICE ON **17 September**
2010.

Examiner: Devin E. Almeida

/rfasth/

Date: 17 September 2010

Rolf Fasth
Attorney for ApplicantTRANSMITTAL LETTERELECTRONIC SUBMISSIONCOMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450Enclosed for filing in the above-referenced application are the
following:

- (X) Response to Advisory Action dated 13 August 2010.
- (X) Applicant hereby petitions to obtain a two month extension
to respond to the outstanding Office Action.
- (X) The Commissioner is hereby authorized to charge any fees
which may be required in connection with the filing of this
correspondence, or credit over-payment, to Account
No. 06-0243.

Respectfully submitted,

FASTH LAW OFFICES

/rfasth/

Rolf Fasth
Registration No. 36,999FASTH LAW OFFICES
26 Pinecrest Plaza, Suite 2
Southern Pines, North Carolina 28387-4301Telephone: 910-687-0001
Facsimile: 910-295-2152Attorney Ref. No. 290.1053USN

RF:nr 9/17/10 128.699DIV

PATENT

Electronic Patent Application Fee Transmittal

Application Number:	10490933			
Filing Date:	18-Apr-2005			
Title of Invention:	Method and system for ensuring secure forwarding of messages			
First Named Inventor/Applicant Name:	Sami Vaarala			
Filer:	Rolf Fasth/Sloan Smith			
Attorney Docket Number:	290.1053USN			
Filed as Small Entity				
U.S. National Stage under 35 USC 371 Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 2 months with \$0 paid	2252	1	245	245

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Request for continued examination	2801	1	405	405
Total in USD (\$)				650

Electronic Acknowledgement Receipt

EFS ID:	8443827
Application Number:	10490933
International Application Number:	
Confirmation Number:	2431
Title of Invention:	Method and system 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:	290.1053USN
Receipt Date:	17-SEP-2010
Filing Date:	18-APR-2005
Time Stamp:	15:38:31
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	\$650
RAM confirmation Number	2090
Deposit Account	060243
Authorized User	
<p>The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:</p> <ul style="list-style-type: none"> 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	Request for Continued Examination (RCE)	sb0030e_fill.pdf	769098 7c67452871d997b0b5d866d37e8f73d842e1d116	no	3

Warnings:

Information:

2	Miscellaneous Incoming Letter	TRX.PDF	18785 b2f830558174321dfa4818dfc4ffb27d611df071	no	2
---	-------------------------------	---------	---	----	---

Warnings:

Information:

3	Fee Worksheet (PTO-875)	fee-info.pdf	31685 f37605ee515d6408b3aeb6bb2657cea33a47c556	no	2
---	-------------------------	--------------	---	----	---

Warnings:

Information:

Total Files Size (in bytes):	819568
-------------------------------------	--------

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

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

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 10/490,933	Filing Date 04/18/2005	<input type="checkbox"/> To be Mailed
---	---	----------------------------------	---------------------------------------

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

APPLICATION AS AMENDED – PART II					OTHER THAN SMALL ENTITY			
	(Column 1)	(Column 2)	(Column 3)	SMALL ENTITY	OR	SMALL ENTITY	OTHER THAN SMALL ENTITY	
				RATE (\$)		RATE (\$)	ADDITIONAL FEE (\$)	
AMENDMENT	09/17/2010	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA				
	Total <small>(37 CFR 1.16(i))</small>	* 16	Minus	** 20	=	0		
	Independent <small>(37 CFR 1.16(h))</small>	* 1	Minus	*** 3	=	0		
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>							
<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>								
					TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE

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

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

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
10/490,933 04/18/2005 Sami Vaarala 290.1053USN 2431

33369 7590 10/26/2010
FASTH LAW OFFICES (ROLF FASTH)
26 PINECREST PLAZA, SUITE 2
SOUTHERN PINES, NC 28387-4301

Table with 1 column: EXAMINER
ALMEDA, DEVIN E

Table with 2 columns: ART UNIT, PAPER NUMBER
2432

Table with 2 columns: NOTIFICATION DATE, DELIVERY MODE
10/26/2010 ELECTRONIC

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

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

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

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

Office Action Summary	Application No. 10/490,933	Applicant(s) VAARALA ET AL.	
	Examiner DEVIN ALMEIDA	Art Unit 2432	

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

Period for Reply

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

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

Status

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

Disposition of Claims

- 4) Claim(s) 1-16 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) 1-16 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) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

This action is in response to the papers filed 9/17/2010.

Response to Arguments

Applicant's arguments with respect to Sturniolo not teaching the second terminal registering the already established second secure connection as being the active connection. Sturniolo teaches in column 22 lines 50 – column 23 line 9 “Consequently, when a device second device in the system queries the DNS1 for the address of the mobile terminal 36 using known network techniques, the DNS1 provides the querying device with the virtual address of the mobile terminal 36. In the present invention the network address of the mobile terminal 36 as stored in the DNS1 is its virtual address identified by the GATEWAY1. The GATEWAY1 is configured to listen for any information directed to a mobile terminal's 36 virtual address included in its virtual circuit table (FIG. 5b). Using known techniques, the GATEWAY1 receives the information directed to the virtual address of the mobile terminal 36 by accepting connections and/or information from devices initiating communications directed to the virtual address of the mobile terminal 36. In turn, the GATEWAY1 forwards the information to the mobile terminal via the corresponding virtual circuit connection previously established between the GATEWAY1 and the mobile terminal 36. The mobile terminal 36 may respond to such information and if it does its via the GATEWAY1. If the mobile terminal 36 responds, the GATEWAY1 receives the response information from the mobile terminal 36 and forwards such information to the initiating device. In the event the mobile terminal 36 then roams to another LAN or WAN and receives another network address (e.g., steps 72, 74 and 76 in FIG. 9A), the

mobile terminal 36 updates the GATEWAY1 with its new address via the flag field FLG as described above in relation to FIG. 4o.” Therefore there the second terminal is registering the already established second secure connection as being the active connection through the GATEWAY1.

Claim Rejections - 35 USC § 103

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

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

Claims 1-8, 10-14, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sturniolo et al (U.S. 6,091,951) in view of Herle (U.S. 7,165,173).

With respect to claim 1, Sturniolo discloses a method for ensuring secure forwarding of a message in a telecommunication network (see abstract i.e. radio communications system), comprising: providing a first terminal from which the message is sent and a second terminal (end device) to which the message is sent (see abstract):

a) establishing a first connection as being an active connection and extending between a first network address of the first terminal (mobile terminal at AP1) and an original network address of the second terminal (see abstract i.e. device on the network backbone), establishing a second connection extending between a second network address of the first terminal and the original network address of the second terminal (see column 10 line 8-55),

b) the first terminal (mobile terminal) changing from the first network address to the second network address (see column 10 line 8-55), the first terminal checking whether the second connection already exists, and

c) when the second connection already exists the second terminal registering the already established second connection as being the active connection without having to reestablish the second connection (see column 10 line 8-55 and column 21 line 19 – column 23 line 9).

Sturniolo does not teach that the connections are secure connection.

Herle teaches that the connections are secure connection from end point to end point through the access point (see figure 2 and column 8 lines 41-63). It 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 to have secure path between the mobile station and provisioning server to increase security of the path (see column 3 lines 37-46). Therefore one would have been motivated to have a secure path between the mobile station and provisioning server.

With respect to claim 2, wherein the method further comprises establishing the second secure connection when the second secure connections does not already exist (see column 10 line 8-55).

With respect to claim 3, wherein the method further comprises establishing the first secure connection by using the IPSec protocols (see Herle column 9 lines 4-22).

With respect to claim 4, wherein the method further comprises providing the message with IP packets (see column 9 lines 21-38).

With respect to claim 5, checking whether a secure connection between the new network address and the other terminal already exists (see figure 2 and column 10 line 8-55).

With respect to claim 6, checking by using a connection table (see figure 5a and 5b).

With respect to claim 7, a signaling message or signaling message exchange between the first terminal and the second terminal (see figure 2 and column 10 line 8-55).

With respect to claim 8, automatically updating the new network address of the first terminal by the second terminal when the first terminal sends a message from the new network address (see figure 2 and column 10 line 8-55).

With respect to claim 10, using a key exchange performed with Internet key exchange IKE (see Herle figure 2, 3 and column 9 lines 5-22).

With respect to claim 11, the second secure connection is registered for immediate and/or later use (see figure 2 and column 10 line 8-55).

With respect to claim 12, wherein the registration for later use is made by the second terminal in a connection table (see figure 2 and column 10 line 8-55).

With respect to claim 13, to secure traffic between the mobile computer and a destination computer (see figure 2 and column 10 line 8-55).

With respect to claim 14, using a tunneling protocol together with IPSec to provide a tunneling capability (see Herle figure 2, 3 and column 9 lines 5-22).

With respect to claim 16, an IPSec tunnel mode is used to secure traffic between the mobile computer and a destination computer (see Herle figure 2, 3 and column 9 lines 5-22).

Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sturniolo et al (U.S. 6,091,951) in view of Herle (U.S. 7,165,173) in view of Takagi et al (U.S. 7,143,282).

Sturniolo does not teach that a key exchange when establishing the secure connection. Takagi teaches a key exchange when establishing the secure connection (see Takagi column 8 lines 29-34). It 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 to have the Security Associations of Ala-Laurila to be set up manually as taught in Takagi by Internet Key Exchange to increase the compatibility of the system (see Takagi column 8 lines 29-34). Therefore one would have been motivated to have Security Associations be able to be set up manually by Internet Key Exchange.

Claims 14 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sturniolo et al (U.S. 6,091,951) in view of Herle (U.S. 7,165,173) in view of Jorgensen (U.S. 6,452,915).

Sturniolo does not teach with respect to claim 14, using a tunneling protocol together with IPsec to provide a tunneling capability. Jorgensen using a tunneling protocol together with IPsec to provide a tunneling capability (see Jorgensen column 44 lines 8-17). It 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 to have used L2TP over IPsec because L2TP can carry multiple protocols. L2TP also offers transmission capability over non-IP networks (see Jorgensen column 44 lines 8-17). Therefore one would have been motivated to have used L2TP over IPsec.

With respect to claim 15 where the Layer 2 Tunneling Protocol (L2TP) tunneling protocol together with IPsec to provide a tunneling capability (see Jorgensen column 44 lines 8-17).


Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Devin Almeida whose telephone number is 571-270-1018. The examiner can normally be reached on Monday-Thursday from 7:30 A.M. to 5:00 P.M. The examiner can also be reached on alternate Fridays from 7:30 A.M. to 4:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on 571-272-3799. 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.

/Devin Almeida/
Examiner, Art Unit 2432

Index of Claims 	Application/Control No. 10490933	Applicant(s)/Patent Under Reexamination VAARALA ET AL.
	Examiner DEVIN ALMEIDA	Art Unit 2432

✓	Rejected
=	Allowed

-	Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

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

CLAIM		DATE									
Final	Original	10/08/2008	03/18/2009	06/08/2009	10/28/2009	01/05/2010	04/13/2010	10/21/2010			
	1	✓	✓	✓	✓	✓	✓	✓			
	2	✓	✓	✓	✓	✓	✓	✓			
	3	✓	✓	✓	✓	✓	✓	✓			
	4	✓	✓	✓	✓	✓	✓	✓			
	5	✓	✓	✓	✓	✓	✓	✓			
	6	✓	✓	✓	✓	✓	✓	✓			
	7	✓	✓	✓	✓	✓	✓	✓			
	8	✓	✓	✓	✓	✓	✓	✓			
	9	✓	✓	✓	✓	✓	✓	✓			
	10	✓	✓	✓	✓	✓	✓	✓			
	11	✓	✓	✓	✓	✓	✓	✓			
	12	✓	✓	✓	✓	✓	✓	✓			
	13	✓	✓	✓	✓	✓	✓	✓			
	14	✓	✓	✓	✓	✓	✓	✓			
	15	✓	✓	✓	✓	✓	✓	✓			
	16	✓	✓	✓	✓	✓	✓	✓			
	17	✓	-	-	-	-	-	-			
	18	-	-	-	-	-	-	-			

UNITED STATES PATENT AND TRADEMARK OFFICE
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA VA 22313-1451

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

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



**Courtesy Reminder for
Application Serial No: 10/490,933**

Attorney Docket No: 290.1053USN
Customer Number: 33369
Date of Electronic Notification: 10/26/2010

This is a courtesy reminder that new correspondence is available for this application. The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

An email notification regarding the correspondence was sent to the following email address(es) associated with your customer number:

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

Please verify that these email addresses are correct.

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

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

NOTICE OF APPEAL FROM THE EXAMINER TO THE BOARD OF PATENT APPEALS AND INTERFERENCES		Docket Number (Optional) 290.1053USN	
I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] 18 April 2011 (electronically) on _____ Signature <u>/rfasth/</u> Typed or printed name <u>Rolf Fasth</u>		In re Application of Sami Vaarala, Antti Nuopponen, Panu Pietikainen	
		Application Number 10490933	Filed 2004-03-26
		For METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION	
		Art Unit 2432	Examiner Devin E. Almeida
Applicant hereby appeals to the Board of Patent Appeals and Interferences from the last decision of the examiner.			
The fee for this Notice of Appeal is (37 CFR 41.20(b)(1))		\$ <u>540.00</u>	
<input checked="" type="checkbox"/> Applicant claims small entity status. See 37 CFR 1.27. Therefore, the fee shown above is reduced by half, and the resulting fee is:		\$ <u>270.00</u>	
<input type="checkbox"/> A check in the amount of the fee is enclosed.			
<input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached.			
<input type="checkbox"/> The Director has already been authorized to charge fees in this application to a Deposit Account.			
<input checked="" type="checkbox"/> The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. <u>060243</u> .			
<input checked="" type="checkbox"/> A petition for an extension of time under 37 CFR 1.136(a) (PTO/SB/22) is enclosed.			
WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.			
I am the			
<input type="checkbox"/> applicant/inventor.	<u>/rfasth/</u> Signature		
<input type="checkbox"/> assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)	<u>Rolf Fasth</u> Typed or printed name		
<input checked="" type="checkbox"/> attorney or agent of record. Registration number <u>36999</u>	<u>910-687-0001</u> Telephone number		
<input type="checkbox"/> attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34. _____	<u>18 April 2011 (electronically)</u> Date		
NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.			
<input checked="" type="checkbox"/> *Total of <u>1</u> forms are submitted.			

This collection of information is required by 37 CFR 41.31. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Privacy Act Statement

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

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

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Sami Vaarala, Antti Nuopponen,
Panu PietikainenArt Unit 2432
Confirmation No. 2431

Serial No. 10/490,933

CERTIFICATE OF MAILING

Filed: 26 March 2004

For: METHOD AND SYSTEM FOR
ENSURING SECURE
FORWARDING OF MESSAGESI HEREBY CERTIFY THAT THIS PAPER AND THE DOCUMENTS
REFERRED TO AS BEING ATTACHED OR ENCLOSED HERewith
ARE BEING SUBMITTED ELECTRONICALLY TO THE UNITED
STATES PATENT AND TRADEMARK OFFICE ON **18 April**
2011.

Examiner: Devin E. Almeida

/rfasth/

Date: 18 April 2011

Rolf Fasth
Attorney for ApplicantTRANSMITTAL LETTERELECTRONIC SUBMISSIONCOMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450Enclosed for filing in the above-referenced application are the
following:

- (X) Notice of Appeal.
- (X) **Applicant hereby petitions to obtain a three-month extension to respond to the outstanding Office Action.**
- (X) The Commissioner is hereby authorized to charge any fees which may be required in connection with the filing of this correspondence, or credit over-payment, to Account No. 06-0243.

Respectfully submitted,

FASTH LAW OFFICES

/rfasth/

Rolf Fasth
Registration No. 36,999FASTH LAW OFFICES
26 Pinecrest Plaza, Suite 2
Southern Pines, North Carolina 28387-4301Telephone: 910-687-0001
Facsimile: 910-295-2152Attorney Ref. No. 290.1053USN

Electronic Patent Application Fee Transmittal

Application Number:	10490933			
Filing Date:	18-Apr-2005			
Title of Invention:	Method and system for ensuring secure forwarding of messages			
First Named Inventor/Applicant Name:	Sami Vaarala			
Filer:	Rolf Fasth/Sloan Smith			
Attorney Docket Number:	290.1053USN			
Filed as Small Entity				
U.S. National Stage under 35 USC 371 Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Notice of appeal	2401	1	270	270
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension - 3 months with \$0 paid	2253	1	555	555
Miscellaneous:				
Total in USD (\$)				825

Electronic Acknowledgement Receipt

EFS ID:	9904689
Application Number:	10490933
International Application Number:	
Confirmation Number:	2431
Title of Invention:	Method and system 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:	290.1053USN
Receipt Date:	18-APR-2011
Filing Date:	18-APR-2005
Time Stamp:	19:18:24
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	\$825
RAM confirmation Number	5364
Deposit Account	060243
Authorized User	
<p>The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:</p> <ul style="list-style-type: none"> Charge any Additional Fees required under 37 C.F.R. 1.492 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees) 	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)
 Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)
 Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Notice of Appeal Filed	sb0031.pdf	248699 855caa7a809aa76d8190e6ca0102961ef4b62ac1	no	2

Warnings:

Information:

2	Miscellaneous Incoming Letter	TRX.PDF	19716 f3c273dd4c48804b83037ca620d4c2fa122822ff	no	1
---	-------------------------------	---------	---	----	---

Warnings:

Information:

3	Fee Worksheet (PTO-875)	fee-info.pdf	31717 a3ffd6f8d6eb7f3203a1724a48f0228d2da0215a	no	2
---	-------------------------	--------------	---	----	---

Warnings:

Information:

Total Files Size (in bytes): 300132

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

Attorney Docket No. 290.1053USN 4/18/11

Serial No. 10/490,933
Filed: 18 April 2005
Art Unit: 2432

Attorney Matter No. 290.1053USN

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF APPEALS AND INTERFERENCES

In re application of: Sami Vaarala et al

)	
)	
Serial No. 10/490,933)	
)	APPEAL BRIEF
)	
Filed: 18 April 2005)	
)	
For: METHOD AND SYSTEM FOR)	
ENSURING SECURE FORWARDING)	
OF MESSAGES)	
)	
)	Art Unit 2432
)	
)	Examiner Devin E. Almeida
)	
)	
)	

Date: 19 April 2011

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

APPELLANT'S BRIEF ON APPEAL

Real Party in Interest

The real party in interest is MPH Technologies Oy,
Tekniikantie 14, FIN-02150 Espoo, Finland, the recorded assignee
of the above-captioned patent application.

Related Appeals and Interferences

No related appeals or interferences of this application are known to the Appellant, the Appellant's legal representative or assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

Status of the Claims

Rejection 1

Claims 1-8, 10-14, and 16 stand rejected in the Office action dated 26 October 2010 as being obvious over Sturniolo et al (US 6,091,951) in view of Herle (US 7,165,173).

Rejection 2

Claim 9 stands rejected in the Office action dated 26 October 2010 as being obvious over Sturniolo et al (US 6,091,951) in view of Herle (US 7,165,173) and further in view of Takagi et al (US 7,143,282).

Rejection 3

Claims 14-15 stand rejected in the Office action dated 26 October 2010 as being obvious over Sturniolo et al (US 6,091,951) in view of Herle (US 7,165,173) and further in view of Jorgensen (US 6,452,915).

The application has been rejected at least twice. A copy of the claims is reproduced as Claims Appendix hereto. The rejections of claims 1-16 are appealed. Claims 17-18 were canceled in a previous response.

Status of Amendments

All Amendments have been entered.

Summary of Claimed Subject Matter

The application has one independent claim (i.e. claim 1). Independent claim 1 refers to a method for ensuring secure forwarding of a message in a telecommunication network (page 1, lines 6-7 and page 12, lines 22-23). A first terminal is provided from which the message is sent and a second terminal is provided to which the message is sent (page 12, lines 23-24). A first secure connection is established as being an active connection and extending between a first network address of the first terminal and an original network address of the second terminal (page 12, lines 25-27). A second secure connection is established extending between a second network address of the first terminal and the original network address of the second terminal (page 12, lines 27-30). The first terminal changes from the first network address to the second network address (page 12,

lines 27-28). The first terminal checks whether the second secure connection already exists (page 19, lines 5-7). When the second secure connection already exists, the second terminal registers the already established second secure connection as being the active connection without having to reestablish the second secure connection (page 19, lines 9-17).

Claim 2 refers to the step of establishing the second secure connection when the second secure connection does not already exist (original claim 2 and page 13, lines 1-3). Claim 3 refers to the step of establishing the first secure connection by using IPsec protocols (original claim 3 and page 13, lines 18-20). Claim 4 refers to the step of providing the message with IP packets (original claim 4 and page 13, lines 19-20). Claim 5 refers to the step of checking whether a secure connection between the new network address and the second terminal already exists (original claim 5 and page 19, lines 4-10). Claim 6 refers to the step of checking by using a connection table (original claim 6 and page 13, lines 24-26). Claim 7 refers to the step of using a signaling message or signaling message exchange between the first terminal and the second terminal (original claim 7 and page 14, lines 6-9). Claim 8 refers to the step of automatically updating the new network address of the first terminal by the second terminal when the first terminal sends a message from the new network address (original claim 8

and page 14, lines 11-22). Claim 9 refers to the step of using a key exchange when establishing the first secure connection (original claim 9). Claim 10 refers to the step of using a key exchange performed with Internet Key Exchange (IKE) (original claim 10). Claim 11 refers to the step of registering the second secure connection for immediate and/or later use (original claim 11). Claim 12 refers to the step of the second terminal doing the registration for later use in a connection table (original claim 12). Claim 13 refers to the step of sending the message to secure traffic between a mobile computer and a destination computer (original claim 13). Claim 14 refers to the step of using a tunneling protocol together with IPsec to provide a tunneling capability (original claim 14). Claim 15 refers to the step of using a Layer 2 Tunneling Protocol (L2TP) tunneling protocol together with IPsec to provide a tunneling capability (original claim 15 and page 15, lines 18-21)). Claim 16 refers to the step of using an IPsec tunnel mode to secure traffic between a mobile computer and a destination computer (original claim 16 and page 15, lines 4-9).

Grounds Of Rejection To Be Reviewed On Appeal

Rejection 1

Whether the Examiner properly rejected claims 1-8, 10-14 and 16 as being obvious over Sturniolo in view of Herle.

Rejection 2

Whether the Examiner properly rejected claim 9 as being obvious over Sturniolo in view of Herle and further in view of Takagi.

Rejection 3

Whether the Examiner properly rejected claims 14-15 as being obvious over Sturniolo in view of Herle and further in view of Jorgensen.

Argument (Rejection 1) - 35 U.S.C. 103 (Obviousness)

Reconsideration of the application is respectfully requested. To provide some background, one problem with IPSec connections or mobile connections in the past was that the end points of the IPsec tunnel mode SA (security association) were fixed. There was no feature in conventional systems in the past for changing any of the parameters of an SA other than by establishing a new SA that replaces the previous SA. More particularly, since mobile terminals move and thus change their network points frequently and since IPsec connections are bound to fixed addresses, the mobile terminals must establish new IPsec connections from each new point of attachment. This requires the exchange of keys etc. which is a cumbersome process that uses computation time. The method of the present invention provides a solution to this problem by enabling the second terminal to

register an already established second secure connection as being the active connection without having to reestablish the second secure connection.

On page 3, lines 1-4 of the Office action the Examiner concludes that the second terminal (the "device" in Sturniolo) registers the already established second secure connection as being the active connection through the GATEWAY1. Appellants respectfully disagree and cannot follow the rationale of the Examiner. The Examiner does not seem to have noticed that in Sturniolo the same mobile terminal (first terminal) is both moving and updating its new address (but the second terminal is not involved). In the present invention, the first terminal moves and the second terminal is registering the second secure connection as being the active connection.

The text copied by the Examiner (col. 22, lines 50 - col. 23, line 9 of Sturniolo) seems to merely state that "the mobile terminal 36 updates the GATEWAY1 with its new address via the flag field FLG as described above in relation to Fig. 4o." Appellants cannot see that "the mobile terminal updating the Gateway1 with its new address" is the same thing as the device (second terminal) "registering the already established second secure connection as being the active connection without having to reestablish the second secure connection" as required by claim 1. Firstly, the mobile terminal is not equivalent to the "second

terminal" in claim 1. Secondly, updating the intermediary computer with a new address is not the same thing as registering an already established secure connection as being the active connection. Thirdly, the device does not seem to be involved at all. There are good reasons for this because the address of the mobile terminal is transparent to Sturniolo's device which is not even aware of the address change of the mobile terminal, as explained in detail below.

Appellants submit that Sturniolo is distinctly different from the present invention. In Sturniolo when the mobile terminal moves the mobile terminal merely updates its address to Gateway1 but the same secure connection is being used. In the present invention there are, in general, two different secure connections involved and which secure connection is used changes when the first terminal moves from one network to another network.

In Sturniolo the gateway (GATEWAY1) does not even inform the device (that the mobile terminal is communicating with) as the system transparent to the devices in the network. This means the "second terminal" in Sturniolo (i.e. the device) that communicates with the first terminal uses the same address both before and after the move of the first terminal. In Sturniolo, the "second terminal " ("the device") that communicates with the first terminal (the mobile terminal 36)

uses the same address for the first terminal when sending a message to the first terminal both before the moving and after moving. This is explained in many places in Sturniolo. For example, col. 2, lines 45 - 47 states: "By serving as an intermediary (reference made to the gateway), the actual network addresses of the mobile terminal become transparent to the devices with which the mobile terminals are communicating." In col. 2, lines 63 - 65, Sturniolo explains: "With the gateway in the present invention, however, it is not necessary for the devices to know the new network address of the mobile terminal." In col. 2, line 67 - column 3, line 1, he states: "There is no need to first inform the devices of the new network address." Col. 4, lines 6-9 further explains that "the device is able to maintain network communications with the mobile terminal without requiring knowledge of a change in the network address of the mobile terminal." In other words, from second terminal's (Sturniolo's "device") point of view, the address of the mobile terminal does not change as the mobile terminal moves from one network to another. In contrast, the address does change in the present invention. Thus, in Sturniolo, the second terminal does not know that the mobile terminal (the first terminal) has changed address. This unawareness is well summarized in col. 7, lines 23 - 26 which states: "The devices with which the mobile terminal 36 is communicating remain unaware that the mobile

terminal 36 has received a new network address." The last sentence of the abstract states: "The device is able to maintain communications with the mobile terminal without requiring knowledge of a change in the network address of the mobile terminal." Because the device is unaware of the change of address of the mobile terminal the device would not register a second secure connection as being the active connection. Since the device is unaware there is not even anything to trigger such as registration step. The above cited text segments are explained in more detail below.

As indicated earlier, on page 2, lines 45-52, Sturniolo explains that the actual network addresses of the mobile terminal becomes transparent to the device so that even if the mobile terminal roams from one LAN to another the communication between the mobile terminal and the device is not interrupted so as to provide seamless roaming. This means the device is using the same address before and after the mobile terminal roams. At the end of the abstract, Sturniolo explains that "the device is able to maintain communications with the mobile terminal without requiring knowledge of a change in the network address of the mobile terminal." This means Sturniolo's device would not be able to know when to register an already established second secure connection as being the active connection since it does not even know about the change of address of the mobile terminal.

The lack of knowledge of the device is further explained in col. 7, lines 21-29 where Sturniolo states that the device remains "unaware that the mobile terminal 36 has received a new network address." An important point is that Sturniolo's device ("the second terminal") does not know or need to know that the first terminal has changed address since Sturniolo has arranged a gateway (intermediate computer or perhaps a host) to take care of the change. It is submitted that Sturniolo never had the problem of the security connection not working after an address change of the mobile terminal since there is no secure connection established in Sturniolo, as agreed by the Examiner on page 4 of the Office action. Sturniolo merely uses an un-secure connection.

On a different note, the Examiner has compared the "device" of Sturniolo with the "other terminal" of the present invention. In a way this is not a correct comparison. Sturniolo aims to solve roaming problems in mobile telecommunications networks when the serving base station (access point) changes as a result of a move by the mobile terminal. In Sturniolo, the device communicates with the mobile terminal via the access point (host), so in fact it is the host that should be considered as the other terminal not the device. In Sturniolo, when the mobile terminal moves, also the host changes and after the move of the mobile terminal a different host will be used. In the present

invention, the mobile terminal communicates with a host which is the second terminal (also called "other terminal) and the secure connection is between the mobile terminal and the host, as shown in Fig. 2.

Herle does not cure these deficiencies either. Herle was merely cited to show a secure connection defined from one end point to another end point. It is submitted that Herle also fails to address the issue of how to handle the change of address of the mobile terminal when using secure connections. The Examiner has been respectfully requested to point out where Herle addresses this issue but the Examiner has not responded to this request. It is submitted that the address of the mobile terminal does not even change in Herle. Herle uses a SSH tunnel over a TCP/IP connection, as shown in Fig. 3 of Herle, so that the IP addresses cannot change.

It is important to realize that the problem solved by the present invention lies in the secure connection itself, i.e. how to handle the secure connection when a move of the mobile terminal has taken place. Although Herle discloses some kind of secure connections but none of them, not even when combined with the teachings of Sturniolo, is able to handle a move by a mobile terminal while maintaining the connection secure, which was the problem to be solved by the present invention. In the present invention, it is not necessary use any key exchange after the

move by the mobile terminal since there is no need to setup a new secure connection. It is merely necessary for the second terminal to register an already existing secure connection instead.

If a secure connection is setup in Sturniolo, a key exchange is first needed. In addition, there can only be one security connection setup (for one address only, which never changes) in Sturniolo, since from the other terminal's (the device) point of view, the address of the mobile terminal does never change. Sturniolo has a special network with an extra gateway for handling moves by mobile terminals, while the system of the present invention is implemented in a normal IP network, wherein the address of the mobile terminal changes at moving also from the other terminal's point of view.

In summary, an important distinction over the cited patents is thus that it is the second terminal that registers the already established second secure connection as being the active connection. As pointed out above, Sturniolo's device ("second terminal") is not even aware of the address change of the mobile terminal ("first terminal") and would thus not know when to register an already established second secure connection as being the active connection as required by the amended claim 1. Therefore, it is submitted that it would not make sense and it would not be obvious to modify Sturniolo and the other cited

references so that the device registers an already established second secure connection as being the active connection, as required by the amended claim 1. As indicated above, Herle teaches nothing about how to handle the change of secure connections as a result of the first terminal changing network address.

Appellants cannot see why a person of ordinary skill in the art would look to Sturniolo, Herle or the combination thereof to learn about the features of the amended claim 1 when those features are completely missing in the cited references. If a secure connection is set up in Sturniolo a key exchange is first required and there can only be one secure connection setup i.e. for one address only for the device which never changes since Sturniolo's device is not even aware of or affected by any change of the addresses of the mobile terminal. It is submitted that the cited references would require extensive modifications that are not taught or suggested, to arrive at all of the method steps of the amended claim 1. It is submitted that the cited references would require extensive modifications to arrive at all the limitations of claim 1.

Even assuming *arguendo* that the requisite method steps of claim 1 are shown by the combination of Sturniolo and Herle, *prima facie* support for combining the references, according to the requirements as set forth in M.P.E.P. § 2142 has not been

provided in the Office Actions.

As provided in M.P.E.P. § 2142, the Supreme Court in *KSR International v. Teleflex Inc.*, 82 USPQ2d 1385, 1396 (2007) specified that the analysis supporting a rejection under 35 U.S.C. § 103 should be made explicit. “[R]ejections on obviousness cannot be sustained with mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.” *In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006). Furthermore, the Examiner must make “explicit” this rationale of “the apparent reason to combine the known elements in the fashion claimed,” including a detailed explanation of “the effects of demands known to the design community or present in the marketplace” and “the background knowledge possessed by a person having ordinary skill in the art” (KSR, page 14).

The only rationale provided in support of the 103(a) rejection of claim 1 is in the middle of page 4 of the Office action, which merely asserts it would have been obvious to modify the teaching method of Sturniolo with Herle “to increase security of the path (see column 3 lines 37-46). Therefore one would have been motivated to have a secure path between the mobile station and the provisioning server” (emphasis added). The Examiner has merely provided one benefit, or advantage of the modification as

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

However, merely stating that a benefit of the modification exists, as done above, does not provide the "articulated reasoning with some rationale underpinning to support the legal conclusion of obviousness, required under *KSR*. By definition, every patentable invention must be "beneficial" - and *arguendo* every invention contemplates at least some new benefit(s) in arriving at the invention - certainly this does not render the benefit obvious or expected. Because every modification or element has a corresponding use or benefit, the above reasoning could be applied to any improvement. It appears therefore that "hindsight construction" may have perhaps played a role in arriving at the present ground for rejection in the Office action - which though difficult perhaps to avoid in many cases, is nonetheless impermissible in making a *prima facie* showing of obviousness.

According to M.P.E.P. 2142, "the examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness" (emphasis added). It is respectfully submitted that the Examiner has not factually supported the *prima facie* conclusion of obviousness. Because a *prima facie* conclusion of

obviousness has not been provided in the Office Action, Appellants respectfully request reconsideration and withdrawal of this ground for rejection.

In view of the amended claim 1, Appellants respectfully request the rejection of claim 1 is withdrawn because the proposed combination of Sturniolo and Herle fails to teach or suggest all the limitations of the amended claim 1 and the Examiner has not met his burden of establishing a *prima facie* case of obviousness.

Argument (Rejection 2) - 35 U.S.C. 103 (Obviousness)

Claim 9 is submitted to be allowable because the claim depends upon the allowable base claim 1 and because the claim includes limitations that are not taught or suggested in the cited references.

Argument (Rejection 3) - 35 U.S.C. 103 (Obviousness)

Claims 14-15 are submitted to be allowable because the claims depend upon the allowable base claim 1 and because the claims include limitations that are not taught or suggested in the cited references.

Attorney Docket No. 290.1053USN 4/18/11

Serial No. 10/490,933
Filed: 18 April 2005
Art Unit: 2432

In view of the above arguments, Appellants respectfully request that the Board reverse the Examiner's rejections.

Respectfully submitted,

FASTH LAW OFFICES

/rfasth/
Rolf Fasth
Registration No. 36,999

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

Claims Appendix

1. (Previously presented) A method for ensuring secure forwarding of a message in a telecommunication network, comprising:

providing a first terminal from which the message is sent and a second terminal to which the message is sent,

a) establishing a first secure connection as being an active connection and extending between a first network address of the first terminal and an original network address of the second terminal, establishing a second secure connection extending between a second network address of the first terminal and the original network address of the second terminal,

b) the first terminal changing from the first network address to the second network address, the first terminal checking whether the second secure connection already exists, and

c) when the second secure connection already exists, the second terminal registering the already established second secure connection as being the active connection without having to reestablish the second secure connection.

2. (Previously presented) The method of claim 1, wherein the method further comprises establishing the second secure connection when the second secure connection does not already exist.

3. (Previously presented) The method of claim 1, wherein the method further comprises establishing the first secure connection by using IPsec protocols.

4. (Previously presented) The method of claim 1, wherein the method further comprises providing the message with IP packets.

5. (Previously presented) The method of claim 1, wherein the method further comprises checking whether a secure connection between the new network address and the second terminal already exists.

6. (Previously presented) The method of claim 5, wherein the method further comprises checking by using a connection table.

7. (Previously presented) The method of claim 1, wherein the method further comprises using a signaling message or signaling message exchange between the first terminal and the second terminal.

8. (Previously presented) The method of claim 1, wherein the method further comprises automatically updating the new network address of the first terminal by the second terminal when the

first terminal sends a message from the new network address.

9. (Previously presented) The method of claim 1, wherein the method further comprises using a key exchange when establishing the first secure connection.

10. (Previously presented) The method of claim 2, wherein the method further comprises using a key exchange performed with Internet Key Exchange (IKE).

11. (Previously presented) The method of claim 1, wherein the second secure connection is registered for immediate and/or later use.

12. (Previously presented) The method of claim 11, wherein the registration for later use is made by the second terminal in a connection table.

13. (Previously presented) The method of claim 3, wherein the method further comprises sending the message to secure traffic between a mobile computer and a destination computer.

14. (Previously presented) The method of claim 13, wherein the method further comprises using a tunneling protocol together with

IPSec to provide a tunneling capability.

15. (Previously presented) The method of claim 14, wherein the method further comprises using a Layer 2 Tunneling Protocol (L2TP) tunneling protocol together with IPSec to provide a tunneling capability.

16. (Previously presented) The method of claim 3, wherein the method further comprises using an IPSec tunnel mode to secure traffic between a mobile computer and a destination computer.

17-18. (Canceled)

Attorney Docket No. 290.1053USN 4/18/11

Serial No. 10/490,933
Filed: 18 April 2005
Art Unit: 2432

Evidence Appendix

There is no evidence to be presented in this appendix.

Attorney Docket No. 290.1053USN 4/18/11

Serial No. 10/490,933
Filed: 18 April 2005
Art Unit: 2432

Related Proceedings Appendix

There is no related proceeding to be presented in this appendix.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Sami Vaarala, Antti Nuopponen,
Panu PietikainenArt Unit 2432
Confirmation No. 2431

Serial No. 10/490,933

CERTIFICATE OF MAILING

Filed: 26 March 2004

For: METHOD AND SYSTEM FOR
ENSURING SECURE
FORWARDING OF MESSAGESI HEREBY CERTIFY THAT THIS PAPER AND THE DOCUMENTS
REFERRED TO AS BEING ATTACHED OR ENCLOSED HERewith
ARE BEING SUBMITTED ELECTRONICALLY TO THE UNITED
STATES PATENT AND TRADEMARK OFFICE ON **20 April**
2011.

Examiner: Devin E. Almeida

/rfasth/

Date: 20 April 2011

Rolf Fasth
Attorney for ApplicantTRANSMITTAL LETTERELECTRONIC SUBMISSIONCOMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450Enclosed for filing in the above-referenced application are the
following:

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

Respectfully submitted,

FASTH LAW OFFICES

/rfasth/

Rolf Fasth
Registration No. 36,999FASTH LAW OFFICES
26 Pinecrest Plaza, Suite 2
Southern Pines, North Carolina 28387-4301Telephone: 910-687-0001
Facsimile: 910-295-2152Attorney Ref. No. 290.1053USN

Electronic Patent Application Fee Transmittal

Application Number:	10490933			
Filing Date:	18-Apr-2005			
Title of Invention:	Method and system for ensuring secure forwarding of messages			
First Named Inventor/Applicant Name:	Sami Vaarala			
Filer:	Rolf Fasth/Sloan Smith			
Attorney Docket Number:	290.1053USN			
Filed as Small Entity				
U.S. National Stage under 35 USC 371 Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Filing a brief in support of an appeal	2402	1	270	270
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				270

Electronic Acknowledgement Receipt

EFS ID:	9918412
Application Number:	10490933
International Application Number:	
Confirmation Number:	2431
Title of Invention:	Method and system 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:	290.1053USN
Receipt Date:	20-APR-2011
Filing Date:	18-APR-2005
Time Stamp:	13:42:01
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$270
RAM confirmation Number	23
Deposit Account	060243
Authorized User	
<p>The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:</p> <ul style="list-style-type: none"> Charge any Additional Fees required under 37 C.F.R. 1.492 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees) 	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)
 Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)
 Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Appeal Brief Filed	APPEAL_BRIEF.PDF	45375 b0f0cd371fd989eb645625d8dbbf201e5d3ce5b	no	24

Warnings:

Information:

2	Miscellaneous Incoming Letter	TRX.PDF	18081 1e8e296422697469f55e378706bccce96227bf2	no	1
---	-------------------------------	---------	--	----	---

Warnings:

Information:

3	Fee Worksheet (PTO-875)	fee-info.pdf	29897 0a12986a7bcafbca1b8a7da67ad45fedc773b316	no	2
---	-------------------------	--------------	---	----	---

Warnings:

Information:

Total Files Size (in bytes): 93353

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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



UNITED STATES PATENT AND TRADEMARK OFFICE

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

33369 7590 06/17/2011
FASTH LAW OFFICES (ROLF FASTH)
26 PINECREST PLAZA, SUITE 2
SOUTHERN PINES, NC 28387-4301

EXAMINER
ALMEIDA, DEVIN E
ART UNIT 2432 PAPER NUMBER

DATE MAILED: 06/17/2011

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

TITLE OF INVENTION: METHOD AND SYSTEM FOR ENSURING SECURE FORWARDING OF MESSAGES

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

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

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

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

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

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

If the SMALL ENTITY is shown as NO:

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

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

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

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

PART B - FEE(S) TRANSMITTAL

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

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

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

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

33369 7590 06/17/2011
FASTH LAW OFFICES (ROLF FASTH)
 26 PINECREST PLAZA, SUITE 2
 SOUTHERN PINES, NC 28387-4301

Certificate of Mailing or Transmission

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

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/490,933	04/18/2005	Sami Vaarala	290.1053USN	2431

TITLE OF INVENTION: METHOD AND SYSTEM 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	09/19/2011

EXAMINER	ART UNIT	CLASS-SUBCLASS
ALMEIDA, DEVIN E	2432	713-160000

<p>1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).</p> <p><input type="checkbox"/> Change of correspondence address (or Change of Correspondence Address Form PTO/SB/122) attached.</p> <p><input type="checkbox"/> "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. Use of a Customer Number is required.</p>	<p>2. For printing on the patent front page, list</p> <p>(1) the names of up to 3 registered patent attorneys or agents OR, alternatively, _____ 1</p> <p>(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. _____ 2</p> <p>_____ 3</p>
---	---

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

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

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

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

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

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

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

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

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

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



UNITED STATES PATENT AND TRADEMARK OFFICE

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

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
10/490,933 04/18/2005 Sami Vaarala 290.1053USN 2431

33369 7590 06/17/2011
FASTH LAW OFFICES (ROLF FASTH)
26 PINECREST PLAZA, SUITE 2
SOUTHERN PINES, NC 28387-4301

EXAMINER

ALMEIDA, DEVIN E

ART UNIT PAPER NUMBER

2432

DATE MAILED: 06/17/2011

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 709 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 709 day(s).

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

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

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

Privacy Act Statement

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

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

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

Notice of Allowability	Application No.	Applicant(s)	
	10/490,933	VAARALA ET AL.	
	Examiner	Art Unit	
	DEVIN ALMEIDA	2432	

-- 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 3/21/2011.
2. The allowed claim(s) is/are 1-16.
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)

- | | |
|---|--|
| <ol style="list-style-type: none"> 1. <input type="checkbox"/> Notice of References Cited (PTO-892) 2. <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) 3. <input type="checkbox"/> Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____ 4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit of Biological Material | <ol style="list-style-type: none"> 5. <input type="checkbox"/> Notice of Informal Patent Application 6. <input type="checkbox"/> Interview Summary (PTO-413),
Paper No./Mail Date _____. 7. <input type="checkbox"/> Examiner's Amendment/Comment 8. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance 9. <input type="checkbox"/> Other _____. |
|---|--|

/Devin Almeida/
Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432

Allowable Subject Matter

The following is an examiner's statement of reasons for allowance: The arguments presented in the Appeal Brief filed 4/20/2011 are persuasive.

In particular, the argument that the prior art does not teach the second terminal registering the already established second secure connection in combination with the other limitations of the claim. The closest prior art Sturniolo et al 6,091,951 only teaches the seamless roaming where the second device is not involved with the change in connection.

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

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Devin Almeida whose telephone number is 571-270-1018. The examiner can normally be reached on Monday-Thursday from 7:30 A.M. to 5:00 P.M. The examiner can also be reached on alternate Fridays from 7:30 A.M. to 4:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.


Application/Control Number: 10/490,933
Art Unit: 2432

Page 3

Information regarding the status of an application may be obtained from the
Patent Application Information Retrieval (PAIR) system.

/Devin Almeida/
Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432

Search Notes 	Application/Control No. 10490933	Applicant(s)/Patent Under Reexamination VAARALA ET AL.
	Examiner DEVIN ALMEIDA	Art Unit 2432

SEARCHED			
Class	Subclass	Date	Examiner
713	160, 162, 151, 171	6/9/2011	DA

SEARCH NOTES			
Search Notes		Date	Examiner
See east printout		10/8/2008	DA
See east printout		1/5/2010	DA

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner
	Original adj network adj address and second adj terminal and first adj network adj address).clm.(6/13/2011	DA

/DEVIN ALMEIDA/ Examiner.Art Unit 2432	
---	--

EAST Search History**EAST Search History (Prior Art)**

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	717	update with address with new adj address	US- PGPUB; USPAT	OR	ON	2011/06/09 11:15
S2	0	update with address with new adj network adj address	US- PGPUB; USPAT	OR	ON	2011/06/09 11:16
S3	34	update with address with new adj network adj address	US- PGPUB; USPAT	OR	ON	2011/06/09 11:16
S4	9	update with address with new adj network adj address with message	US- PGPUB; USPAT	OR	ON	2011/06/09 11:17
S5	4748	update with address with message	US- PGPUB; USPAT	OR	ON	2011/06/09 11:17
S6	203	update with network adj address with message	US- PGPUB; USPAT	OR	ON	2011/06/09 11:17
S7	1209	update with network adj address	US- PGPUB; USPAT	OR	ON	2011/06/09 11:18
S8	82	update with network adj address and ipsec	US- PGPUB; USPAT	OR	ON	2011/06/09 11:19
S9	668	713/160.ccls.	US- PGPUB; USPAT	OR	ON	2011/06/09 11:20


S10	500	713/162.ccls.	US-PGPUB; USPAT	OR	ON	2011/06/09 11:20
S11	929	713/151.ccls.	US-PGPUB; USPAT	OR	ON	2011/06/09 11:20
S12	1811	713/171.ccls.	US-PGPUB; USPAT	OR	ON	2011/06/09 11:20
S13	1	10/490933	US-PGPUB; USPAT	OR	ON	2011/06/09 11:39
S14	134	"6091951"	US-PGPUB; USPAT	OR	ON	2011/06/09 11:47

EAST Search History (I nterference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	0	(original adj network adj address and second adj terminal and first adj network adj address).clm.	USPAT; UPAD	OR	ON	2011/06/13 08:22

6/ 13/ 2011 8:22:53 AM

**C:\ Documents and Settings\ dalmeida\ My Documents\ EAST\ Workspaces
 \ 10490933new.wsp**

Issue Classification 	Application/Control No. 10490933	Applicant(s)/Patent Under Reexamination VAARALA ET AL.
	Examiner DEVIN ALMEIDA	Art Unit 2432

ORIGINAL						INTERNATIONAL CLASSIFICATION												
CLASS			SUBCLASS			CLAIMED					NON-CLAIMED							
713			160			H	0	4	L	9 / 00 (2006.0)								
CROSS REFERENCE(S)						H	0	4	L	29 / 06 (2006.01.01)								
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)																	
713	162	168																

<input checked="" type="checkbox"/> Claims renumbered in the same order as presented by applicant <input type="checkbox"/> CPA <input type="checkbox"/> T.D. <input type="checkbox"/> R.1.47															
Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1		17												
2	2		18												
3	3														
4	4														
5	5														
6	6														
7	7														
8	8														
9	9														
10	10														
11	11														
12	12														
13	13														
14	14														
15	15														
16	16														

/DEVIN ALMEIDA/ Examiner. Art Unit 2432 (Assistant Examiner)		Total Claims Allowed: 16	
/GILBERTO BARRON JR/ Supervisory Patent Examiner. Art Unit 2432 (Primary Examiner)		06/10/2011 (Date)	O.G. Print Claim(s) 1
			O.G. Print Figure 1



UNITED STATES PATENT AND TRADEMARK OFFICE

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

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
Row 1: 10/490,933, 04/18/2005, Sami Vaarala, 290.1053USN, 2431
Row 2: 7590, 08/08/2011, FASTH LAW OFFICES (ROLF FASTH), EXAMINER ALMEIDA, DEVIN E
Row 3: 26 PINECREST PLAZA, SUITE 2, ART UNIT 2432, PAPER NUMBER
Row 4: SOUTHERN PINES, NC 28387-4301

DATE MAILED: 08/08/2011

PRIORITY ACKNOWLEDGMENT

- 1. Receipt is acknowledged of priority papers submitted under 35 U.S.C. 119. The papers have been placed of record in the file.
2. Applicant's claim for priority, based on papers filed in parent Application Number PCT FJ02 00771 submitted under 35 U.S.C. 119, is acknowledged.
3. The priority papers, submitted _____, after payment of the issue fee are
- acknowledged
- While the priority claim or certified copy filed will be placed in the file record, neither will be reviewed and the patent when published will not include the priority claim. See 37 CFR 1.55(a)(2).
- not acknowledged since the processing fee in 37 CFR 1.17(i) has not been received.
4. For utility and plant applications filed on or after November 29, 2000, the priority claim is not entered because the claim was not presented within the time limit required by 37 CFR 1.55(a)(1). A petition to accept a delayed claim for priority under 35 U.S.C. 119(a) - (d) or (f), or 365(a) may be filed. See 37 CFR 1.55(c) and MPEP 201.14(a).

Midel GERONIMO
For:
571-272-4200 or 1-888-786-0101
Application Assistance Unit
Office of Data Management

PART B - FEE(S) TRANSMITTAL

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

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

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

33369 7590 06/17/2011
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.

<i>Sloan Smith</i>	(Depositor's name)
<i>Sloan Smith</i>	(Signature)
<i>12 September 2011</i>	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/490,933	04/18/2005	Sami Vaarala	290.1053USN	2431

TITLE OF INVENTION: METHOD AND SYSTEM 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	09/19/2011

EXAMINER	ART UNIT	CLASS-SUBCLASS
ALMEIDA, DEVIN E	2432	713-160000

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

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

1 FASTH LAW OFFICES
 2 Rolf Fasth
 3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)
 PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: MOBILITY PATENT HOLDING MPH OY, FINLAND
 (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 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 12 September 2011
 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.

Attorney Ref. No. 290.1053USN

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
In re application of Art Unit 2432
Confirmation No. 2431
Sami Vaarala, Antti
Nuopponen, Panu Pietikainen

CERTIFICATE OF MAILING

Serial No. 10/490,933
Filed: 26 March 2004

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 12 September 2011.

For: METHOD AND SYSTEM FOR
ENSURING SECURE
FORWARDING OF MESSAGES

/rfasth/

Examiner: Devin E. Almeida

Rolf Fasth
Attorney for Applicant

Date: 12 September 2011

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 Ref. No. 290.1053USN

Electronic Patent Application Fee Transmittal

Application Number:	10490933			
Filing Date:	18-Apr-2005			
Title of Invention:	METHOD AND SYSTEM FOR ENSURING SECURE FORWARDING OF MESSAGES			
First Named Inventor/Applicant Name:	Sami Vaarala			
Filer:	Rolf Fasth/Sloan Smith			
Attorney Docket Number:	290.1053USN			
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:	10931555
Application Number:	10490933
International Application Number:	
Confirmation Number:	2431
Title of Invention:	METHOD AND SYSTEM 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:	290.1053USN
Receipt Date:	12-SEP-2011
Filing Date:	18-APR-2005
Time Stamp:	21:46:41
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	7808
Deposit Account	060243
Authorized User	
<p>The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:</p> <ul style="list-style-type: none"> 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	190805 a0627438a8f74ef6632339e12f76ce08627a9c14	no	1

Warnings:

Information:

2	Miscellaneous Incoming Letter	TRX.PDF	66216 34f8b2a78b641cb61d2477abcdf2bbc7b1b77ff7	no	1
---	-------------------------------	---------	---	----	---

Warnings:

Information:

3	Fee Worksheet (SB06)	fee-info.pdf	31736 8881ea24a95ff53f865753a801b447934e1e191	no	2
---	----------------------	--------------	--	----	---

Warnings:

Information:

Total Files Size (in bytes):	288757
-------------------------------------	--------

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/490,933	10/11/2011	8037302	290.1053USN	2431

33369 7590 09/21/2011
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 927 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

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

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

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

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

Sami Vaarala, Espoo, FINLAND;
Antti Nuopponen, Espoo, FINLAND;
Panu Pietikainen, Espoo, FINLAND;

J07700.100-A01

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Sami Vaarala	Confirmation No. 2431
Application No. 10/490,933	Patent No. 8,037,302
Filed: April 18, 2005	Issued: October 11, 2011
For: METHOD AND SYSTEM FOR ENSURING SECURE FORWARDING OF MESSAGES	

LOSS OF ENTITLEMENT TO SMALL ENTITY STATUS

Mail Stop Maintenance Fee
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Honorable Commissioner:

Pursuant to 37 C.F.R. §1.27(g)(2), Patent Owner hereby informs the USPTO that the above-identified patent is no longer eligible for small entity status. Please update the Office records accordingly.

The Office is invited to direct any questions to the undersigned practitioner at the below-listed telephone number.

Respectfully submitted,
Sami Vaarala

/Abe Hershkovitz/

Abraham Hershkovitz
Reg. No. 45,294

April 1, 2015

HERSHKOVITZ & ASSOCIATES, PLLC
2845 Duke Street
Alexandria, VA 22314
Telephone 703-370-4800
Facsimile 703-370-4809

J07700.100-A01; AH/cra