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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
02 June 2022 (02.06.2022)

WIPO | PCT

(10) International Publication Number
WO 2022/112646 A1

(51) International Patent Classification:
H04L 12/46 (2006.01) *H04L 9/40* (2022.01)
H04L 9/08 (2006.01) *H04W 12/03* (2021.01)

(21) International Application Number:
PCT/FI2021/050725

(22) International Filing Date:
27 October 2021 (27.10.2021)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20206200 25 November 2020 (25.11.2020) FI

(71) Applicant: **NOKIA SOLUTIONS AND NETWORKS OY** [FI/FI]; Karakaari 7, 02610 Espoo (FI).

(72) Inventors: **SAMAL, Ashok, Kumar**; Plot No 132 (Ground Floor), BapujiNagar, Lane No 9, Odisha, Dist: Khurda, Bhubaneswar 751009 (IN). **NISHANT, Nishit**; C-203, Monica Apartment, Ambedkarpath, Khajpura, Bailey Road, Bihar, Patna 800014 (IN).

(74) Agent: **NOKIA TECHNOLOGIES OY** et al.; Ari Aarnio, IPR Department, Karakaari 7, 02610 Espoo (FI).

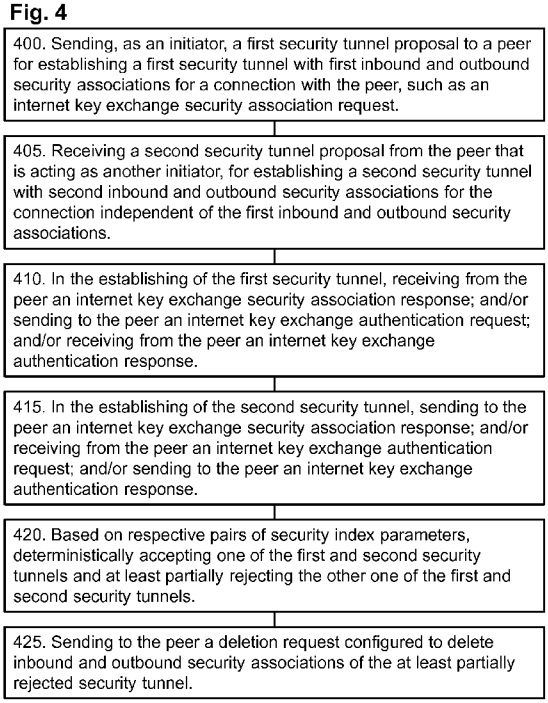
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report (Art. 21(3))*

(54) Title: METHOD AND APPARATUS FOR REDUCING REDUNDANCY OF INTERNET SECURITY

Fig. 4



(57) Abstract: Method, apparatus, computer program and memory medium carrying same, for sending by an apparatus, as an initiator, a first security tunnel proposal to a peer for establishing a first security tunnel with first inbound and outbound security associations for a connection with the peer (400); receiving a second security tunnel proposal from the peer that is acting as another initiator, for establishing a second security tunnel with second inbound and outbound security associations for the connection independent of the first inbound and outbound security associations (405); and based on respective security parameter indexes, deterministically accepting one of the first and second security tunnels (420) and at least partially rejecting the other one of the first and second security tunnels (425).

WO 2022/112646 A1

METHOD AND APPARATUS FOR REDUCING REDUNDANCY OF INTERNET SECURITY

TECHNICAL FIELD

Various example embodiments relate to reducing redundancy of internet security.

BACKGROUND

This section illustrates useful background information without admission of any technique described herein representative of the state of the art.

On the internet, data are exchanged using layered protocols. For internet security, there are protocols such as the Internet Protocol Security (IPsec) running on the network or internet layer and layer 2 transport protocol (L2TP). These protocols enable forming virtual private network (VPN) connections with wide native support of operating systems.

Like many internet protocols, IPsec is based on other protocols, such as internet key exchange (IKE) that is used for performing mutual authentication and establishing and maintaining security associations (SAs) between peers.

The internet communications are exploited in a tremendous scale. Unlike past, most information transferred on the internet is encrypted. Any performance issues in this scale get repeated at such a rate that even minute improvements may have significant effects in total data throughput, energy consumption and session capacity.

SUMMARY

The scope of protection sought for various embodiments of the invention is set out by the independent claims. The embodiments and features, if any, described in this specification that do not fall under the scope of the independent claims are to be interpreted as examples useful for understanding various embodiments of the invention.

According to a first example aspect of the present invention, there is provided an

apparatus, comprising:

at least one memory and processor configured to cause the apparatus to perform at least:

sending, as an initiator, a first security tunnel proposal to a peer for establishing a first security tunnel with first inbound and outbound security associations for a connection with the peer;

receiving a second security tunnel proposal from the peer that is acting as another initiator, for establishing a second security tunnel with second inbound and outbound security associations for the connection independent of the first inbound and outbound security associations; and

based on respective security parameter indexes, deterministically accepting one of the first and second security tunnels and at least partially rejecting the other one of the first and second security tunnels.

The connection may refer to a logical connection over which data can be transferred between the apparatus and the peer. One or more security tunnels may be formed for the connection before rejecting one of the first and second security tunnels.

The inbound security association may refer to a security association used for incoming or ingress traffic of the apparatus. The outbound security association may refer to a security association used for outgoing or egress traffic of the apparatus.

The first security tunnel proposal may be an internet key exchange security association request.

The establishing of the first security tunnel may comprise receiving from the peer an internet key exchange security association response.

The establishing of the first security tunnel may comprise sending to the peer an internet key exchange authentication request.

The establishing of the first security tunnel may comprise receiving from the peer an internet key exchange authentication response.

The second security tunnel proposal may be an internet key exchange security association request.

The establishing of the second security tunnel may comprise sending to the peer an internet key exchange security association response.

The establishing of the second security tunnel may comprise receiving from the peer an internet key exchange authentication request.

The establishing of the second security tunnel may comprise sending to the peer an internet key exchange authentication response.

The establishing of the first security tunnel may temporally overlap with the establishing of the second security tunnel.

The method may comprise sending to the peer a deletion request configured to delete the inbound and outbound security associations of the rejected one of the first and second security tunnels. The method may comprise sending to the peer a deletion request configured to delete the inbound and outbound security associations of the rejected one of the first and second security tunnels only if necessary to enable the peer to delete redundant security associations. The method may comprise sending the deletion request if the peer has not sent the deletion request within a given deletion time. The method may comprise sending the deletion request if the accepted one of the first and second security tunnels is the one for which the establishing of the security tunnel has completed first. The method may comprise sending the deletion request if the accepted one of the first and second security tunnels is the one for which the establishing of the security tunnel has completed last. The method may comprise sending the deletion request if the apparatus is configured to support removal of a redundant security tunnel on creation of the connection. The method may comprise waiting for a random period and not sending the deletion request if a deletion request is received in the meanwhile from the peer.

Alternatively, both peers may locally delete the rejected one of the first and second security tunnels without either peer notifying the other one, when the remaining one of the security tunnels will remain. The apparatus may locally delete the rejected one of the first and second security tunnels without notifying the peer if the peer has indicated support for implied deletion of the redundant security tunnel. The support for implied deletion may be indicated by an internet key exchange message received from the peer. The apparatus may keep count of local deletions of the security tunnel and only once for one peer perform the local deletion within a given period of time. The given period of time may be at least 5 ms; 10 ms; 20 ms; 50 ms; 100 ms; 1 s; 2 s; 10 s; 30 s; 1 min. The given period of time may be at most 10 ms; 20 ms; 50 ms; 100 ms; 1 s; 2 s; 10 s; 30 s; 1 min; or 2 min.

The first inbound and outbound security associations may be child security associations resulting from a first security association request. The second inbound and outbound security associations may be child security associations resulting from a second security association request. The first inbound and outbound security associations may be internet key exchange security associations. The second inbound and outbound security associations may be internet key exchange associations. The first security association request may be sent by one of the apparatus and the peer and the second security association request may be sent by the remaining one of the apparatus and the peer. The first security association request may be sent before or after the second security association request. The first security association request may be sent by one of the apparatus and the peer and the second security association request may be sent by the remaining one of the apparatus and the peer. The first security association request may be sent before or after the second security association request.

The partial rejecting of a security tunnel may refer to deleting a portion of security associations of the security tunnel. The portion of security associations may comprise one or more child security associations.

The deterministic accepting may comprise combining security parameter indexes of inbound and outbound security associations to a combination for each of the first and

second security tunnels, respectively. The deterministic accepting may comprise comparing the combinations according to a predefined rule. The combining may comprise or be summing. The combining may comprise or be string concatenation. The predefined rule may be accepting first one in an ascending order. The predefined rule may be accepting first one in a descending order. The order may be numeric order. The order may be alphabetic order.

According to a second example aspect of the present invention, there is provided a method in an apparatus, comprising:

sending, as an initiator, a first security tunnel proposal to a peer for establishing a first security tunnel with first inbound and outbound security associations for a connection with the peer;

receiving a second security tunnel proposal from the peer that is acting as another initiator, for establishing a second security tunnel with second inbound and outbound security associations for the connection independent of the first inbound and outbound security associations; and

based on respective security parameter indexes, deterministically accepting one of the first and second security tunnels and at least partially rejecting the other one of the first and second security tunnels.

According to a third example aspect of the present invention, there is provided a computer program comprising computer executable program code configured to execute the method of the second example aspect.

The computer program may be stored in a computer readable memory medium.

Any foregoing memory medium may comprise a digital data storage such as a data disc or diskette, optical storage, magnetic storage, holographic storage, opto-magnetic storage, phase-change memory, resistive random access memory, magnetic random access memory, solid-electrolyte memory, ferroelectric random access memory, organic memory or polymer memory. The memory medium may be formed into a device without other substantial functions than storing memory or it may be formed as part of a device with other functions, including but not limited to a memory of a

computer, a chip set, and a sub assembly of an electronic device.

According to a fourth example aspect of the present invention, there is provided an apparatus comprising means for performing the method of the second example aspect.

Different non-binding example aspects and embodiments of the present invention have been illustrated in the foregoing. The embodiments in the foregoing are used merely to explain selected aspects or steps that may be utilized in implementations of the present invention. Some embodiments may be presented only with reference to certain example aspects of the invention. It should be appreciated that corresponding embodiments may apply to other example aspects as well.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of example embodiments of the present invention, reference is now made to the following descriptions taken in connection with the accompanying drawings in which:

Fig. 1 shows an architectural drawing of a system of an example embodiment;

Fig. 2 shows a signalling chart of a first process of an example embodiment;

Fig. 3 shows a signalling chart of a second process of an example embodiment;

Fig. 4 shows a flow chart of a process of an example embodiment;

Fig. 5 shows a flow chart of a process of an example embodiment; and

Fig. 6 shows a block diagram of an apparatus of an example embodiment.

DETAILED DESCRIPTON OF THE DRAWINGS

An example embodiment of the present invention and its potential advantages are understood by referring to Figs. 1 through 6 of the drawings. In this document, like reference signs denote like parts or steps.

Fig. 1 shows an architectural drawing of a system 100 of an example embodiment. The system 100 comprises an apparatus 110 and a peer 120. Fig. 1 further shows a data communication network 130 comprising one or more networks which enable communication between the apparatus 110 and the peer 120 using internet protocols

such as L2TP/IPsec.

The apparatus 110 is referred to as apparatus without intention to imply any particular nature. The apparatus 110 can be a mobile phone, a tablet computer, an Internet of Things device, a personal computer, a Linux server, a Windows® server, a network element such as firewall, router, switch, gateway, security gateway, or service function. Same applies to the peer 120.

In example embodiment, customer network topologies configure both peers as Initiators to facilitate load balancing. In such cases, parallel security tunnels may however result with different inbound and outbound security associations (SAs), while the peer uses only one SA at a time. The other redundant SA pair or security tunnel may then in vain occupy IPsec SA resources.

Fig. 2 shows a signalling chart of a first process of an example embodiment. Fig. 2 indicates one example of normal exchange of signals when two peers (apparatus and peer) both operate as initiators for forming a security tunnel so ultimately forming two security tunnels in parallel. In this case, one security tunnel is completed before another one is formed.

Fig. 2 shows 200. sending a first security association initiation request from an apparatus to a peer, such as an internet key exchange security association initiation request, IKE_SA_INIT request. This initiation request may represent a first security association proposal belonging to a first security tunnel forming process A. Signals relating to this first security tunnel process are labelled in Fig. 3 with “A:”

Fig. 2 further shows 205. receiving by the apparatus a first security association response from the peer, such as an IKE_SA_INIT response.

Fig. 2 further shows 210. sending a first security association authentication request from the apparatus to the peer, such as an internet key exchange security association authentication request, IKE_AUTH request.

Fig. 2 further shows 215. receiving by the apparatus a first security association authentication response from the peer, such as an internet key exchange security association authentication response IKE_AUTH response.

Fig. 2 further shows 220. sending a second security association initiation request from the peer to the apparatus, such as an internet key exchange security association initiation request, IKE_SA_INIT request. This initiation request may represent a second security association proposal belonging to a second security tunnel forming process B. Signals relating to this second security tunnel process are labelled in Fig. 3 with “B:”

Fig. 2 further shows 225. receiving by the peer a security association response from the apparatus, such as an IKE_SA_INIT response.

Fig. 2 further shows 230. sending a second security association authentication request from the peer to the apparatus, such as an internet key exchange security association authentication request, IKE_AUTH request.

Fig. 2 further shows 235. receiving by the peer a security authentication response from the apparatus, such as an internet key exchange security association authentication response, IKE_AUTH response.

After completion of forming both the first and second security tunnels, there are first inbound and outbound security associations formed for the apparatus and peer based on the first security tunnel proposal initiated by the apparatus. Concurrently, there are also second inbound and outbound security associations formed for the apparatus and peer based on the second security tunnel proposal initiated by the peer.

The first inbound security association of the apparatus is correspondingly an outbound security association at the peer. Likewise, the first inbound security association of the peer is correspondingly an outbound security association at the apparatus. Each security association is represented by a common security parameter index, SPI, at both ends (the apparatus and peer). Each security tunnel may comprise inbound and

outbound IKE security associations and child security associations, each represented by a corresponding security parameter index. Both ends may have four security parameter indexes for the first security tunnel and four security parameter indexes for the second security tunnel. Both ends may have same SPIs for each security association so that there are four different SPIs for one security tunnel, two of which SPIs being parent or IKE security associations and other two being child security associations.

In result of Fig. 2 process, there are two bi-directional security tunnels created one after another (one SA pair created by a first message sequence denoted by A: and a second message sequence denoted by B:). Ideally, both ends use same child SA pair for inbound and outbound traffic as usually obtained by the latest one, and it is easy to identify the redundant SA. In Fig. 2, SA initiated by a second message sequence (B:) i.e., a child SPI pair such as <0xc8cf556a,0xc1619f09> will be used for both peers since it's the latest SA and the SA initiated by a first message sequence (A:) i.e., a child SPI pair such as <0xcc8271c9, 0xc4ee5061> will be redundant SA. It is to be appreciated that alternatively or additionally the parent or IKE security associations are used in some example embodiments to mutually identify one of plural concurrent security tunnels for removal of redundancy.

Fig. 2 further shows 240. determining (e.g., at both the apparatus and the peer) whether there is security association redundancy. If security association redundancy is determined, then an information message is sent to the other end to instruct of deleting determined redundant security associations. Also the determined redundant associations are deleted when determined so these redundant security associations will be deleted already on forming the security tunnel at both ends. The redundant security associations include in an example embodiment IKE and child security associations of the redundant security tunnel.

There are various implementations that will be further discussed in connection with flow chart shown in Fig. 4. First, let us yet turn into Fig.3 to review another scenario in which the forming of the two security tunnels become intertwined. This may happen, for example, due to varying delays in data transmission, e.g., if routing of some packets

changes or some other delay occurs, such as renewing a DHCP lease.

Fig. 3 shows a signalling chart of a second process of an example embodiment. The second process corresponds to the first process except for the order of some signals and events. Here, the apparatus receives 215 the first security association authentication response from the peer after the second security tunnel has already been established. Also the determination and deletion of security association redundancy is postponed until completion of the incomplete first security tunnel by the receiving 215 of the first security association authentication response.

In case of Fig. 2, the first security tunnel is first complete and then the second security tunnel is completed. The apparatus would use the second security tunnel which is the latest and would not use the first security tunnel at all. In case of Fig. 3, the forming of the first security tunnel is partly completed, i.e., an outbound security association gets established for the apparatus, while the inbound security association of that connection is formed only after the second security tunnel is completed with its inbound and outbound secure associations. Hence, the apparatus would normally use after the second process in part the first security tunnel (outbound direction) and in part the second security tunnel (inbound direction) and 50 % of the formed security associations should be maintained while they are redundant.

In Fig. 3, the SPI <0xc8cf556a> from a child SA negotiated by a second message sequence (B:) will be used for outbound traffic by the peer. An example SPI <0xc4ee5061> is used for outbound traffic by the apparatus from child SA negotiated by the first message sequence (A:). Similarly, the peer uses an SPI <0xc4ee5061> while the apparatus uses SPI <0xc8cf556a> for inbound traffic, i.e., SPIs of two different SAs.

Normally, this would result in some technical problems:

- In case there are two security tunnels and both peers use different security tunnels for communication, the system must maintain both security tunnels even if the communication could have proceeded by using a single security tunnel. It cannot delete one of the security tunnels during rekey as per the

standard implementation either the inbound or outbound security association will be in use but not both of same security tunnel, as two security tunnels are taken into use. Even in normal message sequence each of the security associations must be maintained for their rekey lifetimes. So, in any case this results in unnecessary resource consumption and affects system performance.

- When the peer uses security associations of different security tunnels, one node can err to delete the security associations of another security tunnel assuming that as inactive if there is unidirectional traffic (e.g., in case of predominantly downlink traffic) for the entire rekey lifetime. It will delete the idle security association (or associations, when taking into account both IKE and child SAs) under the assumption that no traffic is flowing though that security association and in doing so will delete the security association from the peer as well. When the peer decides to send uplink traffic it will have to form and switch to using a new security association for the uplink traffic (so forming new IKE and child SAs). Since there is no standard recommendation as to when to switch between security associations, different implementations can do this at different times leading to potential temporary traffic disruptions until both nodes start using the same security association. Traffic loss may result until a new security association is created.
- There is no universal manner to identify a redundant security tunnel since SPIs of both security tunnels are in use and there is no difference in the roles of the peers: both are initiators for one security association. So, both peers must keep security associations of both security tunnels for inbound direction. Both peers may also use different security associations for the outbound traffic from two different security tunnels.

Let us next discuss in further detail how the redundancy in security associations is addressed by some example embodiments of this document.

Fig. 4 shows a flow chart of a process of an example embodiment. The process comprises 400. Sending, as an initiator, a first security tunnel proposal to a peer for establishing first inbound and outbound security associations for a connection with the peer, such as an internet key exchange security association request.

Fig 4 further shows 405. Receiving a second security tunnel proposal from the peer that is acting as another initiator, for establishing a second security tunnel with second inbound and outbound security associations for the connection independent of the first inbound and outbound security associations. In an example embodiment, the second security tunnel proposal is an internet key exchange security association request.

Fig 4 further shows 410. In the establishing of the first security tunnel, receiving from the peer an internet key exchange security association response; and/or sending to the peer an internet key exchange authentication request; and/or receiving from the peer an internet key exchange authentication response.

Fig 4 further shows 415. In the establishing of the second security tunnel, sending to the peer an internet key exchange security association response; and/or receiving from the peer an internet key exchange authentication request; and/or sending to the peer an internet key exchange authentication response.

The establishing of the first security tunnel may temporally overlap with the establishing of the second security tunnel.

Fig 4 further shows 420. Based on respective pairs of security parameter indexes, deterministically accepting one of the first and second security tunnels and at least partially rejecting the other one of the first and second security tunnels. In an example embodiment, the pairs of security parameter indexes are obtained from any of the security association initialisation or authentication messages. In an example embodiment, the pairs of security parameter indexes are obtained from the internet key exchange security association authentication request and response messages. In an example embodiment, the deterministic accepting uses additional information on top of the respective pairs of security parameter indexes. For example, security parameter indexes may be used related to both the internet key exchange security associations and the child security associations so that there are four security parameter indexes used for the deterministic accepting.

Fig 4 further shows 425. Sending to the peer a deletion request configured to delete at least some or all security associations of the at least partially rejected security tunnel. By sending the deletion request to the peer, the apparatus may cause the peer to delete redundant security associations regardless of whether the peer itself is capable to determining the redundant security associations. The deletion request may be directed to the inbound and outbound internet key exchange security associations of the redundant security tunnel for deleting both the IKE SAs and related child SAs at the peer. This may be the case even if the deterministic accepting of one security tunnel were performed using the SPIs of the child SAs. Alternatively, the deletion request may be directed to only the inbound and outbound child security associations, in which case the IKE SAs may be left alive. In an example embodiment, the deletion request may be formed using the SPIs of the child SAs and still interpreted as a deletion request for the entire security tunnel including the IKE SAs.

In an example embodiment, sending the deletion request is performed if the peer has not sent the deletion request within a given deletion time. The process comprises in an example embodiment sending the deletion request if the accepted one of the first and second security tunnels is the one for which the establishing of the security tunnel has completed first. In an embodiment, the process comprises sending the deletion request if the accepted one of the first and second security tunnels is the one for which the establishing of the (IKE or child) inbound and outbound security associations has completed last. In an example embodiment, the process comprises waiting for a random period and not sending the deletion request if a deletion request is received in the meanwhile from the peer. In an embodiment, the apparatus attempts to deterministically determine whether the apparatus or the peer is responsible for sending the deletion request. The deterministic determination may be performed by comparing identifiers such as internet addresses of the apparatus and the peer based on a predetermined rule, such as ascending or descending numeric order of numeric parts of the internet addresses or an alphabetic order of the identifiers. The deterministic determination may be based on the deterministic accepting so that the initiator or recipient of the accepted or at least partially rejected security tunnel proposal is selected.

In an example embodiment, the apparatus and the peer locally delete the at least partially rejected one of the first and second security tunnels without notifying each other. In an example embodiment, the apparatus locally deletes at least partially the rejected one of the first and second security tunnels without notifying the peer if the peer has indicated support for implied deletion of redundant security associations. In an example embodiment, the support for implied deletion is indicated by an internet key exchange message received from the peer. In an example embodiment, the apparatus keeps count of local deletions of security associations and only once for one peer perform the local deletion within a given period of time. In an example embodiment, if the apparatus detects subsequent traffic from the peer based on the security association that was determined by the apparatus to be redundant, the apparatus falls back into sending the deletion request. In an example embodiment, the given period of time is at least 5 ms; 10 ms; 20 ms; 50 ms; 100 ms; 1 s; 2 s; 10 s; 30 s; 1 min. In an example embodiment, the given period of time is at most 10 ms; 20 ms; 50 ms; 100 ms; 1 s; 2 s; 10 s; 30 s; 1 min; or 2 min.

In an example embodiment, the first inbound and outbound security associations are child security associations resulting from a first security association request. In an example embodiment, the second inbound and outbound security associations are child security associations resulting from a second security association request. In an example embodiment, the first inbound and outbound security associations are parent or internet key exchange security associations. In an example embodiment, the second inbound and outbound security associations are parent or internet key exchange associations. In an example embodiment, the first security association request is sent by one of the apparatus and the peer and the second security association request may be sent by the remaining one of the apparatus and the peer. In an example embodiment, the first security association request is sent before or after the second security association request.

In an example embodiment, the deterministic accepting comprises combining security parameter indexes of inbound and outbound security associations to a combination for each of the first and second security tunnels, respectively. For example, the comparison may be based on the inbound IKE SA; and outbound IKE SA; on inbound

child SA; and outbound child SA; or on inbound IKE SA; outbound IKE SA; inbound child SA; and outbound child SA. In an example embodiment, the deterministic accepting comprises comparing the combinations according to a predefined rule. In an example embodiment, the combining comprises or is summing. In an example embodiment, the combining comprises or is a string concatenation. In an example embodiment, the predefined rule is accepting first one in an ascending order. In an example embodiment, the predefined rule is accepting first one in a descending order. In an example embodiment, the order is a numeric or alphabetic order.

Fig. 5 shows a flow chart of a process of an example embodiment, comprising:
500. Forming a child SA initiated from apparatus with an outbound SPI for secure outbound communication with the peer;
505. Receiving a child SA response from the peer with an inbound SPI for secure inbound communication with the peer as intended by the peer;
510. Checking if both inbound and outbound SAs are already present for a current security policy (connection number, guiding rules for the traffic etc.) with the peer;
515. Deterministically selecting one of new and old SPIs to keep, and accordingly proceeding to step 520 for keeping old or 525 to adopting new one;
520. Continuing to use the old SA, deleting new SA (optionally sending a deletion message), and returning to step 500;
525. Adopting the new SA and deleting the old one;
530. Sending (in some embodiments) to the peer a deletion message for the old SA;
535. Adopting the new SA;
540. In case the checking in 510 was negative, 540. adding the new SA and continuing to 535.

Fig. 6 shows a block diagram of an apparatus of an example embodiment. The apparatus 600 comprises a memory 640 including a persistent computer program code 646. The apparatus 600 further comprises a processor 620 for controlling the operation of the apparatus 600 using the computer program code 640, a communication unit 610 for communicating with other nodes. The communication unit 610 comprises, for example, a local area network (LAN) port; a wireless local area network (WLAN) unit; Bluetooth unit; cellular data communication unit; or satellite data

communication unit. The processor 620 comprises, for example, any one or more of: a master control unit (MCU); a microprocessor; a digital signal processor (DSP); an application specific integrated circuit (ASIC); a field programmable gate array; and a microcontroller.

As used in this application, the term "circuitry" may refer to one or more or all of the following:

(a) hardware-only circuit implementations (such as implementations in only analog and/or digital circuitry) and;

(b) combinations of hardware circuits and software, such as (as applicable):

(i) a combination of analog and/or digital hardware circuit(s) with software/firmware; and

(ii) any portions of hardware processor(s) with software (including digital signal processor(s)), software, and memory(ies) that work together to cause an apparatus, such as a mobile phone or server, to perform various functions); and

(c) hardware circuit(s) and or processor(s), such as a microprocessor(s) or a portion of a microprocessor(s), that requires software (e.g., firmware) for operation, but the software may not be present when it is not needed for operation.

This definition of circuitry applies to all uses of this term in this application, including in any claims. As a further example, as used in this application, the term circuitry also covers an implementation of merely a hardware circuit or processor (or multiple processors) or portion of a hardware circuit or processor and its (or their) accompanying software and/or firmware. The term circuitry also covers, for example and if applicable to the particular claim element, a baseband integrated circuit or processor integrated circuit for a mobile device or a similar integrated circuit in server, a cellular network device, or other computing or network device.

Without in any way limiting the scope, interpretation, or application of the claims appearing below, a technical effect of one or more of the example embodiments disclosed herein is that redundant security associations may be deleted without waiting until next rekeying. Another technical effect of one or more of the example

embodiments disclosed herein is that connection capacity of security association count restricted network devices may be increased. Yet another technical effect of one or more of the example embodiments disclosed herein is that redundant connections with an apparatus with a peer that lacks support for detecting and deleting redundant security associations on forming connections.

Embodiments of the present invention may be implemented in software, hardware, application logic or a combination of software, hardware, and application logic. The software, application logic and/or hardware may reside on the apparatus or peer. In an example embodiment, the application logic, software, or an instruction set is maintained on any one of various conventional computer-readable media. In the context of this document, a "computer-readable medium" may be any non-transitory media or means that can contain, store, communicate, propagate, or transport the instructions for use by or in connection with an instruction execution system, apparatus, or device, such as a computer, with one example of a computer described and depicted in Fig. 6. A computer-readable medium may comprise a computer-readable storage medium that may be any media or means that can contain or store the instructions for use by or in connection with an instruction execution system, apparatus, or device, such as a computer.

If desired, the different functions discussed herein may be performed in a different order and/or concurrently with each other. Furthermore, if desired, one or more of the before-described functions may be optional or may be combined.

Although various aspects of the invention are set out in the independent claims, other aspects of the invention comprise other combinations of features from the described embodiments and/or the dependent claims with the features of the independent claims, and not solely the combinations explicitly set out in the claims.

It is also noted herein that while the foregoing describes example embodiments of the invention, these descriptions should not be viewed in a limiting sense. Rather, there are several variations and modifications which may be made without departing from the scope of the present invention as defined in the appended claims. Moreover,

example embodiments of the invention can be used in parallel or alternatively so that in some circumstances, parallel security tunnels are formed. For example, quality of service related needs may benefit from parallel security associations in which case there may be two or more security associations for one direction between the apparatus and peer. It is also possible to use some example embodiments to remove redundant further security tunnels in case that N security associations are needed for one pair of peers and N+1 unidirectional security associations are formed.

CLAIMS

1. An apparatus, comprising:

at least one memory and processor configured to cause the apparatus to perform at least:

sending, as an initiator, a first security tunnel proposal to a peer for establishing first inbound and outbound security associations for a connection with the peer;

receiving a second security tunnel proposal from the peer that is acting as another initiator, for establishing second inbound and outbound security associations for the connection independent of the first inbound and outbound security associations; and

based on respective security parameter indexes, deterministically accepting one of the first and second security tunnels and at least partially rejecting the other one of the first and second security tunnels.

2. The apparatus of claim 1, wherein the first security tunnel proposal is an internet key exchange security association request and the establishing of the first security tunnel comprises receiving from the peer an internet key exchange security association response.

3. The apparatus of claim 1 or 2, wherein the second security tunnel proposal is an internet key exchange security association request and the establishing of the second security tunnel comprises sending to the peer an internet key exchange security association response.

4. The apparatus of any one of preceding claims, wherein the at least one memory and processor are further configured to cause the apparatus to perform at least sending to the peer a deletion request configured to delete the at least partially rejected one of the first and second security tunnels.

5. The apparatus of claim 4, wherein the at least one memory and processor are further configured to cause the apparatus to perform at least sending the deletion request only if necessary to enable the peer to delete redundant security associations.

6. The apparatus of any one of preceding claims, wherein the deterministic

accepting comprises combining security parameter indexes of inbound and outbound security associations to a combination for each of the first and second security tunnels, respectively.

7. The apparatus of claim 6, wherein the deterministic accepting comprises comparing the combination according to a predefined rule.

8. A method in an apparatus, comprising:

sending, as an initiator, a first security tunnel proposal to a peer for establishing a first security tunnel with first inbound and outbound security associations for a connection with the peer;

receiving a second security tunnel proposal from the peer that is acting as another initiator, for establishing a second security tunnel with second inbound and outbound security associations for the connection independent of the first inbound and outbound security associations; and

based on respective security parameter indexes, deterministically accepting one of the first and second security tunnels and at least partially rejecting the other one of the first and second security tunnels.

9. The method of claim 8, wherein the first security tunnel proposal is an internet key exchange security association request; and the establishing of the first inbound and outbound security associations may comprise receiving from the peer an internet key exchange security association response.

10. The method of claim 8 or 9, further comprising sending to the peer a deletion request configured to delete inbound and outbound security associations of the at least partially rejected security tunnel.

11. The method of claim 8 or 9, further comprising sending to the peer a deletion request configured to delete inbound and outbound security associations of the at least partially rejected security tunnel only if necessary to enable the peer to delete redundant security associations.

12. The method of any one of claims 8 to 11, wherein the deterministic accepting

comprises combining security parameter indexes of inbound and outbound security associations to a combination for each of the first and security tunnels, respectively.

13. The method of claim 12, wherein deterministic accepting comprises comparing the combinations according to a predefined rule.

14. A computer program comprising computer executable program code configured to execute the method of any one of claims 8 to 13.

15. A computer-readable medium encoded with instructions that, when executed by a computer, perform:

sending, as an initiator, a first security tunnel proposal to a peer for establishing a first security tunnel with first inbound and outbound security associations for a connection with the peer;

receiving a second security tunnel proposal from the peer that is acting as another initiator, for establishing a second security tunnel with second inbound and outbound security associations for the connection independent of the first inbound and outbound security associations; and

based on respective security parameter indexes, deterministically accepting one of the first and second security tunnels and at least partially rejecting the other one of the first and second security tunnels.

Fig. 1

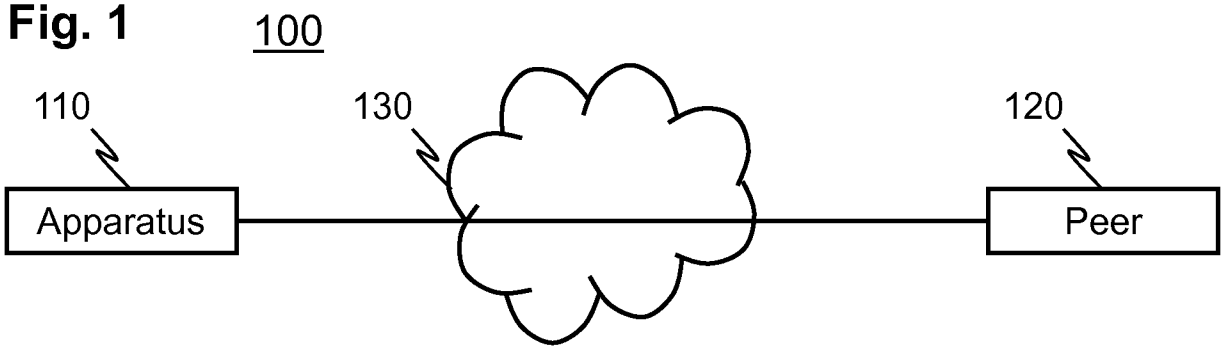

100
110
130
120
Apparatus
Peer

Fig. 2

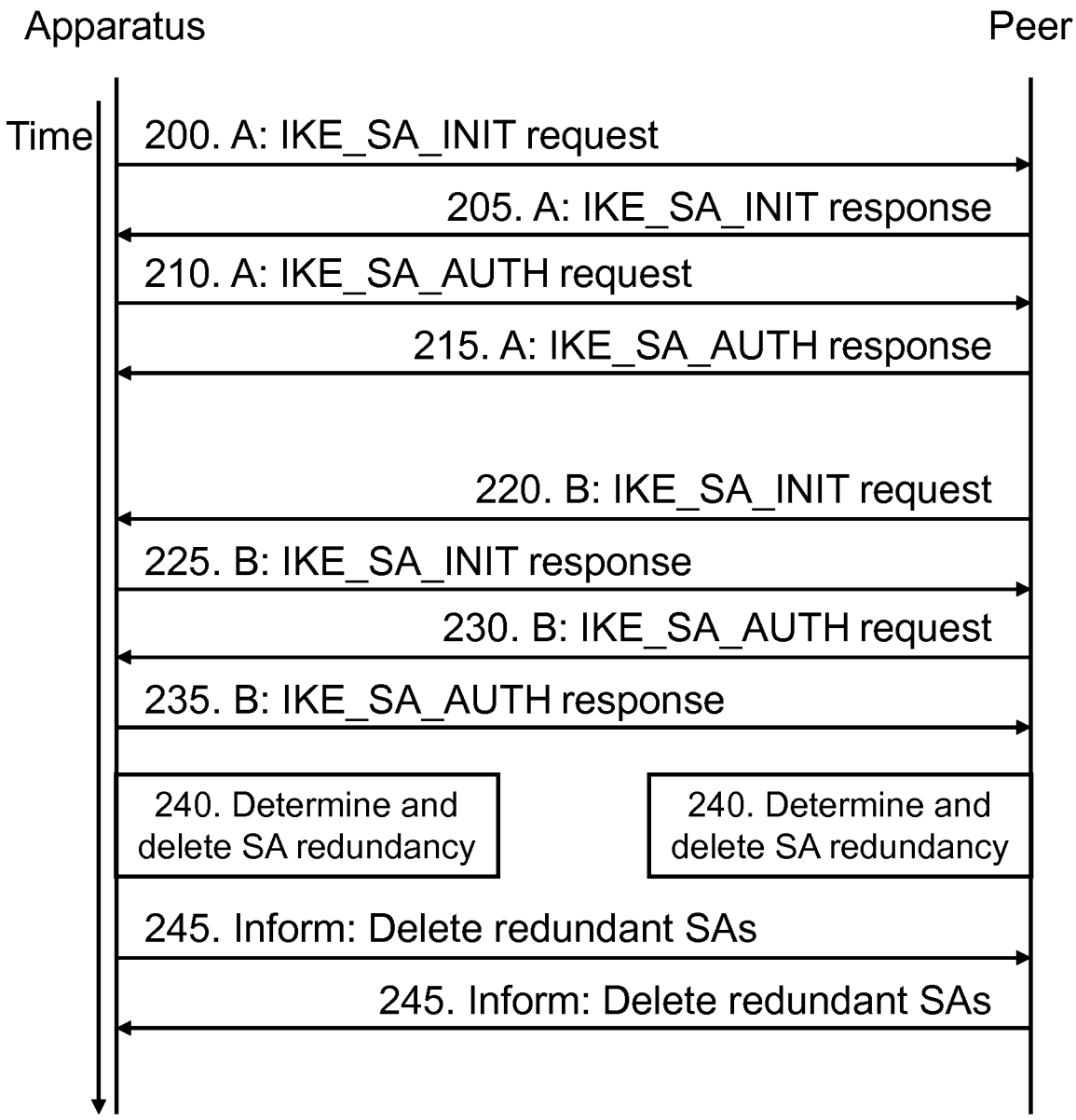

Apparatus
Peer
Time
200. A: IKE_SA_INIT request
205. A: IKE_SA_INIT response
210. A: IKE_SA_AUTH request
215. A: IKE_SA_AUTH response
220. B: IKE_SA_INIT request
225. B: IKE_SA_INIT response
230. B: IKE_SA_AUTH request
235. B: IKE_SA_AUTH response
240. Determine and delete SA redundancy
240. Determine and delete SA redundancy
245. Inform: Delete redundant SAs
245. Inform: Delete redundant SAs

Fig. 3

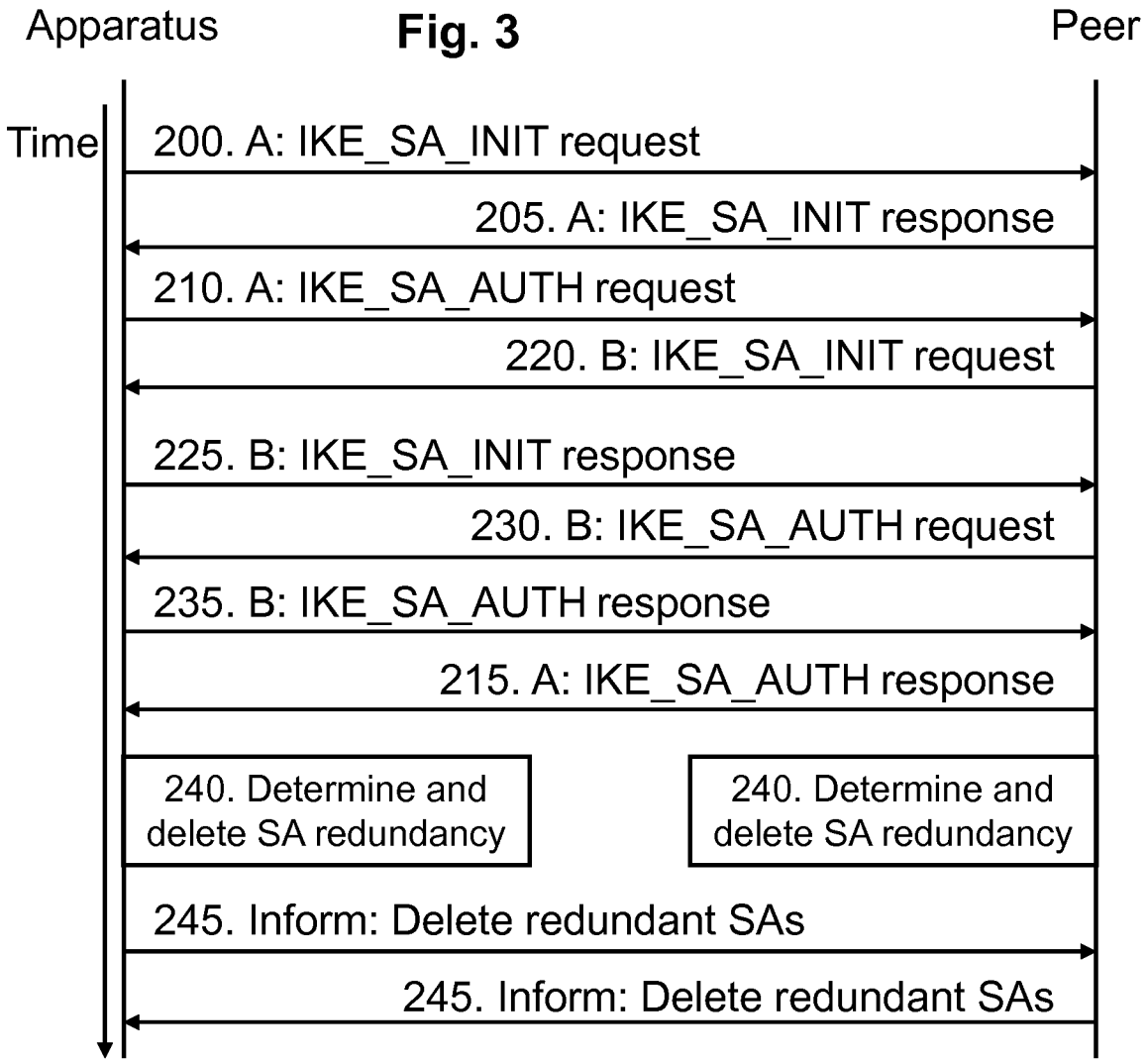

Apparatus
Peer
Time
200. A: IKE_SA_INIT request
205. A: IKE_SA_INIT response
210. A: IKE_SA_AUTH request
220. B: IKE_SA_INIT request
225. B: IKE_SA_INIT response
230. B: IKE_SA_AUTH request
235. B: IKE_SA_AUTH response
215. A: IKE_SA_AUTH response
240. Determine and delete SA redundancy
240. Determine and delete SA redundancy
245. Inform: Delete redundant SAs
245. Inform: Delete redundant SAs

Fig. 6

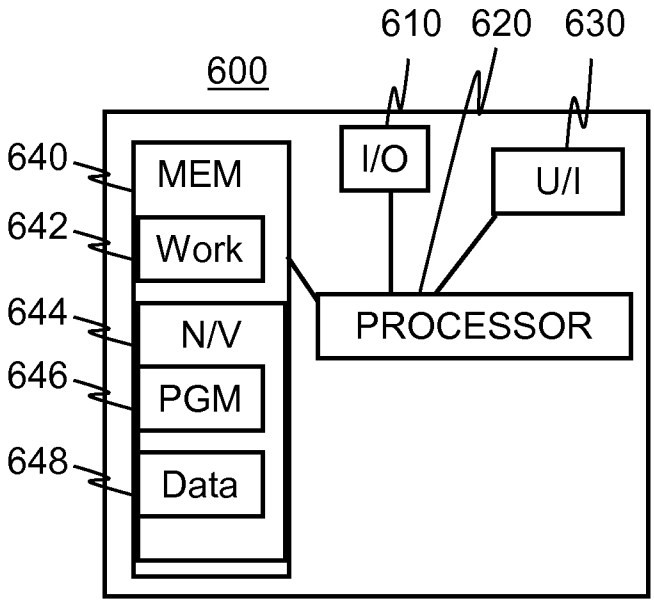

610
620
630
600
640
MEM
642
Work
644
N/V
646
PGM
648
Data
I/O
U/I
PROCESSOR

Fig. 4

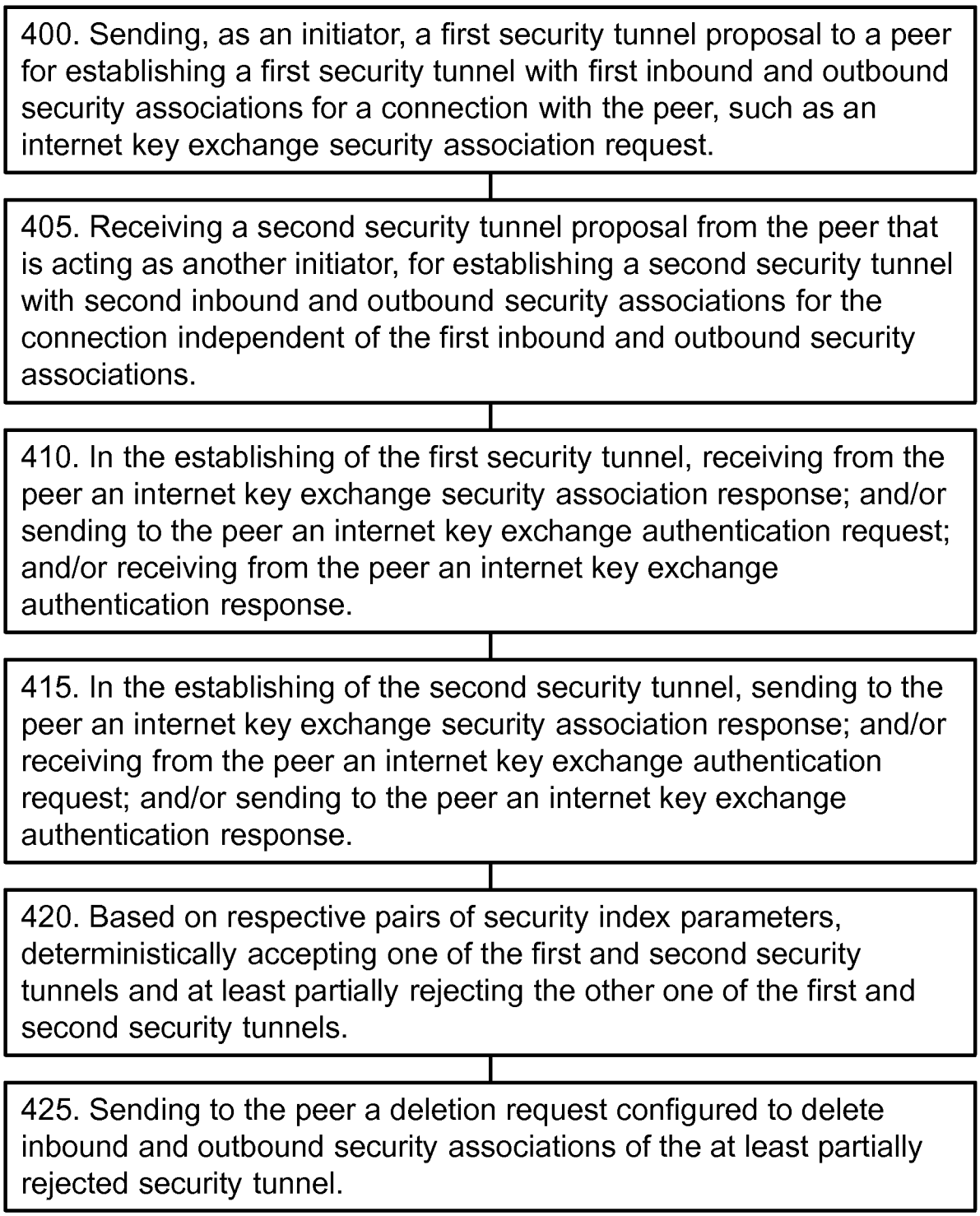
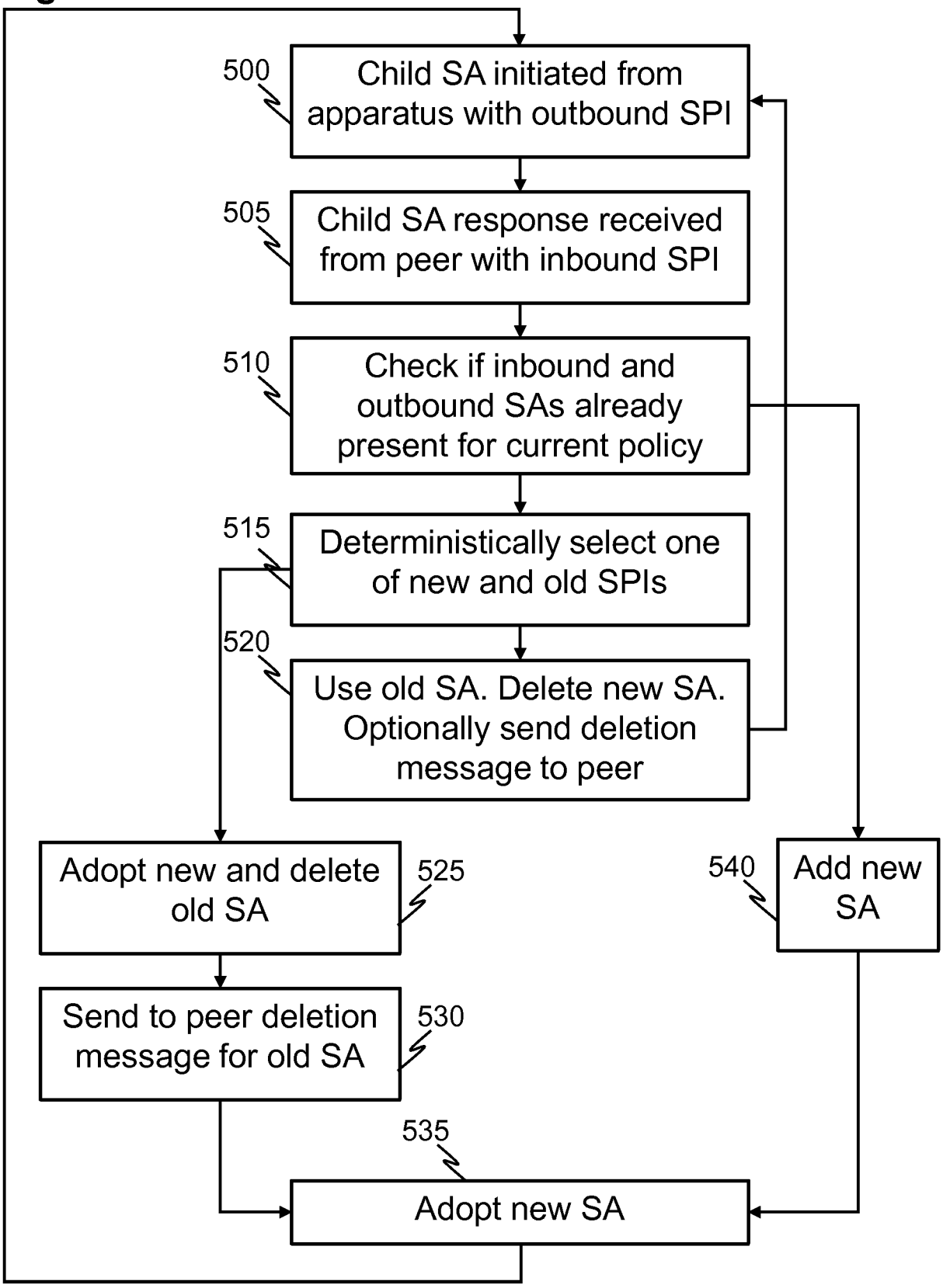

400. Sending, as an initiator, a first security tunnel proposal to a peer for establishing a first security tunnel with first inbound and outbound security associations for a connection with the peer, such as an internet key exchange security association request.
405. Receiving a second security tunnel proposal from the peer that is acting as another initiator, for establishing a second security tunnel with second inbound and outbound security associations for the connection independent of the first inbound and outbound security associations.
410. In the establishing of the first security tunnel, receiving from the peer an internet key exchange security association response; and/or sending to the peer an internet key exchange authentication request; and/or receiving from the peer an internet key exchange authentication response.
415. In the establishing of the second security tunnel, sending to the peer an internet key exchange security association response; and/or receiving from the peer an internet key exchange authentication request; and/or sending to the peer an internet key exchange authentication response.
420. Based on respective pairs of security index parameters, deterministically accepting one of the first and second security tunnels and at least partially rejecting the other one of the first and second security tunnels.
425. Sending to the peer a deletion request configured to delete inbound and outbound security associations of the at least partially rejected security tunnel.

Fig. 5


500
Child SA initiated from apparatus with outbound SPI
505
Child SA response received from peer with inbound SPI
510
Check if inbound and outbound SAs already present for current policy
515
Deterministically select one of new and old SPIs
520
Use old SA. Delete new SA. Optionally send deletion message to peer
Adopt new and delete old SA
525
Send to peer deletion message for old SA
530
540
Add new SA
535
Adopt new SA

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2021/050725

A. **CLASSIFICATION OF SUBJECT MATTER**

See extra sheet

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: H04L, H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

FI, SE, NO, DK

Electronic data base consulted during the international search (name of data base, and, where practicable, search terms used)

EPO-Internal full-text databases, Full-text translation databases from Asian languages, XP3GPP, XPAIP, XPCPVO, XPESP, XPETSI, XPI3E, XPI3ES, XPIEE, XPIETF, XPIOP, XPIPCOM, XPJPEG, XPMISC, XPOAC, XPRD, XPSPRNG, XPTK, COMPDX, INSPEC, TDB, PRH-Internal, ACM, Springer, IPRally

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 3605976 A1 (HUAWEI TECH CO LTD [CN]) 05 February 2020 (05.02.2020) the whole document, in particular, Figs. 2-3, 5A; paragraphs [0034]-[0038], [0054]-[0081]	1-15
X	EP 2093975 A1 (FUJITSU LTD [JP]) 26 August 2009 (26.08.2009) the whole document, in particular, Figs. 1, 9, 12; paragraphs [0050], [0114]-[0116], [0128]-[0130]	1, 8, 14-15
X	US 10516652 B1 (HASHMI OMER [US] et al.) 24 December 2019 (24.12.2019) the whole document, in particular, Figs. 4-6; column 6, lines 11-15; column 11, line 18 – column 12, line 49; column 12, line 62 – column 13, line 53	1, 8, 14-15

☒ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

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

"D" document cited by the applicant in the international application

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 January 2022 (18.01.2022)	19 January 2022 (19.01.2022)

Name and mailing address of the ISA/FI
Finnish Patent and Registration Office
FI-00091 PRH, FINLAND
Facsimile No. +358 29 509 5328

Authorized officer
Yrjö Raivio
Telephone No. +358 29 509 5000

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2021/050725

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 102271061 A (HANGZHOU H3C TECHNOLOGIES CO., LTD) 07 December 2011 (07.12.2011) Figs. 1-2, 4 & abstract [online] EPO & machine translation into English by the EPO [online] [retrieved on 2022-01-14] the whole document, in particular, page 1, lines 27-36; page 3, lines 9-17; page 4, line 25 – page 5, line 22	1, 8, 14-15
A	KAUFMAN, C. et al. RFC 7296. Internet Key Exchange Protocol Version 2 (IKEv2). IETF, [online], October 2014, ISSN 2070-1721, [retrieved on 2022-01-13]. Retrieved from <https://www.rfc-editor.org/rfc/pdfrfc/rfc7296.txt.pdf>, the whole document, in particular, Section 2.8.1	7, 13
T	LIU, D. et al. IKEv2 Rekey Priority Extension. IETF, [online], 2021-11-21, [retrieved on 2022-01-14]. Retrieved from <https://datatracker.ietf.org/doc/pdf/draft-liu-ipsecme-ikev2-rekey-redundant-sas-00>,	1-15

EP 3605976 A1	05/02/2020	EP 3605976 B1	24/02/2021
		CN 107682284 A	09/02/2018
		CN 107682284 B	01/06/2021
		EP 3866434 A1	18/08/2021
		US 2020120078 A1	16/04/2020
		WO 2019024880 A1	07/02/2019
EP 2093975 A1	26/08/2009	JP 2009200689 A	03/09/2009
		JP 4998316 B2	15/08/2012
		US 2009207855 A1	20/08/2009
		US 8089936 B2	03/01/2012
US 10516652 B1	24/12/2019	None	
CN 102271061 A	07/12/2011	CN 102271061 B	25/12/2013

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2021/050725

CLASSIFICATION OF SUBJECT MATTER

IPC
H04L 12/46 (2006.01)
H04L 9/08 (2006.01)
H04L 9/40 (2022.01)
H04W 12/03 (2021.01)