

(51) International Patent Classification:
H04L 29/06 (2006.01) *H04L 12/22* (2006.01)(21) International Application Number:
PCT/EP2009/057203(22) International Filing Date:
10 June 2009 (10.06.2009)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant (for all designated States except US): **NOKIA SIEMENS NETWORKS OY** [FI/FI]; Karaportti 3, FI-02610 Espoo (FI).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **SCHNEIDER, Peter** [DE/DE]; Blumenstraße 21, 83607 Holzkirchen (DE). **HORN, Guenther** [DE/DE]; Prälat-Zistl-Str. 12, 80331 München (DE).(74) Common Representative: **NOKIA SIEMENS NETWORKS OY** et al.; COO RTP IPR, Patent Administration, 80240 Munich (DE).

(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, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

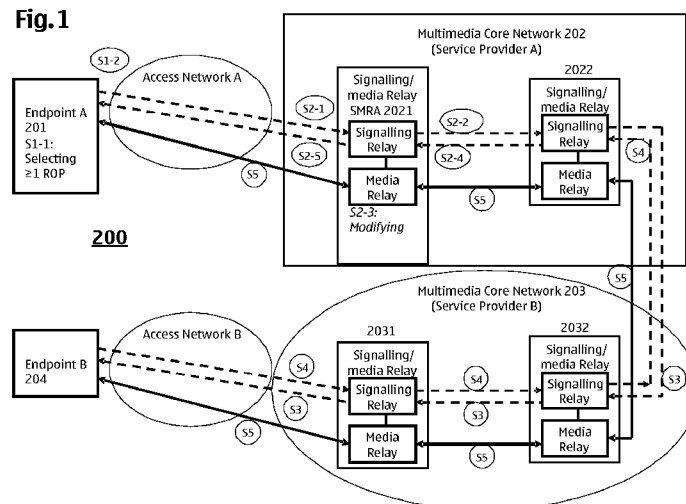
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT,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

Published:

— with international search report (Art. 21(3))

(54) Title: METHODS, APPARATUSES, AND RELATED COMPUTER PROGRAM PRODUCT FOR NETWORK SECURITY

Fig. 1



(57) Abstract: It is disclosed a method (and related apparatus) comprising selecting, at a first endpoint entity, at least one range of protection to be granted, the range of protection relating to one of a plurality of network elements in at least one access network and at least one core network and to a second endpoint entity, and transmitting, to a network element entity, a signaling message comprising first establishment information indicating the at least one range of protection to be granted; and a method (and related apparatus) comprising receiving, at the network element entity, the signaling message from the first endpoint entity, obtaining, from a second endpoint entity and based on the first establishment information, second establishment information indicating protection granted by the second endpoint entity, and signaling, from the network element entity to the first endpoint entity, third establishment information indicating the protection granted to the first endpoint entity.

DESCRIPTION

TITLE

5

METHODS, APPARATUSES, AND RELATED COMPUTER PROGRAM PRODUCT
FOR NETWORK SECURITY

FIELD OF THE INVENTION

10

[0001] Examples of the present invention relate to network security. More specifically, the examples of the present invention relate to methods, apparatuses, and a related computer program product for network security. The examples of the present invention may be applicable to network security e.g. based on a session initiation/description protocol (SIP/SDP) or 3rd generation partnership project (3GPP) internet protocol (IP) multimedia subsystem (IMS).

20 BACKGROUND

[0002] In traditional time division multiplex (TDM) networks, voice may be transmitted mostly "in cleartext", i.e. without any cryptographic protection like encryption, as traditional TDM networks were considered to be secure enough for the needs of the vast majority of users.

[0003] If voice or, more generally, multimedia communication is transmitted over packet networks, e.g. IP based networks like the Internet, the security aspect may differ: It is considered much more likely that communication may be eavesdropped, e.g. at WLAN hotspots, or by a person or entity having gained control over any infrastructure component in a media path, e.g. a router or switch within an IP based network.

[0004] So, it may be considered to apply cryptographic protection to media communication over packet networks. From a user perspective, the protection should be end-to-end (e2e), i.e. the cryptographic protocol should run between the communicating endpoints, with no network element in-between
5 accessing the cleartext of the communication.

[0005] In many cases however, there may be a need for access to the cleartext, e.g. in case of transcoding of the media
10 e.g. in order to transport media over specific network sections. Subscribers may trust their multimedia service provider (SP) to perform such necessary operations. In that case, the SP may require knowledge e.g. of cryptographic parameters such as keys used for encryption and/or integrity
15 protection. Therefore, key management protocols may be used that perform the key exchange by usage of signaling message elements such that the encryption keys are visible to the network elements (NWEs) in the network that process the signaling messages (called "signaling relays" in the
20 following). Examples of such key exchange protocols used for multimedia security over IP networks are SDP security descriptions (SDS) or MIKEY-NULL that can be used to establish keys for a secure real time transport protocol (SRTP) which may be designed for securing multimedia
25 communication based on the real time transport protocol (RTP).

[0006] When using such protocols, signaling may be protected during transport between endpoints and signaling relays or
30 between signaling relays against eavesdropping by third parties. Such protection of the signaling messages can be performed by running e.g. a cryptographic protocol between each pair of entities that exchange signaling messages. For example, if SIP is used for signaling, the cryptographic
35 protocol may be IP secure (IPsec) encapsulating security

payload (ESP) or transport layer security (TLS).

[0007] Another reason why e2e security for the multimedia communication may not be possible is that it cannot be
5 expected that all end user equipment acting as communication endpoint will support the respective mechanisms. In fact, devices used for such multimedia communication may not be capable of supporting the above mechanisms.

10 [0008] In particular, the connection between an end user and a multimedia core network over a so called "access network" may be exposed to attacks (e.g. if WLAN or wire-line shared media techniques are used in the access network). So, it may be reasonable to secure the multimedia communication at least
15 over the access network, providing what is called end-to-middle (e2m) security in the following.

[0009] In consideration of the above, according to examples of the present invention, methods, apparatuses and a related
20 computer program product for network security are provided.

[0010] In this connection, the examples of the present invention enable one or more of the following:
- Establishing optimum media security range of protection
25 (e2e being better than e2m being better than no security) for a media stream in an efficient way: user A of a multimedia communication service wants to apply media security to a multimedia session he is going to establish with another user B. Media security mechanisms are supported by the endpoint used by A. A's service provider generally supports media
30 security mechanisms and, for each individual media stream, may or may not be willing and able to terminate media security within the multimedia core network. User A does not know whether user B's endpoint is able to support media
35 security. User A wants to set up e2e security in case user B's endpoint supports this and to set up e2m security

otherwise. User A may even be willing to perform unsecured communication, if A's service provider should be unable to provide e2m security for a particular multimedia stream. Moreover, when the session is established, A may have

5 information on what type of security is provided: e2e, e2m or none at all;

- Distinguishing between e2e and e2m security;
- No requirement for an enhancement of the registration procedure (e.g. SIP REGISTER message)

10 - Making use of all media security variants, e.g. end-to-middle (e2m) security, by endpoints being capable of media security but not being capable of the enhanced registration procedure;

- Ensuring optimal security, i.e. e2m security only if e2e security is impossible, or no security only if e2m security is impossible: when an endpoint A requests the setup of a secured media stream, there may be no way for the network serving endpoint A (i.e. the network of A's multimedia service provider) to find out what the media security

15 capabilities of the other endpoint are. This could e.g. be the case, if the other endpoint is served by another network;

- Enabling an endpoint to request for different ranges of protection;
- Establishing e2e security whenever supported;

25 - Establishing, in case e2e security is not supported, e2m security if it is supported, and only in the worst case, no security is established at all;

- Establishing security even in cases where signaling/media relay (SMR) A cannot support security termination/origination

30 (which may be a temporary condition, e.g. overload with respect to crypto-processing), by not declining requests to set up "e2m security at least" in this case but rather trying to establish e2e security (only if this fails, the media stream set up fails altogether);

35 - Providing an endpoint that requested the establishment of a media stream with an indication on the protection range

that is provided for this media stream;

- Enabling an efficient mechanism, as only a few or no additional signaling elements are required and no additional exchanges of signaling messages is introduced;

5 - Enabling an efficient and robust mechanism, as no support by relays other than SMRA is required (Legacy relays not being able to process the indicated protection range can ignore it and pass it on unchanged. Even if the remote endpoint does not support the mechanism, still the best possible protection range will be established);

10 - Independency of the procedure for establishing optimum security from how and whether the achieved protection range is indicated to the endpoint;

15 BRIEF DESCRIPTION OF THE DRAWINGS

[0011] The examples of the present invention are described herein below with reference to the accompanying drawings, in which:

20

[0012] Fig. 1 shows an example network where methods for network security according to examples of the present invention can be applied;

25 [0013] Fig. 2 shows a detail of the methods for network security according to the examples of the present invention; and

[0014] Fig. 3 shows apparatuses for network security
30 according to the examples of the present invention.

DETAILED DESCRIPTION OF THE EXAMPLES OF THE PRESENT INVENTION

[0015] The examples of the present invention are described
35 herein below by way of example with reference to the

accompanying

drawings.

[0016] It is to be noted that for this description, the terms "media streams; best effort security, at least end-to-middle security, only end-to-middle security, and/or end-to-end security; at least capable of end-to-middle security; secured data stream between the first and second endpoints; secured datastream between the first endpoint and the network element entity and an unsecured datastream between the network element entity and the other endpoint; unsecured data stream between the first and second endpoints; signaling and media relay entity; extension to a session initiation/description protocol." are examples for "data streams; types of range of protection; types of the protection capabilities; end-to-end security; end-to-middle security; no security; network element entity; first, second and/or third code type", respectively, without restricting the latter-named terms to the special technical or implementation details imposed to the first-named terms.

20

[0017] A so-called "probing" may be employed, e.g. requesting e2e security in a first trial to establish a media stream, and in case this fails, making a second trial requesting e2m security, and possibly even making a third trial, establishing the media stream without security.

25

[0018] Figs. 1 and 2 show the methods for network security according to the examples of the present invention.

[0019] As shown in Figs. 1 and 2, a communication system 200 may comprise a first endpoint A 201, a first multimedia core network 202, a second multimedia core network 203 and a second endpoint B 204. In turn, the multimedia core networks 202 and 203 may each comprise at least one signaling/media relay 2021, 2022, 2031, 2032. Each signaling/media relay 2021, 2022, 2031, 2032 may comprise a signaling relay and a

30

35

media relay.

[0020] As shown in Figs. 1 and 2, if security cannot function in an e2e fashion, it would still be beneficial to secure the communication at least over a part of the communication path where the security mechanisms are supported.

[0021] So, it should be considered to secure the multimedia communication at least over the access network, providing what is called end-to-middle (e2m) security in the following. Providing e2m security may comprise a media stream being relayed over a network element capable of terminating security (in the direction from the endpoint which uses security) and originating security (in the direction towards the endpoint which uses security). A media relay that terminates/originates security may be controlled by the signaling relay instructing the media relay to forward data streams and terminate or originate security for data streams. The signaling relay also may provide security parameters to the media relay, e.g. the keys. As mentioned above, the signaling relay and corresponding media relay together are referred to as "signaling/media relay" 2021, 2022, 2031, 2032 in the following.

[0022] Fig. 1 shows a scenario realizing communication between the two endpoints A 201 and B 204 involving two access networks A and B and the two interconnected multimedia core networks 202, 203, e.g. operated by two different service providers A and B. Signaling and media traffic between the endpoints 201, 204 passes several signaling and media relays 2021, 2022, 2031, 2032, respectively. Each media relay may be controlled by the signaling relay.

[0023] The dotted arrows labeled S1-2, S2-1, S2-2, and S3 show the passing of e.g. a signaling message requesting the establishment of a media stream from endpoint A via the four

signaling relays to endpoint B 204.

[0024] The dotted arrows labeled S4, S2-4 and S2-5 show the passing of e.g. an answer signaling message from endpoint B
5 204 via the four signaling relays to endpoint A 201. The signaling relays may modify certain parts of a signaling message before they pass it on towards the next destination. The purpose of such modifications may be to ensure that the subsequent answer signaling message is routed again via this
10 signaling relay (which might otherwise not necessarily be the case) or to make sure that the subsequent media stream is routed via the media relay controlled by the signaling relay.

[0025] The arrows labeled S5 show the media stream that is
15 relayed between endpoints A 201 and B 201 by the four media relays.

[0026] Fig. 1 shows two core networks 202, 203 and two access networks. However, there could also be a single core network,
20 and endpoints A 201 and B 204 could use a single access network to this core network. There could also be one or more additional core networks be involved, acting as transit core networks between the core networks shown in the figure. Note that there can also be signaling relays that do not control a
25 media relay. The number of involved signaling/media relays can vary. There may be at least one signaling/media relay that serves as the entry point for signaling traffic and media traffic of endpoint A 201 into the core network 202. For endpoint A 201 in Figs. 1 and 2, this is the
30 signaling/media relay SMRA 2021.

[0027] In the example shown in Fig. 2, it is assumed that endpoints A 201 and B1 204-a as well as signaling/media relay
SMR A 2021 support media security mechanisms. Endpoint B2
35 204-b may not support media security mechanisms. All signaling/media relays 2021, 2022, 2031, 2032 may support

transport of signaling elements, including those needed for signaling secured media streams. All media relays may support transport of cleartext or encrypted media. Endpoint A 201 may have a multimedia session with endpoint B1 204-a, where the media stream may be secured in an e2e fashion. Endpoint A 201 may have another session, with endpoint B2 204-b, where the media stream may be secured in an e2m fashion between endpoint A 201 and SMR A 2021.

[0028] Note that in this example, protecting the media communication between endpoint A 201 and endpoint B2 204-b only over the access network A may have relevance although the rest of the communication may be unprotected. For example, the two core networks may be considered secure in the sense that mechanisms such as physical protection make it unlikely that communication can be eavesdropped there. Access network B on the other hand might use its own, access network specific security mechanism, e.g. it could be a 3GPP mobile network applying the encryption mechanisms specified by 3GPP for such networks.

[0029] First, in step S1-1, e.g. endpoint A 201 may perform selecting, at a first endpoint entity (e.g. endpoint A 201 itself), at least one range of protection to be granted, the range of protection relating to a plurality of network elements in at least one access network and at least one core network, or to a second endpoint entity.

[0030] Then, in step S1-2, e.g. endpoint A 201 may perform transmitting, to a network element entity (e.g. SMR A 2021), a signaling message comprising first establishment information indicating the at least one range of protection to be granted. In step S2-1, e.g. SMR A 2021 may perform receiving, at the network element entity (e.g. SMR A 2021 itself), the signaling message from the first endpoint entity, the signaling message comprising the first

establishment information indicating the at least one range
of protection to be granted.

[0031] Then, in steps S2-2 and S2-4 (and further in steps S3
5 and S4), e.g. SMR A 2021 may perform obtaining, at the
network element entity (e.g. SMR A 2021 itself), from the
second endpoint entity different from the first endpoint
entity and based on the first establishment information,
second establishment information indicating protection
10 granted by the second endpoint entity.

[0032] Further, in an optional step S2-5, e.g. SMR A 2021 may
perform signaling, from the network element entity (e.g. SMR
A 2021) to the first endpoint entity (e.g. endpoint A 201),
15 third establishment information indicating the protection
granted to the first endpoint entity.

[0033] As for further developments of the methods pertaining
to endpoint A 201 and SMR A 2021, the first, second and third
20 establishment information may respectively relate to a data
stream to be established. Further, the first information may
comprise an explicit information element for indicating a
desired type of the range of protection.

[0034] Moreover, the second or third establishment
information may comprise an explicit information element for
indicating the granted protection. Alternatively, the first,
second or third establishment information may comprise an
explicit information element for indicating the protection
30 capabilities of the first endpoint entity, second endpoint
entity or a network element entity respectively.
Alternatively, no explicit information element indicating the
range of protection may be contained in the first
establishment information.

35

[0035] Further, in an optional step S5, e.g. endpoint A 201 and SMR A 2021 may perform establishing end-to-end security if possible, else end-to-middle security if possible, else no security.

5

[0036] In addition to the above, the first establishment information may indicate one secured data stream to be established and one unsecured data stream to be established, and the second and third establishment information may indicate the secured data stream and/or the unsecured data stream. In that case, the secured data stream and the unsecured data stream may have to be established as parallel data streams according to the indication in the first establishment information. Further, the signaling may be repeated with the first establishment information indicating only the secured data stream. In that case, the signaling may be repeated in case the second endpoint has signaled grant of both the secured and the unsecured data stream.

[0037] As an alternative to the above, the secured data stream and the unsecured data stream may be signaled to be established as alternative data streams.

[0038] Alternatively, the first and third establishment information may indicate one secured data stream to be established, and the second establishment information may indicate an unsecured data stream. In that case, in an optional step S2-3, e.g. SMR A 2021 may perform modifying, upon receiving the first establishment information comprising an indication of the range of protection, the first establishment information to indicate an unsecured data stream, wherein the modifying may be performed prior to a transmission of the modified first establishment information to the second endpoint entity. In that case, the range of protection comprised in the first establishment information

may be end-to-middle-only.

[0039] Alternatively, the first establishment information may indicate one secured data stream to be established, the
5 second and third establishment information may indicate failure, and wherein after signaling of the third establishment information, the receiving may comprise a repeated receiving of the first establishment information with a range of protection to be granted different from the
10 range of protection to be granted which was used when having received the first establishment earlier. In that case, the range of protection comprised in the repeated first establishment information may be end-to-middle-only. Further, the third establishment information may comprise capability
15 information.

[0040] In addition to the above, if the transmitting and the signaling are based on a session initiation/description protocol, the establishment information messages may be
20 headed by a first code type indicating the requested type of data stream. In that case, the first code type may be followed by a second code type indicating the type of range of protection. In that case, the second code type may be followed by a third code type indicating the protection
25 capabilities.

[0041] In addition to the above, the transmitting, receiving and signaling may be performed dynamically.

30 [0042] For example, for each media stream to be established by the endpoint 201, the endpoint 201 can signal to the network the "protection range" either by using an explicit signaling element within the signaling message used to establish the media stream, or in an implicit way, as
35 described herein below. Up to three or more different protection ranges "best effort security" (PR_BE), "e2m

security at least" (PR_e2m_at_least), and "e2e security mandatory" (PR_e2e) may be supported, i.e. they can be signaled (explicitly or implicitly) by the endpoints 201 or 204, and the network may establish security accordingly.

5

[0043] Fig. 3 shows apparatuses (e.g. endpoint 201 and SMR 2021) for network security according to the examples of the present invention. Within Fig. 3, for ease of description, means or portions which may provide main functionalities are depicted with solid functional blocks or arrows and/or a normal font, while means or portions which may provide optional functions are depicted with dashed functional blocks or arrows and/or an italic font.

10

[0044] The endpoint 201 may comprise a CPU (or core functionality CF) 2011, a memory 2012, a transmitter (or means for transmitting) 2013, an optional receiver (or means for receiving) 2014 and a selector (or means for selecting) 2015. Further, the endpoint 205 may comprise elements (not shown) identical or similar to those of endpoint 201.

20

[0045] And, the SMR 2021 may comprise a CPU (or core functionality CF) 20211, a memory 20212, a transmitter (or means for transmitting) 20213, a receiver (or means for receiving) 20214, an obtainer (or means for obtaining) 20215, a signaler (or means for signaling) 20216 and an optional modifier (or means for modifying) 20217.

25

[0046] As indicated by the dashed extensions of the functional blocks of the CPU 2011 or 20221, the means for selecting 20215 of the endpoint 201 as well as the means for obtaining 20215, means for signaling 20216 and the means for modifying 20217 of the SMR 2021 may be functionalities running on the CPU 2011 or 20221 of the endpoint 201 or SMR 2021, or may alternatively be separate functional entities or

35

means.

[0047] The CPUs 20x1 (wherein x = 1 and 21) may respectively be configured, for example by software residing in the memory 20x2, to process various data inputs and to control the functions of the memories 20x2, the means for transmitting 20x3 and the means for receiving 20x4 (and the means for selecting 20215 of the endpoint 201 as well as the means for obtaining 20215, means for signaling 20216 and the means for modifying 20217 of the SMR 2021). Further, it is to be noted that the CPUs 20x1, the means for transmitting 20x3 and the means for receiving 20x4 may constitute means for establishing 205 in the sense of the examples of the present invention. The memories 20x2 may serve e.g. for storing code means for carrying out e.g. the methods according to the example of the present invention, when run e.g. on the CPUs 20x1. It is to be noted that the means for transmitting 20x3 and the means for receiving 20x4 may alternatively be provided as respective integral transceivers. It is further to be noted that the transmitters/receivers may be implemented i) as physical transmitters/receivers for transceiving e.g. via the air interface (e.g. endpoint 201 and SMR 2021), ii) as routing entities e.g. for transmitting/receiving data packets e.g. in a PS (packet switching) network (e.g. between SMR 2021 and another SMR 2022 when disposed as separate network entities), iii) as functionalities for writing/reading information into/from a given memory area (e.g. in case of shared/common CPUs or memories e.g. between SMR 2021 and another SMR 2022 when disposed as an integral network entity), or iv) as any suitable combination of i) to iii).

[0048] First, e.g. the means for selecting 2015 of endpoint A 201 may perform selecting, at a first endpoint entity (e.g. endpoint A 201 itself), at least one range of protection to be granted, the range of protection relating to a plurality

of network elements in at least one access network and at least one core network, or to a second endpoint entity.

[0049] Then, e.g. the means for transmitting 2013 of endpoint
5 A 201 may perform transmitting, to a network element entity
(e.g. SMR A 2021), a signaling message comprising first
establishment information indicating the at least one range
of protection to be granted. For example, the means for
receiving 20214 of SMR A 2021 may perform receiving, at the
10 network element entity (e.g. SMR A 2021 itself), the
signaling message from the first endpoint entity, the
signaling message comprising the first establishment
information indicating the at least one range of protection
to be granted.

15
[0050] Then, e.g. the means for obtaining 20215 of SMR A 2021
may perform obtaining, at the network element entity (e.g.
SMR A 2021 itself), from the second endpoint entity (e.g.
second endpoint 204) different from the first endpoint entity
20 and based on the first establishment information, second
establishment information indicating protection granted by
the second endpoint entity.

[0051] Further, e.g. the means for signaling 20216 of SMR A
25 2021 may perform signaling, from the network element entity
(e.g. SMR A 2021) to the first endpoint entity (e.g. endpoint
A 201), third establishment information indicating the
protection granted to the first endpoint entity.

30 [0052] As for further developments of endpoint A 201 and SMR
A 2021, the first, second and third establishment information
may respectively relate to a data stream to be established.
Further, the first information may comprise an explicit
information element for indicating a desired type of the
35 range of protection.

[0053] Moreover, the second or third establishment information may comprise an explicit information element for indicating the granted protection. Alternatively, the first, second or third establishment information may comprise an explicit information element for indicating the protection capabilities of the first endpoint entity, second endpoint entity or a network element entity respectively. Alternatively, no explicit information element indicating the range of protection may be contained in the first establishment information.

[0054] Further, e.g. the means for establishing 205 of endpoint A 201 and SMR A 2021 may perform establishing end-to-end security if possible, else end-to-middle security if possible, else no security.

[0055] In addition to the above, the first establishment information may indicate one secured data stream to be established and one unsecured data stream to be established, and the second and third establishment information may indicate the secured data stream and/or the unsecured data stream. In that case, the secured data stream and the unsecured data stream may have to be established as parallel data streams according to the indication in the first establishment information. Further, the signaling may be repeated with the first establishment information indicating only the secured data stream. In that case, the signaling may be repeated in case the second endpoint has signaled grant of both the secured and the unsecured data stream.

[0056] As an alternative to the above, the secured data stream and the unsecured data stream may be signaled to be established as alternative data streams.

[0057] Alternatively, the first and third establishment information may indicate one secured data stream to be

established, and the second establishment information may indicate an unsecured data stream. In that case, e.g. the means for modifying 20217 of SMR A 2021 may perform modifying, upon receiving the first establishment information
5 comprising an indication of the range of protection, the first establishment information to indicate an unsecured data stream, wherein the modifying may be performed prior to a transmission of the modified first establishment information to the second endpoint entity. In that case, the range of
10 protection comprised in the first establishment information may be end-to-middle-only.

[0058] Alternatively, the first establishment information may indicate one secured data stream to be established, the
15 second and third establishment information may indicate failure, and wherein after signaling of the third establishment information, the receiving may comprise a repeated receiving of the first establishment information with a range of protection to be granted different from the
20 range of protection to be granted which was used when having received the first establishment earlier. In that case, the range of protection comprised in the repeated first establishment information may be end-to-middle-only. Further, the third establishment information may comprise capability
25 information.

[0059] In addition to the above, if the means for transmitting and the means for signaling are configured to perform based on a session initiation/description protocol,
30 the establishment information messages may be headed by a first code type indicating the requested type of data stream. In that case, the first code type may be followed by a second code type indicating the type of range of protection. In that case, the second code type may be followed by a third code
35 type indicating the protection capabilities.

[0060] In addition to the above, the transmitting, receiving and signaling may be performed dynamically.

[0061] For example, for each media stream to be established by the endpoint 201, the endpoint 201 can signal to the network the "protection range" either by using an explicit signaling element within the signaling message used to establish the media stream, or in an implicit way, as described herein below. Up to three different protection ranges "best effort security" (PR_BE), "e2m security at least" (PR_e2m_at_least), and "e2e security mandatory" (PR_e2e) may be supported, i.e. they can be signaled (explicitly or implicitly) by the endpoints 201 or 204, and the network may establish security accordingly.

15

[0062] It is to be noted that any of the apparatus and/or method features cited herein below merely constitute optional method/apparatus features.

20 [0063] **Support of different sets of protection ranges**

[0064] As stated before, it is not necessary that all 3 protection ranges are supported (i.e. can be explicitly or implicitly be signaled, and the network behaves accordingly). So, any combination may be used.

25

[0065] An exemplary subset could e.g. comprise only PR_BE and PR_e2e (i.e. no signaling of "e2m security at least" is possible). In this case, if a data stream is to be established by the endpoint A 201 with at least e2m security, the endpoint A 201 can indicate PR_BE ("best effort security"), and cancel the media stream setup in case no security can be established. Restricting the method to these two options reduces the effort in the SMR A 2021 (only two cases to distinguish).

35

[0066] For example, it is possible to use only one of two explicit protection range indications (e.g. one of "e2e security" and "e2m security only"). In case one protection range indication is used only, its absence in a signaling answer from SMR A 2021 to endpoint A 201 containing the acceptance of a secured stream may indicate that the other protection range (that cannot be signaled explicitly) has been achieved. It is also possible to completely dispense with the signaling of the achieved protection range, since the establishment of optimum security would still work even without the endpoint A 201 not having information how far the achieved security extends.

[0067] **BE security**

[0068] For example, "Best effort security" (PR_BE) may mean that the endpoint 201 prefers e2e security over e2m security over no security. In this case, the endpoint may signal two alternative media streams, one with security (a secured stream) and one without security (an unsecured stream), and may be prepared to establish the unsecured stream in case no security can be provided, and to establish the secured stream in case e2m or e2e security can be provided. The network may try to establish e2e security, if possible, otherwise it may try to establish e2m security, and if this is also not possible, the media stream may be established without security.

[0069] In other words, when a media stream is to be established by an endpoint A 201 with "best effort security" with an endpoint B 204, endpoint A 201 may send a signaling message containing two alternative streams (one secured and one unsecured stream) and indicating PR_BE to a signaling/media relay SMR A 2021 in the multimedia core network 202 of A's service provider, where the media relay may be capable of originating and terminating security for

media streams. By adding suitable signaling elements to the signaling message, or by suitably changing signaling elements within the signaling message, the SMR A 2021 may ensure that the media stream, once it is established, will be routed via SMR A 2021, and that the answer signaling from the called endpoint B 204 towards A 201 will also be routed via the SMR A 2021. The SMR A 2021 may pass the modified signaling message on towards endpoint B 204. When the signaling message reaches the endpoint B 204, endpoint B 204 may decide which of the data streams it accepts, and may send a respective signaling answer towards endpoint A 201. When this signaling answer reaches SMR A 2021, the SMR A 2021 may inspect the answer. If the answer signals acceptance of the secured stream, SMR A 2021, in its signaling answer to endpoint A 201, may signal acceptance of the secured stream and may indicate "e2e security". If the answer signals acceptance of the unsecured stream only, and the SMR A 2021 is capable to terminate/originate security for this specific media stream, SMR A 2021 may configure its media relay to terminate and originate security from and towards the endpoint A 201, respectively, e.g. to transform the secured media stream from endpoint A 201 into the unsecured stream towards endpoint B 204 and to transform the unsecured media stream from endpoint B 204 into the secured stream towards endpoint A 201. SMR A 2021 may then signal acceptance of the secured stream towards endpoint A 201 and may indicate "e2m security only". If the answer from endpoint B 204 signals acceptance of the unsecured stream only, and SMR A 2021 is not capable to terminate/originate security for this specific media stream, SMR A 2021 may signal acceptance of the unsecured stream only to endpoint A 201. No indication about the protection range may be needed in this answer, as endpoint A 201 may realize that no security can be provided from the fact that only the unsecured stream is accepted.

35

[0070] For example, rather than using explicit signaling elements to indicate the requested protection range, this may be indicated implicitly. For example, signaling only a secured media stream may indicate either PR_e2m_at_least or PR_e2e (which of these may be agreed beforehand between the user A and its service provider) and signaling one secured and one unsecured media stream that are otherwise identical may indicate the request of PR_BE.

[0071] For example, in SIP/SDP signaling, signaling of two streams in parallel may be interpreted as a request to establish both streams. So, if the endpoint B 204 follows this interpretation, endpoint B 204 has the choice to accept either or both of the streams (the unsecured and the secured stream) that are contained in the signaling message. (The same situation may arise if PR_BE had been signaled using an explicit signaling element, but endpoint B 204 is unaware of the mechanism and does not understand the signaling element, or if one of the relays, unaware of the mechanism, has unexpectedly removed the signaling element indicating PR_BE). If in this situation endpoint B 204 decides to accept only one of the streams, the mechanism works as described above.

[0072] To resolve the situation of acceptance of both data streams, there may be two options:

1. Either the means for signaling 20216 of SMR A 2021 may repeat the signaling towards endpoint B 204, this time signaling only the secured stream. B's answer on this second signaling may signal acceptance of the secured stream, and SMR A 2021 may pass this to endpoint A 201 e.g. with the indication "e2e security".

2. Or, the means for signaling 20216 of SMR A 2021 may just pass endpoint B's 204 answer indicating acceptance of both streams to endpoint A 201, leaving it to endpoint A 201 to repeat the signaling with only the secured stream, or to do

anything else A may want to do.

[0073] By using one of these two options, e2e security may be achieved.

5

[0074] For example, in an environment where it is possible to signal two alternative media streams (rather than two parallel media streams, as described above), this feature could be used to signal PR_BE, i.e. the secured and the unsecured stream are signaled as alternative streams, without an explicit signaling element indicating PR_BE.

10

[0075] For example, in SIP/SDP signaling, there may be a way to signal both a secured and an unsecured stream. An endpoint aware of the mechanism may realize that two different, alternative streams are indicated and may accept only one of them. An endpoint not aware of the mechanism may only realize one of the alternative streams and ignore any alternative streams. SMR A 2021, when receiving the answer, may act as described above for BE security. That is, if endpoint B 204 has accepted the secured stream, e2e security is achieved; in case endpoint B 204 has accepted the unsecured stream only, e2m security is achieved.

15

20

25

[0076] For example, in case PR_e2m_at_least is signaled by endpoint A 201 explicitly or implicitly, the means for converting 20216 of the SMR A 2021 may convert this signaling into signaling of PR_BE as described herein below and may use one of the two techniques described above (signaling parallel streams or signaling alternative streams) to signal PR_BE implicitly.

30

[0077] **E2M security**

35

[0078] "e2m security at least" (PR_e2m_at_least) may mean that the endpoint 201 may prefer e2e security over e2m

security and does not accept no security. In this case, the means for transmitting 2013 of the endpoint A 201 may signal a secured stream only. The network may try to establish e2e security, if possible, otherwise it may try to establish e2m security. The stream establishment may intentionally fail if no security can be provided.

[0079] For example, when a media stream is to be established by endpoint A 201 with "e2m security at least" with an endpoint B 204, the means for transmitting 2013 of endpoint A 201 may send a signaling message containing a secured stream (but no alternative unsecured stream) and indicating PR_e2m_at_least to the signaling/media relay SMR A 2021 in the multimedia core network 202 of endpoint A's service provider, where the media relay is capable of originating and terminating security for media streams. The means for signaling 20216 of SMR A 2021 may then signal the secured stream as well as an unsecured stream (with the same characteristics otherwise) towards the endpoint B 204 and may indicates PR_BE. From this point, the procedure may function like BE security described above, with the only difference that if the means for receiving 20214 of SMR A 2021 receives acceptance of the unsecured stream only and is itself not capable to terminate/originate security for this specific media stream, the means for signaling 20216 of SMR A 2021 may not be able to signal acceptance of the unsecured stream towards endpoint A 201, as endpoint A 201 has not signaled this stream in its original request. So, SMR A 2021 may reject the secured stream in its answer to endpoint A 201 and the establishment of a media stream may fail.

[0080] The mechanism described above focuses on signaling originating from endpoint A 201. It may be enhanced by support of e2m security in case endpoint A 201 is the terminating point of an unsecure media stream signaled by some other endpoint B 204. In this case, SMR A 2021, being

the last signaling/media relay before the traffic is passed to endpoint A 201, when receiving a signaling message by which endpoint B 204 requests the establishment of an unsecured media stream, may add an alternative, secured media stream to the signaling message and may indicate "e2m security only" in the signaling message. In case endpoint A 201 accepts the unsecured stream, this has no further effect. In case endpoint A 201 accepts the added secured stream, SMR A 2021 may transform the subsequent media stream between secured (towards endpoint A 201) and unsecured (towards endpoint B 204) as described for BE security above.

[0081] **E2E**

security

[0082] "e2e security mandatory" (PR_e2e) may mean that the endpoint A 201 accepts only e2e security. The endpoint A 201 may signal a secured stream only. The network may try to establish e2e security, and the stream establishment may intentionally fail if e2e security cannot be provided.

20

[0083] When a media stream is to be established by the endpoint A 201 only if e2e security is supported, the endpoint A 201 may transmit a signaling message containing a secured stream (but no alternative unsecured stream) and indicating PR_e2e to the signaling/media relay SMR A 2021 in the multimedia core network 202 of A's service provider. SMR A 2021 may pass this message on towards the endpoint B 204, which may either accept or reject the secured stream. When this signaling answer reaches SMR A 2021, SMR A 2021 may pass it on to endpoint A 201 and may indicate "e2e security".

30

[0084] Moreover, for each secure media stream that is established, the network can signal to the endpoint A 201 that has requested the establishment of the stream either "e2e security" or "e2m security only", where the latter means that security may be terminated e.g. in the core network 202

35

of the endpoint's service provider, and the former means that this may not be the case (and is therefore truly e2e as long as no other networks which are passed by the media stream terminate the security without indicating it). There may e.g.
5 be a gateway to a traditional telephone network, which may terminate media security without necessarily indicating this. Note that an explicit indication of "no security" is not needed, because an endpoint may get this information from the fact that a secured stream is not accepted.

10 [0085] **Variants in signaling of the achieved protection range**

[0086] For example, A's service provider (e.g. in core network 202) may decide to replace the indication "e2e
15 security" it would send to endpoint A 201 according to the mechanism by a new indication "e2m security at least" in all cases where the media stream traverses core networks of other service providers. With this modification, an indication of "e2e security" may mean that the media stream is secured on
20 each hop between endpoint and media relay or between media relays. The indication of "e2m security at least" may mean that the media stream is protected over the access network between endpoint A 201 and the core network 202 of A's service provider and all through A's service provider's core
25 network and may also be protected on the rest of the communication path.

[0087] **Application of the mechanism to SIP/SDP**

30 [0088] The mechanism described above is applicable to IP networks e.g. with SIP/SDP signaling, where the signaling relays may be SIP proxies or SIP back-to-back user agents. The media relays may be IP-IP-gateways which may - apart from possibly terminating/ originating media security - perform
35 tasks like NAT traversal, far end NAT support, policy control or other border control functions. An instance of a

signaling/ media relay may be a so called session border controller applicable e.g. to voice over IP (VoIP) networks.

[0089] For example, in SIP/SDP, media streams may be described by so called "m-lines", followed by attributes. E.g. an m-line describing an audio stream could have the format:

```
m=audio          12345          RTP/SAVP          ...  
a=crypto                ....
```

[0090] Here, the transmitter of this session description indicates it is prepared to receive an audio stream using SRTP, where the crypto parameters (in particular the key) are specified in an attribute labeled "crypto".

[0091] In this context, protection ranges PR_BE, PR_e2m_at_least, and PR_e2e may be signaled by adding a line
a=req_prot_range:best_effort,
a=req_prot_range:e2m_at_least
and
a=req_prot_range:e2e_mandatory,
respectively.

[0092] In an answer from SMR A 2021 to endpoint A 201, SMR A 2021 could indicate the achieved protection range by adding a line:

```
a=prot_range:e2e,  
a=prot_range:e2m_at_least,  
or  
a=prot_range:e2m_only.
```

[0093] In this context, implicit signaling of PR_BE by specifying two alternative streams (as described above) could be done using a capability negotiation method. The difference would be a different behavior of SMR A 2021, which would transform between the secured and the unsecured media stream

in case the endpoint B accepts the unsecure stream, thus achieving e2m security, where the capability negotiation method would result in no security at all.

5 [0094] **Application of the mechanism to the 3GPP IMS**

[0095] The SIP/SDP signaling and transport of media over RTP or SRTP is also part of the IP Multimedia Subsystem (IMS). The methods described above may also be applied to IMS. In
10 this case, SMR A 2021 may be a proxy call session control function (P-CSCF) as the signaling relay plus the IMS access gateway as the media relay.

[0096] Furthermore, at least one of, or more of the above-
15 described means for receiving 20214, means for obtaining 20215, means for signaling 20216, means for selecting 2015, means for transmitting 2013, 20213, means for establishing 205, means for modifying 20217 as well as the endpoint 201 and the SMR 2021, or the respective functionalities carried
20 out, may be implemented as a chipset, module or subassembly.

[0097] Further, the examples of the present invention may also relate to a computer program product comprising code means for performing a method according to the above examples
25 of the present invention when run on a processing means or module.

[0098] Finally, the examples of the present invention also relate to a system which may comprise the endpoint 201 and
30 the SMR 2021 according to the above-described examples of the present invention.

[0099] [Further examples]

35 [0100] For the purpose of the present invention as described herein above, it should be noted that

- an access technology may be any technology by means of which a user equipment can access an access network (or base station, respectively). Any present or future technology, such as WiMAX (Worldwide Interoperability for Microwave
5 Access) or WLAN (Wireless Local Access Network), BlueTooth, Infrared, and the like may be used; although the above technologies are mostly wireless access technologies, e.g. in different radio spectra, access technology in the sense of the present invention may also imply wirebound technologies,
10 e.g. IP based access technologies like cable networks or fixed line.

- a network may be any device, unit or means by which a station entity or other user equipment may connect to and/or utilize services offered by the access network; such services
15 include, among others, data and/or (audio-) visual communication, data download etc.;

- generally, the present invention may be applicable in those network/user equipment environments relying on a data packet based transmission scheme according to which data are
20 transmitted in data packets and which are, for example, based on the Internet Protocol IP. The present invention is, however, not limited thereto, and any other present or future IP or mobile IP (MIP) version, or, more generally, a protocol following similar principles as (M)IPv4/6, is also
25 applicable;

- a user equipment may be any device, unit or means by which a system user may experience services from an access network;

- method steps likely to be implemented as software code portions and being run using a processor at a network element
30 or terminal (as examples of devices, apparatuses and/or modules thereof, or as examples of entities including apparatuses and/or modules therefore), are software code independent and can be specified using any known or future developed programming language as long as the functionality
35 defined by the method steps is preserved;

- generally, any method step is suitable to be implemented as

software or by hardware without changing the idea of the invention in terms of the functionality implemented;

- method steps and/or devices, units or means likely to be implemented as hardware components at the above-defined apparatuses, or any module(s) thereof, are hardware independent and can be implemented using any known or future developed hardware technology or any hybrids of these, such as MOS (Metal Oxide Semiconductor), CMOS (Complementary MOS), BiMOS (Bipolar MOS), BiCMOS (Bipolar CMOS), ECL (Emitter Coupled Logic), TTL (Transistor-Transistor Logic), etc., using for example ASIC (Application Specific IC (Integrated Circuit)) components, FPGA (Field-programmable Gate Arrays) components, CPLD (Complex Programmable Logic Device) components or DSP (Digital Signal Processor) components; in addition, any method steps and/or devices, units or means likely to be implemented as software components may alternatively be based on any security architecture capable e.g. of authentication, authorization, keying and/or traffic protection;
- devices, units or means (e.g. the above-defined apparatuses, or any one of their respective means) can be implemented as individual devices, units or means, but this does not exclude that they are implemented in a distributed fashion throughout the system, as long as the functionality of the device, unit or means is preserved;
- an apparatus may be represented by a semiconductor chip, a chipset, or a (hardware) module comprising such chip or chipset; this, however, does not exclude the possibility that a functionality of an apparatus or module, instead of being hardware implemented, be implemented as software in a (software) module such as a computer program or a computer program product comprising executable software code portions for execution/being run on a processor;
- a device may be regarded as an apparatus or as an assembly of more than one apparatus, whether functionally in cooperation with each other or functionally independently of

each other but in a same device housing, for example.

[0101] According to an example of the present invention, in a first aspect, this object is for example achieved by **a method**

5 comprising:

receiving, at a network element entity, a signaling message from a first endpoint entity, the signaling message comprising first establishment information indicating at least one range of protection to be granted, the range of protection relating to one of a plurality of network elements
10 in at least one access network and at least one core network and to a second endpoint entity;
obtaining, at a network element entity, from a second endpoint entity different from the first endpoint entity and based on the first establishment information, second establishment information indicating protection granted by the second endpoint entity; and
15 signaling, from the network element entity to the first endpoint entity, third establishment information indicating the protection granted to the first endpoint entity.
20

[0102] According to an example of the present invention, in a second aspect, this object is for example achieved by **a**

25 **method** comprising:

selecting, at a first endpoint entity, at least one range of protection to be granted, the range of protection relating to one of a plurality of network elements in at least one access network and at least one core network and to
30 a second endpoint entity; and
transmitting, to a network element entity, a signaling message comprising first establishment information indicating the at least one range of protection to be granted.

35 [0103] According to further refinements of the example of the present invention as defined under the above first and second

aspects,

- the first, second and third establishment information respectively relate to a data stream to be established;

- the first information comprises an explicit information element for indicating a desired type of the range of protection;

- one of the second and third establishment information comprises an explicit information element for indicating the granted protection;

- one of the first, second and third establishment information comprises an explicit information element for indicating the protection capabilities of one of the first endpoint entity, second endpoint entity and a network element entity respectively;

- no explicit information element indicating the range of protection is contained in the first establishment information;

- end-to-end security is established if possible, else end-to-middle security if possible, else no security;

- the first establishment information indicates one secured data stream to be established and one unsecured data stream to be established, and the second and third establishment information indicates at least one of the secured data stream and the unsecured data stream;

- the secured data stream and the unsecured data stream are to be established as parallel data streams according to the indication in the first establishment information;

- the signaling is repeated with the first establishment information indicating only the secured data stream;

- the signaling is repeated in case the second endpoint has signaled grant of both the secured and the unsecured data stream;

- the secured data stream and the unsecured data stream are signaled to be established as alternative data streams;

- the first and third establishment information indicate one secured data stream to be established, and the second

establishment information indicates an unsecured data stream;

- the method further comprises, in the first network element entity and upon receiving the first establishment information comprising an indication of the range of protection,5 modifying the first establishment information to indicate an unsecured data stream, wherein the modifying is performed prior to a transmission of the modified first establishment information to the second endpoint entity;
- the range of protection comprised in the first10 establishment information is end-to-middle-only;
- the first establishment information indicates one secured data stream to be established, the second and third establishment information indicate failure, and wherein after signaling of the third establishment information, the15 receiving comprises a repeated receiving of the first establishment information with a range of protection to be granted different from the range of protection to be granted which was used when having received the first establishment earlier;
- 20 - the range of protection comprised in the repeated first establishment information is end-to-middle-only;
- the third establishment information comprises capability information;
- if the transmitting and the signaling are based on a25 session initiation/description protocol, the establishment information messages are headed by a first code type indicating the requested type of data stream;
- the first code type is followed by a second code type indicating the type of range of protection;
- 30 - the second code type is followed by a third code type indicating the protection capabilities;
- the transmitting, receiving and signaling are performed dynamically;
- the data streams are constituted by media streams;
- 35 - the types of range of protection comprise at least one of best effort security, at least end-to-middle security, only

end-to-middle security, and end-to-end security;
- the types of the protection capabilities comprise at least
capable of end-to-middle security;
- the end-to-end security comprises a secured data stream
5 between the first and second endpoints;
- the end-to-middle security comprises a secured datastream
between the first endpoint and the network element entity and
an unsecured datastream between the network element entity
and the other endpoint;
10 - no security comprises an unsecured data stream between the
first and second endpoints;
- the network element entity is constituted by a signaling
and media relay entity;
- at least one of the first, second and third code types is
15 an extension to a session initiation/description protocol.

[0104] According to an example of the present invention, in a
third aspect, this object is for example achieved by **an**
apparatus comprising:
20 means for receiving, at a network element entity, a
signaling message from a first endpoint entity, the signaling
message comprising first establishment information indicating
at least one range of protection to be granted, the range of
protection relating to one of a plurality of network elements
25 in at least one access network and at least one core network
and to a second endpoint entity;
means for obtaining, at a network element entity, from
a second endpoint entity different from the first endpoint
entity and based on the first establishment information,
30 second establishment information indicating protection
granted by the second endpoint entity; and
means for signaling, from the network element entity
to the first endpoint entity, third establishment information
indicating the protection granted to the first endpoint
35 entity.

[0105] According to an example of the present invention, in a fourth aspect, this object is for example achieved by an apparatus comprising:

means for selecting, at a first endpoint entity, at
5 least one range of protection to be granted, the range of protection relating to one of a plurality of network elements in at least one access network and at least one core network and to a second endpoint entity; and
means for transmitting, to a network element entity, a
10 signaling message comprising first establishment information indicating the at least one range of protection to be granted.

[0106] According to further refinements of the example of the present invention as defined under the above third and fourth aspects,

- the first, second and third establishment information respectively relate to a data stream to be established;
- the first information comprises an explicit information element for indicating a desired type of the range of protection;
- one of the second and third establishment information comprises an explicit information element for indicating the granted protection;
- 25 - one of the first, second and third establishment information comprises an explicit information element for indicating the protection capabilities of one of the first endpoint entity, second endpoint entity and a network element entity respectively;
- 30 - no explicit information element indicating the range of protection is contained in the first establishment information;
- end-to-end security is configured to be established if possible, else end-to-middle security if possible, else no security;
- 35 - the first establishment information indicates one secured

data stream to be established and one unsecured data stream to be established, and the second and third establishment information indicates at least one of the secured data stream and the unsecured data stream;

5 - the secured data stream and the unsecured data stream are configured to be established as parallel data streams according to the indication in the first establishment information;

10 - the means for signaling is configured to repeat signaling with the first establishment information indicating only the secured data stream;

15 - the means for signaling is configured to repeat signaling in case the second endpoint has signaled grant of both the secured and the unsecured data stream;

20 - the secured data stream and the unsecured data stream are configured to be signaled to be established as alternative data streams;

25 - the first and third establishment information indicate one secured data stream to be established, and the second establishment information indicates an unsecured data stream;

30 - the apparatus further comprises means for modifying, in the first network element entity and upon receiving the first establishment information comprising an indication of the range of protection, the first establishment information to indicate an unsecured data stream, wherein the modifying is performed prior to a transmission of the modified first establishment information to the second endpoint entity by the means for transmitting;

35 - the range of protection comprised in the first establishment information is end-to-middle-only;

 - the first establishment information indicates one secured data stream to be established, the second and third establishment information indicate failure, and wherein, after the signaling of the third establishment information performed by the means for signaling, the means for receiving is configured to repeat receiving of the first establishment

information with a range of protection to be granted different from the range of protection to be granted which was used when having received the first establishment earlier;

- 5 - the range of protection comprised in the repeated first establishment information is end-to-middle-only;
- the third establishment information comprises capability information;
- the access network comprises one of session initiation
- 10 protocol proxy entities and session initiation protocol back-to-back user agents and the core network comprises internet protocol-internet protocol gateways;
- the internet protocol-internet protocol gateways are constituted by session border controllers;
- 15 - if the means for transmitting and the means for signaling are configured to perform based on a session initiation/description protocol, the establishment information messages are headed by a first code type indicating the requested type of data stream;
- 20 - the first code type is followed by a second code type indicating the type of range of protection;
- the second code type is followed by a third code type indicating the protection capabilities;
- the core network comprises a signaling media relay which
- 25 is configured to origin and terminate any security type for data streams;
- the means for transmitting, means for receiving and means for signaling are configured to perform dynamically;
- the data streams are constituted by media streams;
- 30 - the types of range of protection comprise at least one of best effort security, at least end-to-middle security, only end-to-middle security, and end-to-end security;
- the types of the protection capabilities comprise at least capable of end-to-middle security;
- 35 - the end-to-end security comprises a secured data stream between the first and second endpoints;

- the end-to-middle security comprises a secured datastream between the first endpoint and the network element entity and an unsecured datastream between the network element entity and the other endpoint;
- 5 - no security comprises an unsecured data stream between the first and second endpoints;
- the network element entity is constituted by a signaling and media relay entity;
- at least one of the first, second and third code types is an extension to a session initiation/description protocol;
- 10 - at least one, or more of means for receiving, means for obtaining, means for signaling, means for selecting, means for transmitting, means for establishing, means for modifying and the apparatus is implemented as a chipset, module or subassembly.
- 15

[0107] According to an example of the present invention, in a fifth aspect, this object is for example achieved by **an apparatus** comprising:

- 20 a receiver configured to receive, at a network element entity, a signaling message from a first endpoint entity, the signaling message comprising first establishment information indicating at least one range of protection to be granted, the range of protection relating to one of a plurality of network elements in at least one access network and at least
- 25 one core network and to a second endpoint entity;
- an obtainer configured to obtain, at a network element entity, from a second endpoint entity different from the first endpoint entity and based on the first establishment
- 30 information, second establishment information indicating protection granted by the second endpoint entity; and
- a signaler configured to signal, from the network element entity to the first endpoint entity, third establishment information indicating the protection granted
- 35 to the first endpoint entity.

[0108] According to an example of the present invention, in a sixth aspect, this object is for example achieved by an apparatus comprising:

5 a selector configured to select, at a first endpoint entity, at least one range of protection to be granted, the range of protection relating to one of a plurality of network elements in at least one access network and at least one core network and to a second endpoint entity; and
10 a transmitter configured to transmit, to a network element entity, a signaling message comprising first establishment information indicating the at least one range of protection to be granted.

[0109] According to further refinements of the example of the present invention as defined under the above fifth and sixth aspects,

- the first, second and third establishment information respectively relate to a data stream to be established;
- the first information comprises an explicit information element for indicating a desired type of the range of protection;
- one of the second and third establishment information comprises an explicit information element for indicating the granted protection;
- 25 - one of the first, second and third establishment information comprises an explicit information element for indicating the protection capabilities of one of the first endpoint entity, second endpoint entity and a network element entity respectively;
- 30 - no explicit information element indicating the range of protection is contained in the first establishment information;
- end-to-end security is configured to be established if possible, else end-to-middle security if possible, else no security;
- 35 - the first establishment information indicates one secured

data stream to be established and one unsecured data stream to be established, and the second and third establishment information indicates at least one of the secured data stream and the unsecured data stream;

5 - the secured data stream and the unsecured data stream are configured to be established as parallel data streams according to the indication in the first establishment information;

- the signaler is configured to repeat signaling with the

10 first establishment information indicating only the secured data stream;

- the signaler is configured to repeat signaling in case the second endpoint has signaled grant of both the secured and the unsecured data stream;

15 - the secured data stream and the unsecured data stream are configured to be signaled to be established as alternative data streams;

- the first and third establishment information indicate one secured data stream to be established, and the second

20 establishment information indicates an unsecured data stream;

- the apparatus further comprises a modifier configured to modify, in the first network element entity and upon receiving the first establishment information comprising an indication of the range of protection, the first

25 establishment information to indicate an unsecured data stream, wherein the modifying is performed prior to a transmission of the modified first establishment information to the second endpoint entity by the transmitter;

- the range of protection comprised in the first

30 establishment information is end-to-middle-only;

- the first establishment information indicates one secured data stream to be established, the second and third establishment information indicate failure, and wherein, after the signaling of the third establishment information

35 performed by the means for signaling, the receiver is configured to repeat receiving of the first establishment

information with a range of protection to be granted different from the range of protection to be granted which was used when having received the first establishment earlier;

- 5 - the range of protection comprised in the repeated first establishment information is end-to-middle-only;
- the third establishment information comprises capability information;
- the access network comprises one of session initiation
- 10 protocol proxy entities and session initiation protocol back-to-back user agents and the core network comprises internet protocol-internet protocol gateways;
- the internet protocol-internet protocol gateways are constituted by session border controllers;
- 15 - if the transmitter and the signaler are configured to perform based on a session initiation/description protocol, the establishment information messages are headed by a first code type indicating the requested type of data stream;
- the first code type is followed by a second code type
- 20 indicating the type of range of protection;
- the second code type is followed by a third code type indicating the protection capabilities;
- the core network comprises a signaling media relay which is configured to origin and terminate any security type for
- 25 data streams;
- the transmitter, the receiver and the signaler are configured to perform dynamically;
- the data streams are constituted by media streams;
- the types of range of protection comprise at least one of
- 30 best effort security, at least end-to-middle security, only end-to-middle security, and end-to-end security;
- the types of the protection capabilities comprise at least capable of end-to-middle security;
- the end-to-end security comprises a secured data stream
- 35 between the first and second endpoints;
- the end-to-middle security comprises a secured datastream

between the first endpoint and the network element entity and
an unsecured datastream between the network element entity
and the other endpoint;
- no security comprises an unsecured data stream between the
5 first and second endpoints;
- the network element entity is constituted by a signaling
and media relay entity;
- at least one of the first, second and third code types is
an extension to a session initiation/description protocol;
10 - at least one, or more of the transmitter, obtainer,
signaler, selector, establisher, modifier and the apparatus
is implemented as a chipset, module or subassembly.

[0110] According to an example of the present invention, in a
15 seventh aspect, this object is for example achieved by a
computer program product comprising code means for performing
a method according to the above first and second aspects.

[0111] According to an example of the present invention, in
20 an eighth aspect, this object is for example achieved by **a**
computer program comprising code means for executing, when
run on a computer:
receiving, at a network element entity, a signaling
message from a first endpoint entity, the signaling message
25 comprising first establishment information indicating at
least one range of protection to be granted, the range of
protection relating to one of a plurality of network elements
in at least one access network and at least one core network
and to a second endpoint entity;
30 obtaining, at a network element entity, from a second
endpoint entity different from the first endpoint entity and
based on the first establishment information, second
establishment information indicating protection granted by
the second endpoint entity; and
35 signaling, from the network element entity to the
first endpoint entity, third establishment information

indicating the protection granted to the first endpoint entity.

[0112] According to an example of the present invention, in a
5 ninth aspect, this object is for example achieved by a
computer program comprising code means for executing, when
run on a computer:
selecting, at a first endpoint entity, at least one
range of protection to be granted, the range of protection
10 relating to one of a plurality of network elements in at
least one access network and at least one core network and to
a second endpoint entity; and
transmitting, to a network element entity, a signaling
message comprising first establishment information indicating
15 the at least one range of protection to be granted.

[0113] According to an example of the present invention, in a
tenth aspect, this object is for example achieved by a system
comprising:
20 an apparatus according to the above third or fifth
aspects, and
an apparatus according to the above fourth or sixth
aspects.

25 [0114] Although the present invention has been described
herein before with reference to particular embodiments
thereof, the present invention is not limited thereto and
various modification can be made thereto.

CLAIMS:

1. A method, comprising:

receiving, at a network element entity, a signaling
5 message from a first endpoint entity, the signaling message
comprising first establishment information indicating at
least one range of protection to be granted, the range of
protection relating to one of a plurality of network elements
in at least one access network and at least one core network
10 and to a second endpoint entity;

obtaining, at a network element entity, from a second
endpoint entity different from the first endpoint entity and
based on the first establishment information, second
establishment information indicating protection granted by
15 the second endpoint entity; and

signaling, from the network element entity to the
first endpoint entity, third establishment information
indicating the protection granted to the first endpoint
entity.

20

2. A method, comprising:

selecting, at a first endpoint entity, at least one
range of protection to be granted, the range of protection
relating to one of a plurality of network elements in at
25 least one access network and at least one core network and to
a second endpoint entity; and

transmitting, to a network element entity, a signaling
message comprising first establishment information indicating
the at least one range of protection to be granted.

30

3. The method according to claim 1 or 2, wherein the first,
second and third establishment information respectively
relate to a data stream to be established.

35 4. The method according to any one of claims 1 to 3, wherein
the first information comprises an explicit information

element for indicating a desired type of the range of protection.

5 5. The method according to any one of claims 1 to 4, wherein one of the second and third establishment information comprises an explicit information element for indicating the granted protection.

10 6. The method according to any one of claims 1 to 3, wherein one of the first, second and third establishment information comprises an explicit information element for indicating the protection capabilities of one of the first endpoint entity, second endpoint entity and a network element entity respectively.

15 7. The method according to any one of claims 1 to 3, wherein no explicit information element indicating the range of protection is contained in the first establishment information.

20 8. The method according to any one of claims 1 to 3, wherein end-to-end security is established if possible, else end-to-middle security if possible, else no security.

25 9. The method according to any one of claims 1 to 8, wherein the first establishment information indicates one secured data stream to be established and one unsecured data stream to be established, and the second and third establishment information indicates at least one of the secured data stream and the unsecured data stream.

30 10. The method according to claim 9, wherein the secured data stream and the unsecured data stream are to be established as parallel data streams according to the indication in the first establishment information.

11. The method according to claim 9 or 10, wherein the signaling is repeated with the first establishment information indicating only the secured data stream.

5 12. The method according to claim 11, wherein the signaling is repeated in case the second endpoint has signaled grant of both the secured and the unsecured data stream.

13. The method according to claim 9, wherein the secured data stream and the unsecured data stream are signaled to be established as alternative data streams.

14. The method according to any one of claims 1 to 5, wherein the first and third establishment information indicate one secured data stream to be established, and the second establishment information indicates an unsecured data stream.

15. The method according to claim 14, further comprising, in the first network element entity and upon receiving the first establishment information comprising an indication of the range of protection, modifying the first establishment information to indicate an unsecured data stream, wherein the modifying is performed prior to a transmission of the modified first establishment information to the second endpoint entity.

16. The method according to claim 15, wherein the range of protection comprised in the first establishment information is end-to-middle-only.

17. The method according to any one of claims 1 to 5, wherein the first establishment information indicates one secured data stream to be established, the second and third establishment information indicate failure, and wherein after signaling of the third establishment information, the receiving comprises a repeated receiving of the first

establishment information with a range of protection to be granted different from the range of protection to be granted which was used when having received the first establishment earlier.

5

18. The method according to claim 17, wherein the range of protection comprised in the repeated first establishment information is end-to-middle-only.

10 19. The method according to claim 17 or 18, wherein the third establishment information comprises capability information.

20. The method according to any one of claims 3 to 19, wherein, if the transmitting and the signaling are based on a session initiation/description protocol, the establishment
15 information messages are headed by a first code type indicating the requested type of data stream.

21. The method according to claim 20, wherein the first code
20 type is followed by a second code type indicating the type of range of protection.

22. The method according to claim 21, wherein the second code type is followed by a third code type indicating the
25 protection capabilities.

23. The method according to any one of claims 1 to 22, wherein at least one of the following applies:

- the transmitting, receiving and signaling are
30 performed dynamically;
- the data streams are constituted by media streams;
- the types of range of protection comprise at least one of best effort security, at least end-to-middle security, only end-to-middle security, and end-to-end security;
- 35 the types of the protection capabilities comprise at least capable of end-to-middle security;

the end-to-end security comprises a secured data stream between the first and second endpoints;

the end-to-middle security comprises a secured datastream between the first endpoint and the network element entity and an unsecured datastream between the network
5 element entity and the other endpoint;

no security comprises an unsecured data stream between the first and second endpoints;

the network element entity is constituted by a
10 signaling and media relay entity;

at least one of the first, second and third code types is an extension to a session initiation/description protocol.

24. An apparatus, comprising:

15 means for receiving, at a network element entity, a signaling message from a first endpoint entity, the signaling message comprising first establishment information indicating at least one range of protection to be granted, the range of protection relating to one of a plurality of network elements
20 in at least one access network and at least one core network and to a second endpoint entity;

means for obtaining, at a network element entity, from a second endpoint entity different from the first endpoint entity and based on the first establishment information,
25 second establishment information indicating protection granted by the second endpoint entity; and

means for signaling, from the network element entity to the first endpoint entity, third establishment information indicating the protection granted to the first endpoint
30 entity.

25. An apparatus, comprising:

means for selecting, at a first endpoint entity, at least one range of protection to be granted, the range of
35 protection relating to one of a plurality of network elements

in at least one access network and at least one core network and to a second endpoint entity; and

means for transmitting, to a network element entity, a signaling message comprising first establishment information
5 indicating the at least one range of protection to be granted.

26. The apparatus according to claim 1 or 2, wherein the first, second and third establishment information
10 respectively relate to a data stream to be established.

27. The apparatus according to any one of claims 24 to 26, wherein the first information comprises an explicit information element for indicating a desired type of the
15 range of protection.

28. The apparatus according to any one of claims 24 to 27, wherein one of the second and third establishment information comprises an explicit information element for indicating the
20 granted protection.

29. The apparatus according to any one of claims 24 to 26, wherein one of the first, second and third establishment information comprises an explicit information element for
25 indicating the protection capabilities of one of the first endpoint entity, second endpoint entity and a network element entity respectively.

30. The apparatus according to any one of claims 24 to 26, wherein no explicit information element indicating the range of protection is contained in the first establishment
30 information.

31. The apparatus according to any one of claims 24 to 26, wherein end-to-end security is configured to be established
35

if possible, else end-to-middle security if possible, else no security.

32. The apparatus according to any one of claims 24 to 31,
5 wherein the first establishment information indicates one secured data stream to be established and one unsecured data stream to be established, and the second and third establishment information indicates at least one of the secured data stream and the unsecured data stream.

10

33. The apparatus according to claim 32, wherein the secured data stream and the unsecured data stream are configured to be established as parallel data streams according to the indication in the first establishment information.

15

34. The apparatus according to claim 32 or 33, wherein the means for signaling is configured to repeat signaling with the first establishment information indicating only the secured data stream.

20

35. The apparatus according to claim 34, wherein the means for signaling is configured to repeat signaling in case the second endpoint has signaled grant of both the secured and the unsecured data stream.

25

36. The apparatus according to claim 32, wherein the secured data stream and the unsecured data stream are configured to be signaled to be established as alternative data streams.

30 37. The apparatus according to any one of claims 24 to 28, wherein the first and third establishment information indicate one secured data stream to be established, and the second establishment information indicates an unsecured data stream.

35

38. The apparatus according to claim 37, further comprising means for modifying, in the first network element entity and upon receiving the first establishment information comprising an indication of the range of protection, the first
5 establishment information to indicate an unsecured data stream, wherein the modifying is performed prior to a transmission of the modified first establishment information to the second endpoint entity by the means for transmitting.
- 10 39. The apparatus according to claim 38, wherein the range of protection comprised in the first establishment information is end-to-middle-only.
40. The apparatus according to any one of claims 24 to 28,
15 wherein the first establishment information indicates one secured data stream to be established, the second and third establishment information indicate failure, and wherein, after the signaling of the third establishment information performed by the means for signaling, the means for receiving
20 is configured to repeat receiving of the first establishment information with a range of protection to be granted different from the range of protection to be granted which was used when having received the first establishment earlier.
- 25 41. The apparatus according to claim 40, wherein the range of protection comprised in the repeated first establishment information is end-to-middle-only.
- 30 42. The apparatus according to claim 40 or 41, wherein the third establishment information comprises capability information.
43. The apparatus according to any one of claims 24 to 42 to
35 42, wherein the access network comprises one of session initiation protocol proxy entities and session initiation

protocol back-to-back user agents and the core network comprises internet protocol-internet protocol gateways.

44. The apparatus according to claim 43, wherein the internet
5 protocol-internet protocol gateways are constituted by session border controllers.

45. The apparatus according to any one of claims 26 to 44,
wherein, if the means for transmitting and the means for
10 signaling are configured to perform based on a session initiation/description protocol, the establishment information messages are headed by a first code type indicating the requested type of data stream.

46. The apparatus according to claim 45, wherein the first
15 code type is followed by a second code type indicating the type of range of protection.

47. The apparatus according to claim 46, wherein the second
20 code type is followed by a third code type indicating the protection capabilities.

48. The apparatus according to any one of claims 24 to 47,
wherein the core network comprises a signaling media relay
25 which is configured to origin and terminate any security type for data streams.

49. The apparatus according to any one of claims 24 to 48,
wherein at least one of the following applies:
30 the means for transmitting, means for receiving and means for signaling are configured to perform dynamically;
 the data streams are constituted by media streams;
 the types of range of protection comprise at least one
of best effort security, at least end-to-middle security,
35 only end-to-middle security, and end-to-end security;

the types of the protection capabilities comprise at least capable of end-to-middle security;

the end-to-end security comprises a secured data stream between the first and second endpoints;

5 the end-to-middle security comprises a secured datastream between the first endpoint and the network element entity and an unsecured datastream between the network element entity and the other endpoint;

10 no security comprises an unsecured data stream between the first and second endpoints;

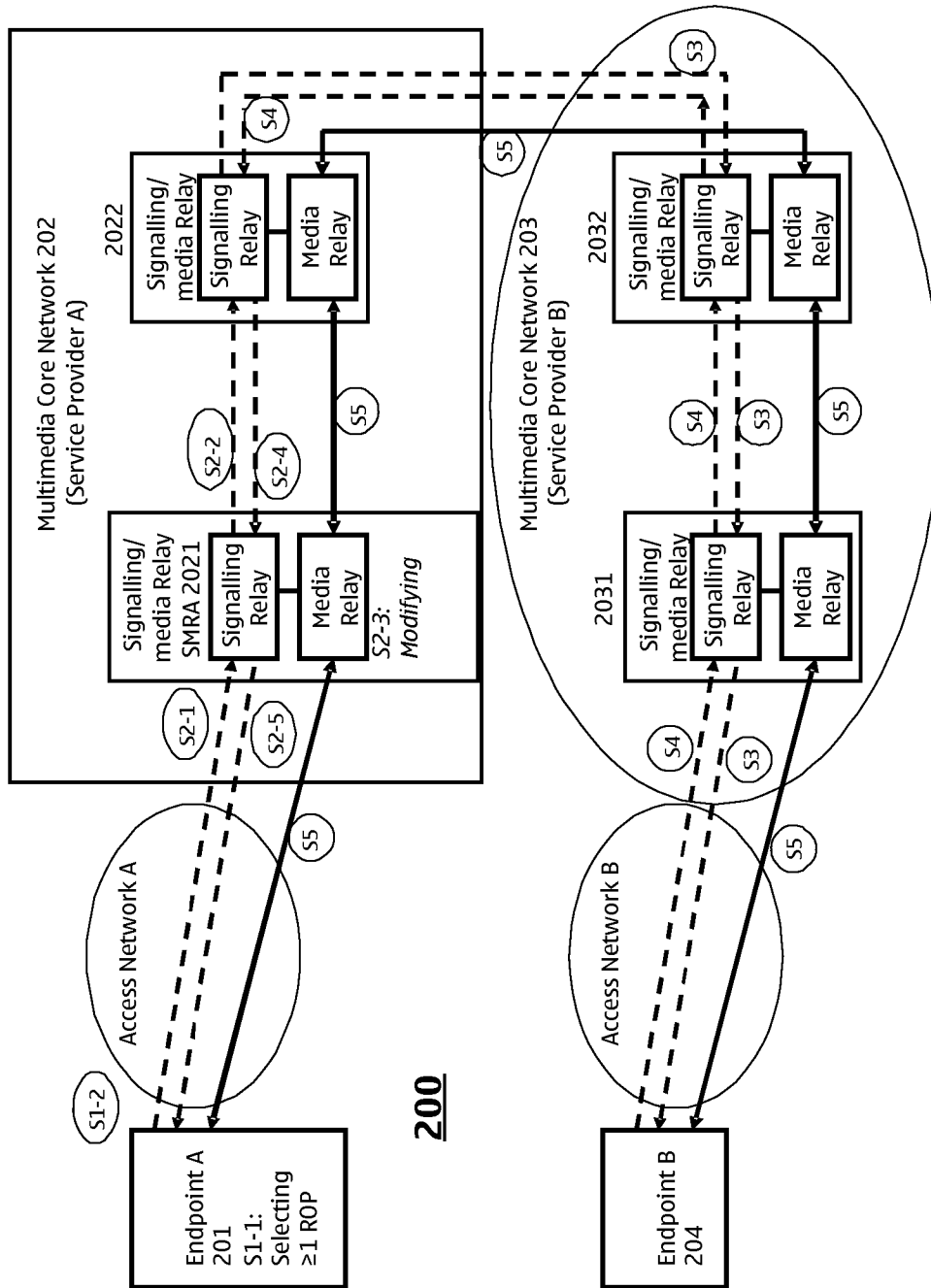
the network element entity is constituted by a signaling and media relay entity;

15 at least one of the first, second and third code types is an extension to a session initiation/description protocol.

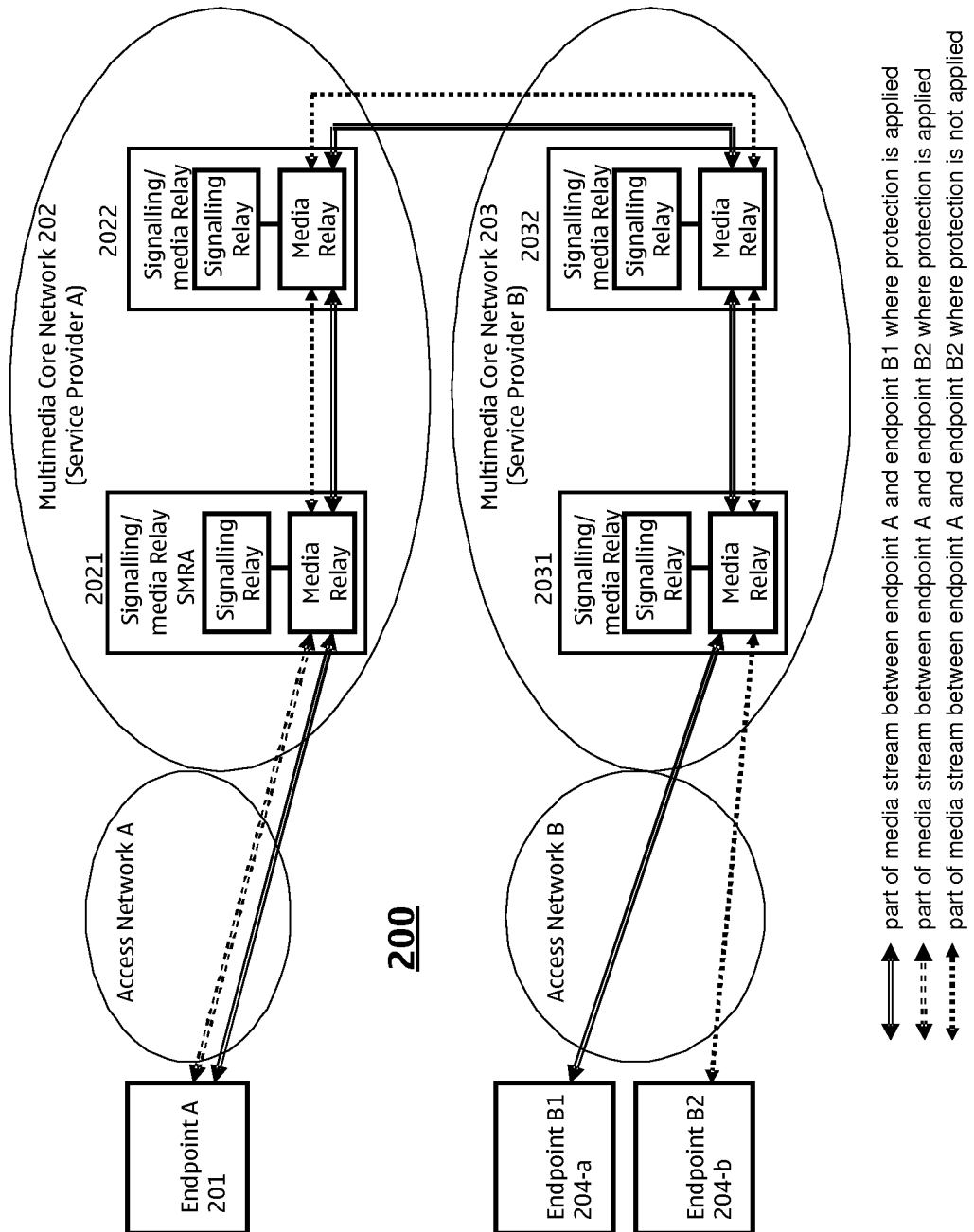
50. The apparatus according to any one of claims 24 to 49, wherein at least one, or more of means for receiving, means for obtaining, means for signaling, means for selecting, means for transmitting, means for establishing, means for
20 modifying and the apparatus is implemented as a chipset, module or subassembly.

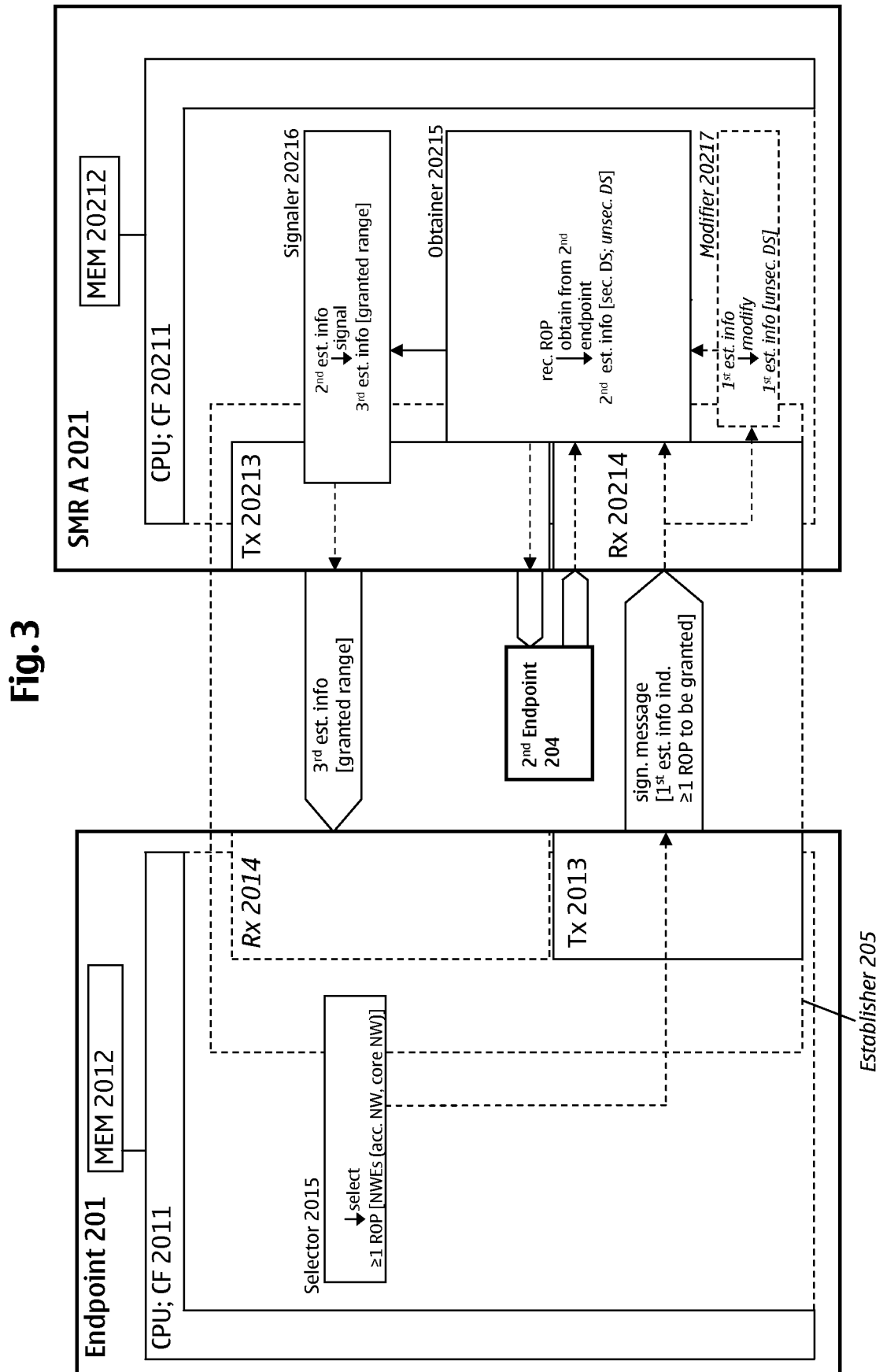
51. A computer program product comprising code means for performing a method according to any one of claims 1 to 23
25 when run on a processing means or module.

Fig.1



200

Fig. 2



INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2009/057203

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L29/06 H04L12/22
ADD.

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)
H04L

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2009/068985 A2 (ERICSSON TELEFON AB L M [SE]; BARRIGA LUIS [SE]; BLOM ROLF [SE]; CHENG) 4 June 2009 (2009-06-04) page 3, line 6 - page 5, line 1 -----	1-51
X	GB 2 411 554 A (TOSHIBA RES EUROP LTD [GB]) 31 August 2005 (2005-08-31) pages 4-5 -----	1-51
X	WO 01/08377 A2 (NORTEL NETWORKS CORP [CA]; RAO SANJAY H [US]; OXENDINE KENNETH W [US]) 1 February 2001 (2001-02-01) page 2, line 16 - page 3, line 11 -----	1-51

☐ 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
- *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.
- *G* document member of the same patent family

Date of the actual completion of the international search

7 July 2010

Date of mailing of the international search report

15/07/2010

Name and mailing address of the ISA/

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

Authorized officer

Veen, Gerardus

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2009/057203

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 2009068985	A2	04-06-2009	NONE		

GB 2411554	A	31-08-2005	NONE		

WO 0108377	A2	01-02-2001	AU	6223300 A	13-02-2001
			CA	2343066 A1	01-02-2001
			DE	60011875 D1	05-08-2004
			DE	60011875 T2	16-12-2004
			EP	1145521 A2	17-10-2001
			US	6757823 B1	29-06-2004
