



(51) International Patent Classification:

H04L 29/06 (2006.01) *H04L 29/08* (2006.01)
H04L 9/00 (2006.01) *H04W 12/06* (2009.01)

(21) International Application Number:

PCT/SE2017/050648

(22) International Filing Date:

16 June 2017 (16.06.2017)

(25) Filing Language:

English

(26) Publication Language:

English

(71) Applicant: **TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)** [SE/SE]; 164 83 Stockholm (SE).

(72) Inventor: **MARTINEZ MINGUITO, Julio**; Lindboda-
gränd 7, 125 58 Älvsjö (SE).

(74) Agent: **SJÖBERG, Mats**; Ericsson AB, Patent Unit Kista,
RAN Implementation & Core (PU-KRIC), 164 80 Stock-
holm (SE).

SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ,
UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,
TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,
EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,
MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,
TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
KM, ML, MR, NE, SN, TD, TG).

Published:

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

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

(54) Title: MEDIA PROTECTION WITHIN THE CORE NETWORK OF AN IMS NETWORK

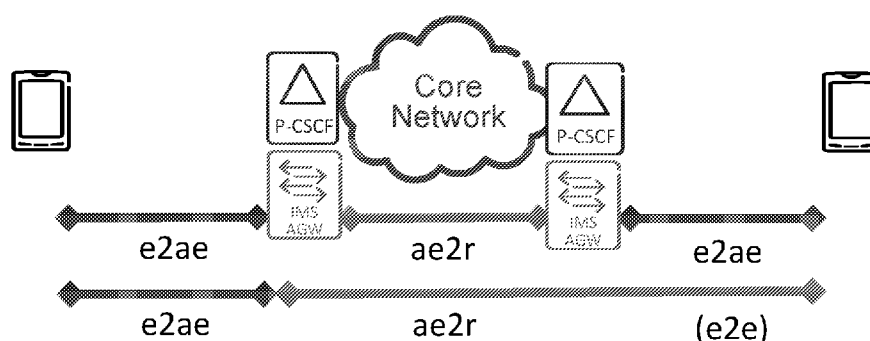


Figure 3

(57) Abstract: A method of securing media across an IP Multimedia Subsystem, IMS, network where the media transits via first and second media gateway functions of the IMS network which are controlled by respective first and second media gateway controllers acting as back-to-back Session Initiation Protocol, SIP, user agents. The method comprises sending from the first media gateway controller to the second media gateway controller, or to a node upstream of the second media gateway controller, security information of the first media gateway function, and using the sent information to secure media between the first and second media gateway functions or between the first media gateway function and said upstream node.



MEDIA PROTECTION WITHIN THE CORE NETWORK OF AN IMS NETWORKTechnical Field

5

The present invention relates to a method and apparatus for establishing a secure media session in a communications network within an IP Multimedia Subsystem (IMS) network. More particularly, the invention relates to establishing a media session for transmitting media securely between two media gateway functions within an IMS network.

10

Background

15

The Internet Protocol (IP) Multimedia Subsystem (IMS) is a well-known Third Generation Partnership Project (3GPP) standard allowing sessions to be set up between two or more parties for a broad variety of services such as voice or video call, interactive messaging sessions or third party specific applications. A few common enablers are defined by 3GPP for common usage among all these services. Examples on such enablers are capability discovery and subscribing to conference events to be used by for example an ad-hoc voice call conference for clients/devices to identify who leaves and enters the conference.

20

25

The protocol chosen by 3GPP is the Session Initiation Protocol (SIP). SIP is an application layer protocol used for controlling multimedia sessions over IP networks. It is a text based protocol which uses the request/response model. SIP defines messages sent between endpoints, which govern establishment, termination and other essential elements of a multimedia connection. SIP can be used for creating, modifying and terminating sessions consisting of one or more media streams. It can be both unicast and multicast. Examples of applications which SIP can establish and control are video conferencing, streaming multimedia distribution, instant messaging, presence information, file transfer, fax over IP and online games.

30

35

SIP provides a mechanism for the registration of user agents and for setting up multimedia sessions. The SIP REGISTER method enables the registration of a user agent's current location and the INVITE method enables the setting up of a session.

SIP does not only allow the registration of users and the set-up of connections. Modification of sessions is also possible, such as adding media to a session or new user agents joining multicast sessions such as video conferencing. In order to assist a user agent in discovering the capabilities of other user agents and events that occur within the session, a number of other SIP methods have been developed. The SIP OPTIONS method enables a user agent to query another user agent or proxy server about its capabilities. This allows a client to discover information about supported methods, content types, extensions, codecs etc. The SUBSCRIBE method is used to request asynchronous notification of an event or set of events at a later time. It is complemented by the NOTIFY command by which these notifications are enacted.

Although SIP enablers such as SUBSCRIBE and OPTIONS are powerful, they are also resource intensive and use valuable signalling bandwidth. IMS separates the control functions and the user traffic, and resource intensive methods such as those used by SIP can place a strain on resources dedicated to signalling within the IMS. For example, signalling must be routed through the home network. Acknowledgement and retransmission messages as well as provisional responses are incorporated in SIP which increase the amount of signalling required. In addition, new logic and commands for networks can only be developed through the standardisation process.

The Session Description Protocol (SDP) is used within SIP signalling to describe and negotiate the media components of the session. Whilst SIP was created as a user-to-user protocol, IMS allows operators and service providers to control user access to services and to charge users accordingly. The 3GPP has chosen SIP for signalling between a User Equipment (UE) and the IMS as well as between the components within the IMS. The term UE is used here as it is defined by 3GPP, or evolutions thereof.

By way of example, Figure 1 illustrates schematically how the IMS fits into the mobile network architecture in the case of a GPRS/PS access network (IMS can of course operate over other access networks). Call/Session Control Functions (CSCFs) operate as SIP proxies within the IMS. The 3GPP architecture defines three types of CSCFs: the Proxy CSCF (P-CSCF) which is the first point of contact within the IMS for a SIP terminal; the Serving CSCF (S-CSCF) which provides services to the user that the user is subscribed to; and the Interrogating CSCF (I-CSCF) whose role is to identify the

correct S-CSCF and to forward to that S-CSCF a request received from a SIP terminal via a P-CSCF.

5 When the access networks are not trusted, media protection can be negotiated to ensure secure transmission of media: (1) from terminal to the access edge of the network (e2ae), i.e. from a user device to an access gateway of the IMS, thereby protecting only the access segment; or (2) "end to end" (e2e) to protect the media from the originating terminal, all the way to the terminating terminal. These two cases are illustrated in Figure 2.

10

The capabilities of the terminals are indicated during the SIP registration, and the networks may have policies for which methods are supported. Whilst it is usual for the access networks to be untrusted, the core network is often assumed to be trusted, making media protection within this part of the network unnecessary. However, with the deployment of telecommunication networks in cloud environments, operators of the media services may no longer be in control of the core infrastructure. Instead, control of a portion of, or indeed the whole of, the core network and its architecture may be delegated to third parties. As a consequence, the core network may not be trusted for transmission of media. For example, media transmitted over the core network may be vulnerable to eavesdropping or man-in-the-middle attacks, i.e. the privacy, integrity or authenticity of the media cannot be guaranteed.

20

It is therefore desirable that protection for media be provided in order to provide users of the IMS network with assurance that their media communications remain authentic and/or confidential. In some circumstances, end-to-end protection (e2e) of the media may be appropriate; however, this type of protection may hinder, or be incompatible with, some important network functionalities. For example, media transcoding may not be possible with e2e protection, which is problematic for transmission of media over networks which use different codecs. Lawful Interception of the protected media by law enforcement agencies, which may be a legal requirement in some jurisdictions, may also not be possible when e2e protection is used.

30

Summary

35

According to a first aspect of the present invention there is provided a method of securing media across an IP Multimedia Subsystem, IMS, network where the media

transits via first and second media gateway functions of the IMS network which are controlled by respective first and second media gateway controllers acting as back-to-back Session Initiation Protocol, SIP, user agents. The method comprises sending from the first media gateway controller to the second media gateway controller, or to a node upstream of the second media gateway controller, security information of the first media gateway function, and using the sent information to secure media between the first and second media gateway functions or between the first media gateway function and said upstream node.

10 The term "Media gateway controller" as used here encompasses nodes including, but not limited to; P-CSCF, IMS-ALG, IBCF, MGCF, and MRFC. Similarly, the term "media gateway function" encompasses nodes including, but not limited to; BGF, IMS AGW, TrGW, and MRFP

15 The method may comprise, at the first media gateway controller, receiving, from the second media gateway controller, further security information of the second media gateway function or said upstream node and using the further security information to secure media between the first and second media gateway functions or between the first media gateway function and said upstream node. The security information and
20 the further security information is used to negotiate one or more encryption keys and using the key(s) to secure the media.

By way of example, the key negotiation may use a Session Description Security Descriptions, SDDES, protocol or a Datagram Transport Layer Security, DTLS, protocol.

25 The method may comprise, at the first media gateway function, receiving media secured using the security information of the first media gateway from the second media gateway function or said upstream node and removing the security from the received media.

30 By way of example, the first and/or second media gateway controller may be a Proxy Call Session Control Function, P-CSCF, an Interconnection Border Control Function, IBCF, or a Media Gateway Control Function, MGCF.

Where the method involves said upstream node, the second media gateway controller may be a Media Resource Function Controller, MRFC and said upstream node may be a Media Resource Function Processor, MRFP.

- 5 Where the method involves said upstream node, said upstream node may be a User Equipment, UE.

By way of example, the security information of the first media gateway function may be sent in a SIP INVITE or SIP UPDATE message. The further security information may
10 be sent in a SIP 18x series or a SIP 200 response message.

The method may comprise receiving, at the second media gateway controller, from the first media gateway controller, the security information of the first media gateway function and data indicating which of the second media gateway function or said
15 upstream node should be sent the security information. The method may further comprise, at the second media gateway controller, obtaining the further security information from either the second media gateway function or said upstream node according to said indicator.

20 According to a second aspect of the present invention there is be provided an apparatus configured to operate as a media gateway controller acting as a back-to-back Session Initiation Protocol, SIP, user agent controlling a media gateway function of an IP Multimedia Subsystem, IMS, network. The apparatus comprises processor circuitry, a storage unit storing instructions executable by the processor circuitry, a
25 receiver for receiving messages and a transmitter for sending messages, whereby the apparatus is operable to:

send security information of the media gateway function to another media gateway controller acting as a back-to-back SIP user agent controlling another media gateway function of the IMS network, or to a node upstream of the other media
30 gateway controller; and

configure the media gateway function to remove the security from media secured using the security information received from the other media gateway function or upstream node.

35 The apparatus may be operable to receive security information of the other media gateway function or said upstream node, send the security information to the media

gateway function, and configure the media gateway function to secure media using the security information for sending to the other media gateway function or said upstream node.

- 5 The apparatus may be operable to send the security information to the media gateway function in response to receiving an 18x series answer containing the security information.

10 According to a third aspect of the present invention there is provided an apparatus configured to operate as a media gateway controller acting as a back-to-back Session Initiation Protocol, SIP, user agent controlling a media gateway function of an IP Multimedia Subsystem, IMS, network. The apparatus comprises processor circuitry, a storage unit storing instructions executable by the processor circuitry, a receiver for receiving messages and a transmitter for sending messages, whereby the apparatus is
15 operable to:

 receive security information of another media gateway function of the IMS network controlled by a media gateway controller acting as a back-to-back SIP user agent;

 send the security information to either the media gateway function or to a node
20 upstream of the media gateway controller; and

 configure the media gateway function or a node upstream of the media gateway controller to use the security information to secure media for sending to the media gateway.

- 25 The apparatus may be operable to send the security information in response to receiving a SIP INVITE or SIP UPDATE containing the security information. The apparatus may also be operable to receive an indicator specifying which of the second media gateway function or said upstream node to send the security information, and send the security information to the second media gateway function or said upstream
30 node according to said indicator.

 The apparatus may be operable to obtain security information from either the media gateway function or the node upstream of the media gateway controller according to said indicator and send the obtained security information to the other media gateway
35 function.

The apparatus may be configured to operate as a Proxy Call Session Control Function, P-CSCF, an Interconnection Border Control Function, IBCF, a Media Resource Function Controller, MRFC, or a Media Gateway Control Function, MGCF.

5 Brief description of the drawings

Figure 1 illustrates schematically an IMS network integrated into a communications system comprising a 3G network;

10 Figure 2 illustrates schematically a known system providing access network media protection;

Figure 3 illustrates schematically a system for core IMS network media protection according to an embodiment of the present invention;

Figure 4 illustrates schematically the system of Figure 3 in more detail;

15 Figure 5 illustrates schematically a system for core IMS network media protection in the case where there are two core IMS networks;

Figure 6 shows signalling associated with a procedure for establishing a secure media session between two UEs;

Figure 7 shows signalling associated with a procedure for establishing a secure media session between a UE and a Media Resource Function, MRF;

20 Figure 8 shows signalling associated with an alternative procedure for establishing a secure media session between two UEs;

Figure 9 shows signalling associated with a procedure for establishing a secure media session between two UEs;

25 Figure 10 shows signalling associated with a procedure for establishing a secure media session between a UE and a Media Resource Function, MRF;

Figure 11 is a flow diagram illustrating a method carried out by a back-to-back user agent of an IMS network;

Figure 12 is a flow diagram illustrating a method carried out by a back-to-back user agent of an IMS network; and

30 Figure 13 is a schematic diagram of a Control Function apparatus.

Detailed description

35 Embodiments will now be described more fully below with reference to the accompanying drawings, in which certain embodiments are shown. However, other embodiments in many different forms are possible within the scope of the present

disclosure. Rather, the following embodiments are provided by way of example so that this disclosure will be thorough and complete, and will fully convey the scope of the disclosure to those skilled in the art.

5 In order to address the problems discussed above, the present invention provides protection of media transmitted across the core network which is separate from the media protection provided for by the access networks. Figure 3 shows schematically a system which provides two ways of implementing this type of media protection. In this example, the system comprises two P-CSCFs, each controlling an Access Gateway
10 (AGW) of an IMS comprising an untrusted core network. In use, an originating UE connects to one of the P-CSCFs over an access network in order to establish a media session with a terminating UE, connected to the other P-CSCF. The UEs then connect via one or both of the AGWs to establish a media session, i.e. the AGWs provide an access edge of the core network.

15

As discussed in more detail below, media protection may, in general, refer to methods for ensuring that the media is transmitted securely between two parts of the network, without an unauthorised party being able to, for example, access or modify the media. For example, media may be protected by encryption, using for example a symmetric
20 encryption technique such as Secure Real-Time Transport Protocol, of the media. Other encryption techniques may also be used of course including asymmetric techniques (e.g. involving the use of public-private key pairs).

20

In the first use case (shown in the upper scheme in Figure 3), the media is protected
25 piecewise across the network from:

25

- originating UE to originating network access edge (e2ae);
- originating network access edge to terminating network access edge, i.e. protection in the core network, from “access edge to remote” (ae2r); and
- terminating network access edge to terminating UE (e2ae).

30

When the media is protected using encryption, the media can be decrypted in the originating access edge, by a Border Gateway Function (BGF) for example, where network functions such as transcoding and Lawful Intercept can be performed if needed. As the BGF are under the control of the operator providing the media service,
35 these network functions can be performed without the need to expose the decrypted media to the core network. The media is subsequently encrypted again before

35

transmission via the core network. The same operations may be performed on the terminating access edge. As a result, all media can be protected during transit with encryption, whilst the network can still perform needed functionality on the media.

5 In the second use case (shown in the lower scheme of Figure 3), the media is protected from: originating UE to originating network access edge (e2ae), and then from terminating network access edge to terminating UE (ae2r). This use case may be selected when one of the UE supports e2ae and the other UE supports e2e encryption, the end-to-end protection in this case being terminated in the access edge instead of
10 the remote UE.

Figure 4 illustrates the system in Figure 3 in more detail. The two P-CSCFs in the signalling plane of the IMS core network communicate via an S-CSCF, which is allocated to handle the signalling to/from the UEs and which may provide services to
15 the UEs using an Application Server (AS). As discussed above, the AGWs each comprise a BGF, which is used to convert between the forms of media protection used for each of the access and core networks. For example, the BGF of the originating network access edge provides a termination point, T1, at which the e2ae protection is removed from the media. At another termination point of the BGF, T2, the ae2r
20 protection is applied so that the media can be transmitted securely across the core network to the BGF terminating network access edge. Here, the ae2r protection is removed at a termination point, T3, before e2ae protection is then applied for transmission of the media to the terminating UE. The media protection at each stage may, for example, make use of the Secure Real-Time Transport Protocol (SRTP) in
25 order to guarantee integrity and confidentiality of media data exchanged by the UEs.

Figure 5 illustrates schematically how the system of Figures 3 and 4 can be extended for use when there are two core IMS networks. A similar approach can of course be used when there are three or more core IMS networks. In this example, the core
30 networks are joined in the signalling plane by respective Interconnection Border Control Functions, IBCFs, and in the media plane by respective Transition Gateways, TrGWs. The media is protected as it is transmitted between the TrGWs, i.e. media transmitted securely across one of the core networks is de-protected by the TrGW at the network edge and subsequently protected for transmission to the other TrGW, which de-
35 protects the media and then applies protection suitable for transmission of the media across the other core network.

Figure 6 illustrates a signalling flow sequence associated with configuring the IMS to support media encryption within the core IMS network. In this example, the signalling is based on the Session Initiation Protocol (SIP). The basic commands used to set up a media session are the REGISTER method and the INVITE method. The REGISTER method allows a user agent to register its location with a registrar server. The INVITE method is the method by which a session is established with another user agent. Other methods in support of these basic commands include the acknowledgement response (ACK), the CANCEL request, and the BYE request to end participation in a session.

Step 1 is a standard procedure in which an originating UE sends a SIP INVITE to a P-CSCF in order to establish a media session. The SIP INVITE message contains Session Description Protocol (SDP) fields which indicate parameters associated with the media session and cryptographic information (crypto UE), such as a public encryption key for the UE or a reference to such a key, which is necessary to establish secure communication from the IMS to the UE over the access network (3g2ae).

In step 2, the P-CSCF sends a pair of SIP REQUESTs to an IMS access gateway (IMS-AGW) to request that the IMS-AGW add an access termination (T1) for communication between the UE and the IMS-AGW, and a core media termination (T2) for communication to/from the IMS-AGW across the IMS core network. In both ADD requests, the P-CSCF also requests encryption capabilities be reserved at the IMS-AGW to allow media to be communicated securely to each termination (T1, T2). In response, step 3, the IMS-AGW sends a pair of REPLY messages to the P-CSCF: each message contains local media parameters for the IMS-AGW and cryptographic information, e.g. a public key, for the one of the terminations (T1, T2).

In step 4, the P-CSCF indicates toward the IMS core a request to encrypt the core media using the encryption key of the core media termination (T2). This is done by the P-CSCF sending a SIP INVITE to the S-CSCF to establish a media session originating at the termination (T2). The SDP fields of the SIP INVITE include parameters associated with the media session, the encryption key for T2 and a new indicator "ae2r" which indicates the need for encryption of the core media whilst explicitly indicating that the media protection is not e2e. The SIP INVITE is then forwarded by the S-CSCF (step 5), via an Application Server (AS) (step 6), to a

second P-CSCF. This P-CSCF then transmits a pair of ADD requests to a second IMS-AGW in order to set up a core media termination (T3) and an access termination (T4) in the second IMS-AGW (step 7). The request for the new core media termination (T3) includes the encryption key (or a reference to the encryption key) for T2, which is then stored by the IMS-AGW so that the new core media termination can encrypt media which is to be received by T2. In step 8, cryptographic information for the terminations (T3, T4) is returned to the P-CSCF.

In step 9, a SIP INVITE is sent from the P-CSCF to a terminating UE in order to establish a media session between the access termination (T4) and the terminating UE. The SDP fields of the SIP INVITE message indicate media information of the access termination (T4), together with cryptographic information to enable the terminating UE to transmit media securely to the access termination over the access network (as designated by the indicator "3g2ae" included in the invite message). The terminating UE responds, via an SDP answer (step 10), with its own media and cryptographic information. The P-CSCF then sends a MODIFY request to the second IMS-AGW so that the access termination (T4) can be configured to use the media information and cryptographic information of the terminating UE.

In steps 12 to 14, the second P-CSCF sends an 18x series answer message to the first P-CSCF (step 14), via the S-CSCF (step 12) and the AS (step 13). The SDP fields of the answer message contain the media information and cryptographic information of the core termination (T3), together with the new indicator "ae2r" to indicate the need for encryption of the core media. The P-CSCF then sends (step 15) a MODIFY request to the first IMS-AGW so that the core termination (T2) can be configured to use the media information and cryptographic information of the core termination (T3) at the second IMS-AGW. The first P-CSCF also sends (step 16) a SIP answer message to the originating UE containing the media information and cryptographic information for the access termination (T1) of the first IMS-AGW.

Step 16 completes the media anchoring so that media can be transmitted between the originating and terminating UEs whilst remaining encrypted as it traverses both the access networks (a2ae encryption) and the core IMS network (ae2r encryption). For example, the originating UE encrypts media using the key negotiated with the access termination (T1) in the first IMS-AGW. The encrypted media is then transmitted via the access network of the first UE to the IMS-AGW, where it is

decrypted and then re-encrypted using the key negotiated with the core termination (T3) in the second IMS-AGW. The encrypted media is then transmitted via the IMS core network to the second IMS-AGW where it is decrypted at core termination (T3) and then re-encrypted using the key negotiated with the terminating UE. Finally, the encrypted media is sent over the access network of the terminating UE and then decrypted by the terminating UE. A similar process occurs when encrypted media is sent from the terminating UE to the originating UE using the keys negotiated for each segment to ensure that the media remains encrypted as it moves between untrusted network entities.

Figure 7 shows signaling for establishing a secure media session between a UE and a Media Resource Function Processor (MRFP), rather than a terminating UE as in Figure 6. In this example, a Media Resource Function Controller (MRFC) takes the place of one of the P-CSCFs. A second IMS-AGW is not needed as a media session can be established directly between the MRFP and the IMS-AGW to which the UE is connected. The signaling is similar to that in Figure 6 except that only a single termination (T3) is established in the MFRP in order for the MFRP to communicate securely with the IMS-AGW.

Figure 8 shows signaling for establishing a secure media session between two UEs, in which the terminating UE requested e2e protection, as already discussed above in relation to Figure 3. In this example, steps 1 to 6 are identical to those of Figure 6. In steps 7 and 8, terminations T3 and T4 are set up at the second IMS-AGW without encryption capabilities. In step 9, the SIP INVITE is sent from the P-CSCF to the terminating UE with the encryption key for termination T2 to enable the terminating UE to transmit media securely to the first IMS-AGW across both its access network and the core network. At step 10, the terminating UE sends an SDP answer to the second P-CSCF with its own media and cryptographic information. The P-CSCF then sends, in step 11, a MODIFY request to the second IMS-AGW so that the access termination (T4) can be configured to use the media information of the terminating UE. Steps 12 to 16 are equivalent to those of Figure 6, except that the cryptographic information of the terminating UE is sent in place of any cryptographic information for termination T3.

In the examples above, the cryptographic protection is negotiated using Session Description Security Descriptions (SDS), but the same principles can be used when

negotiating keys using the Datagram Transport Layer Security/Secure Real-Time Transport Protocol (DTLS/SRTP).

Figure 9 shows signaling which uses DTLS to establish a secure media session between two UEs. Steps 1 to 11 are similar to those of Figure 6, except that the messages sent between the devices include a fingerprint (taken across certificates used in the DTLS negotiation in the media plane), in place of cryptographic information, together with an indicator "dtls" (in reality "UDP/TLS/RTP/SAVP") that key negotiation should use DTLS. For example, in step 9, the terminating P-CSCF (P-CSCF term) sends an INVITE to the terminating UE (UE2) which includes the fingerprint of the terminating IMS-AGW (IMS-AGW term). In response, the UE2 sends an SDP answer which includes its own fingerprint to the P-CSCF (step 10), which then transmits the fingerprint to the terminating IMS-AGW (step 11). The exchanged fingerprints are used to validate the certificates used by the UE and the IMS-AGW during the DTLS negotiation of the keys to be used for the SRTP sessions. Similarly, steps 12-16 complete the fingerprint exchanges necessary to validate the DTLS negotiation of the keys for the SRTP connection between the originating and terminating IMS-AGWs (step 15) and between the originating UE and originating IMS-AGW (step 16).

Figure 10 shows signaling which uses DTLS to establish a secure media session between a UE and a Media Resource Function, MRF.

Figure 11 is a flow diagram illustrating a method carried out by an apparatus configured to operate as a media gateway controller acting as a back-to-back SIP user agent controlling a media gateway function of an IMS network. In step 1101, the apparatus sends security information of the media gateway function to another media gateway controller acting as a back-to-back SIP user agent controlling another media gateway function of the IMS network, or to a node upstream of the other media gateway controller. In step 1102, the apparatus receives security information of the other media gateway function or said upstream node. In step 1103, the apparatus sends the security information to the media gateway function for use in securing media between the media gateway functions or between the media gateway function and said upstream node.

Figure 12 is a flow diagram illustrating a method carried out by an apparatus configured to operate as a media gateway controller acting as a back-to-back SIP user agent controlling a media gateway function of an IMS network. In step 1201, Receive a message comprising security information of another media gateway function of the IMS network controlled by a media gateway controller acting as a back-to-back SIP user agent and an indicator. The apparatus then sends (step 1202) the security information to either the media gateway function or to a node upstream of the media gateway controller.

Figure 13 is a schematic diagram of an exemplary apparatus 1301 for carrying out the above-described methods. The apparatus 1301 comprises: processor circuitry 1302; a storage unit 1303 storing instructions executable by the processor circuitry 1302, a receiver 1304 for receiving messages 1305 and a transmitter 1306 for transmitting messages 1307.

CLAIMS:

1. A method of securing media across an IP Multimedia Subsystem, IMS, network where the media transits via first and second media gateway functions of the IMS network which are controlled by respective first and second media gateway controllers acting as back-to-back Session Initiation Protocol, SIP, user agents, the method comprising, sending from the first media gateway controller to the second media gateway controller, or to a node upstream of the second media gateway controller, security information of the first media gateway function, and using the sent information to secure media between the first and second media gateway functions or between the first media gateway function and said upstream node.
2. A method according to claim 1 and comprising, at the first media gateway controller, receiving, from the second media gateway controller, further security information of the second media gateway function or said upstream node and using the further security information to secure media between the first and second media gateway functions or between the first media gateway function and said upstream node.
3. A method according to claim 2 and comprising using the security information and the further security information to negotiate one or more encryption keys and using the key(s) to secure the media.
4. A method according to claim 3, wherein the key negotiation uses a Session Description Security Descriptions, SDDES, protocol or a Datagram Transport Layer Security, DTLS, protocol.
5. A method according to any one of claims 1 to 4 and comprising, at the first media gateway function, receiving media secured using the security information of the first media gateway from the second media gateway function or said upstream node and removing the security from the received media.
6. A method according to any one of claims 1 to 5, wherein the first and/or second media gateway controller is a Proxy Call Session Control Function, P-CSCF, an

Interconnection Border Control Function, IBCF, or a Media Gateway Control Function, MGCF.

7. A method according to any one of claims 1 to 5, wherein, for the case in which the method involves said upstream node, the second media gateway controller is a Media Resource Function Controller, MRFC and said upstream node is a Media Resource Function Processor, MRFP.

8. A method according to any one of claims 1 to 6, wherein, for the case in which the method involves said upstream node, said upstream node is a User Equipment, UE.

9. A method according to any one of the preceding claims, wherein the security information of the first media gateway function is sent in a SIP INVITE or SIP UPDATE message.

10. A method according to any one of claims 2 to 9, wherein the further security information is sent in a SIP 18x series or a SIP 200 response message.

11. A method according to any one of the preceding claims, wherein the second media gateway controller receives, from the first media gateway controller, the security information of the first media gateway function and data indicating which of the second media gateway function or said upstream node should be sent the security information.

12. A method according to claim 11 as dependent on claim 2 and comprising, at the second media gateway controller, obtaining the further security information from either the second media gateway function or said upstream node according to said indicator.

13. An apparatus configured to operate as a media gateway controller acting as a back-to-back Session Initiation Protocol, SIP, user agent controlling a media gateway function of an IP Multimedia Subsystem, IMS, network, the apparatus comprising: processor circuitry; a storage unit storing instructions executable by the processor circuitry, a receiver for receiving messages and a transmitter for sending messages, whereby the apparatus is operable to:

send security information of the media gateway function to another media gateway controller acting as a back-to-back SIP user agent controlling another media

gateway function of the IMS network, or to a node upstream of the other media gateway controller; and

5 configure the media gateway function to remove the security from media secured using the security information received from the other media gateway function or upstream node.

14. An apparatus according to claim 13, whereby the apparatus is operable to:
 receive security information of the other media gateway function or said upstream node;

10 send the security information to the media gateway function; and
 configure the media gateway function to secure media using the security information for sending to the other media gateway function or said upstream node.

15 15. An apparatus according to claim 14, whereby the apparatus is operable to send the security information to the media gateway function in response to receiving an 18x series answer containing the security information.

20 16. An apparatus configured to operate as a media gateway controller acting as a back-to-back Session Initiation Protocol, SIP, user agent controlling a media gateway function of an IP Multimedia Subsystem, IMS, network, the apparatus comprising: processor circuitry; a storage unit storing instructions executable by the processor circuitry, a receiver for receiving messages and a transmitter for sending messages, whereby the apparatus is operable to:

25 receive security information of another media gateway function of the IMS network controlled by a media gateway controller acting as a back-to-back SIP user agent;

 send the security information to either the media gateway function or to a node upstream of the media gateway controller; and

30 configure the media gateway function or a node upstream of the media gateway controller to use the security information to secure media for sending to the media gateway.

35 17. An apparatus according to claim 16, whereby the apparatus is operable to send the security information in response to receiving a SIP INVITE or SIP UPDATE containing the security information.

18. An apparatus according to claim 16 or 17, whereby the apparatus is operable to:

receive an indicator specifying which of the second media gateway function or said upstream node to send the security information; and

5 send the security information to the second media gateway function or said upstream node according to said indicator.

19. An apparatus according to claim 16, whereby the apparatus is operable to:

10 obtain security information from either the media gateway function or the node upstream of the media gateway controller according to said indicator and send the obtained security information to the other media gateway function.

20. An apparatus according to any one of claims 13 to 15, configured to operate as the apparatus of any one of claims 16 to 19.

15

21. An apparatus according to any one of claims 11 to 19, configured to operate as a Proxy Call Session Control Function, P-CSCF, an Interconnection Border Control Function, IBCF, a Media Resource Function Controller, MRFC, or a Media Gateway Control Function, MGCF.

20

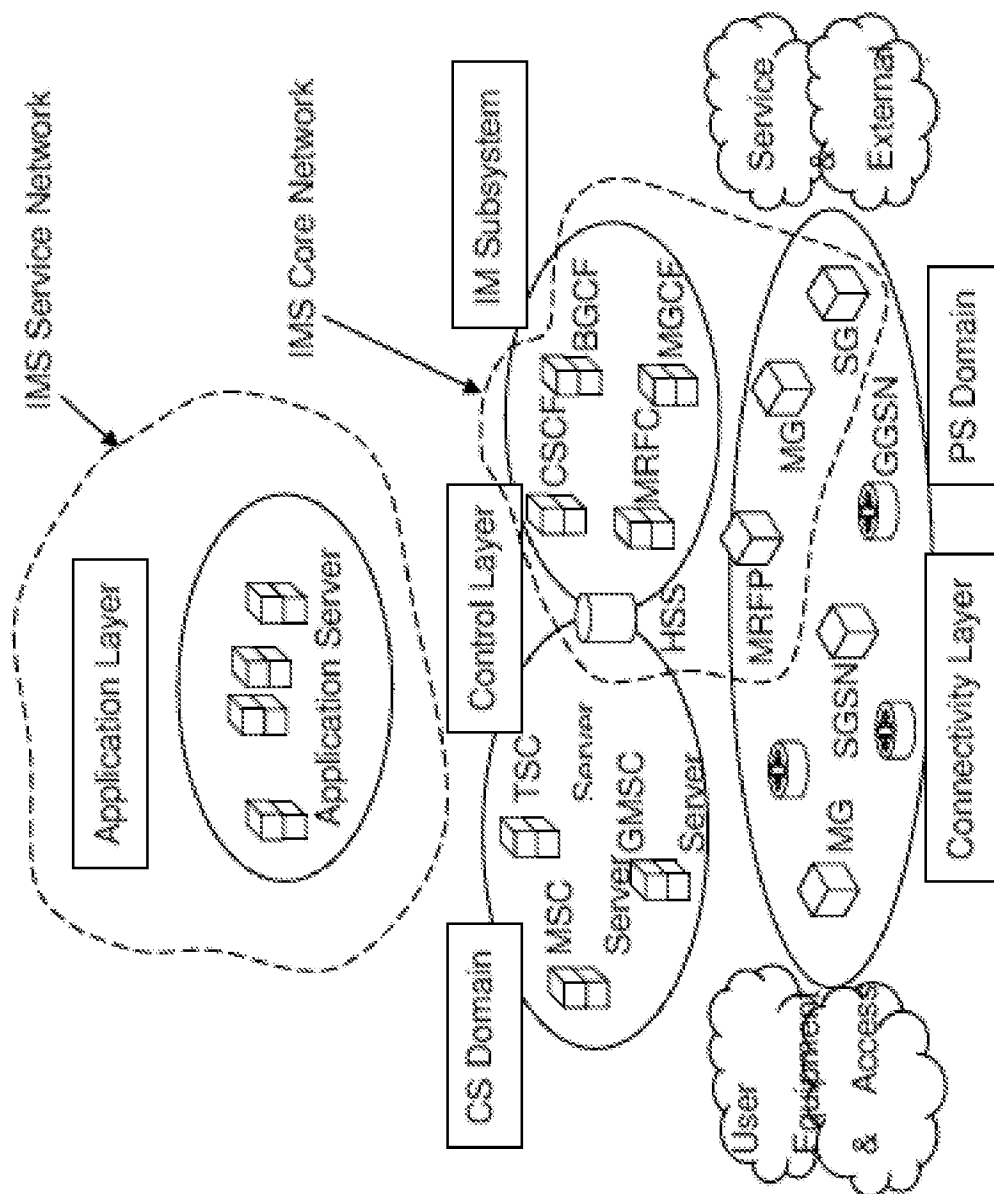


Figure 1

Figure 2

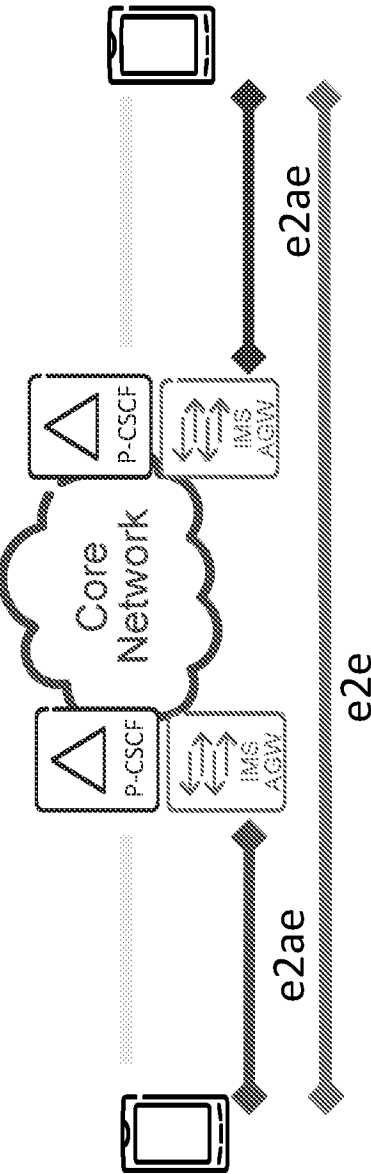
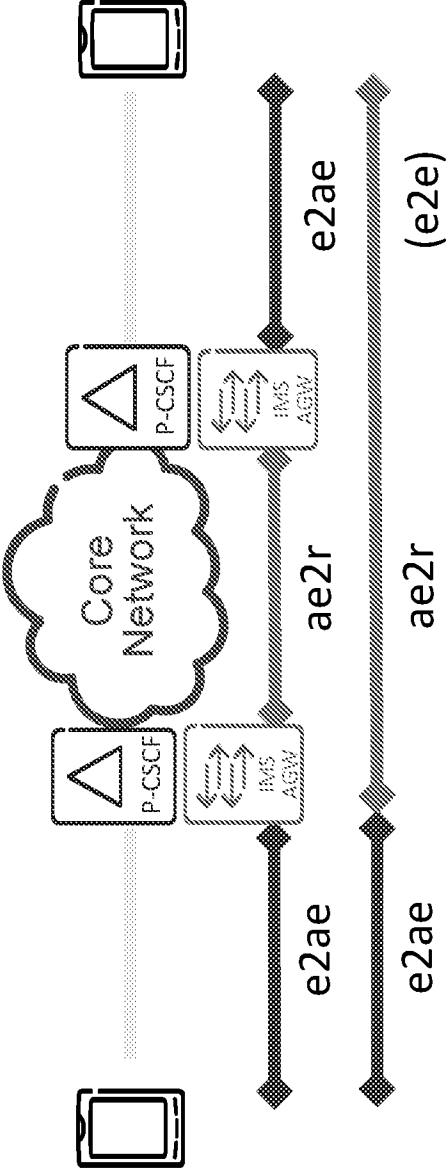


Figure 3



Media is protected using SRTP (Secure RTP).

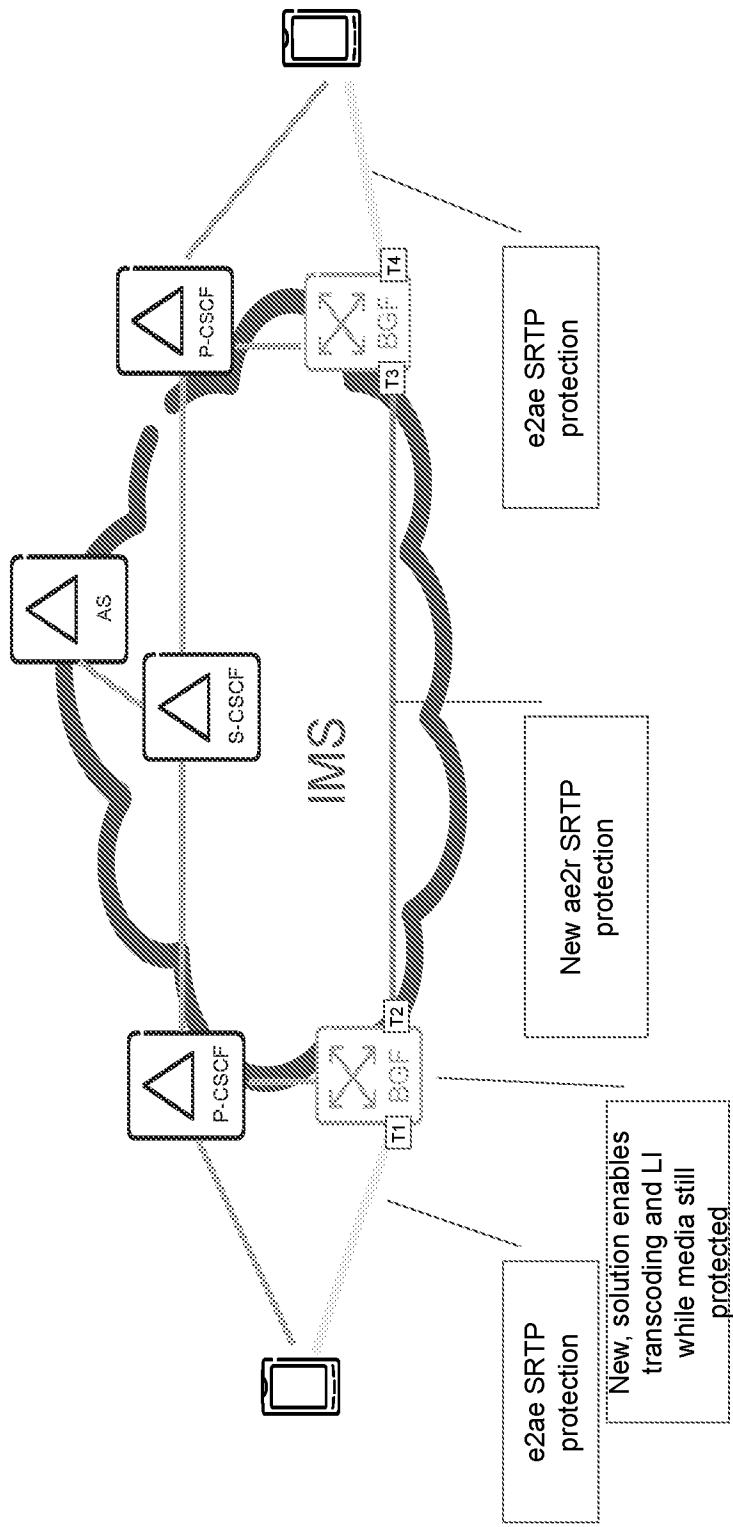


Figure 4

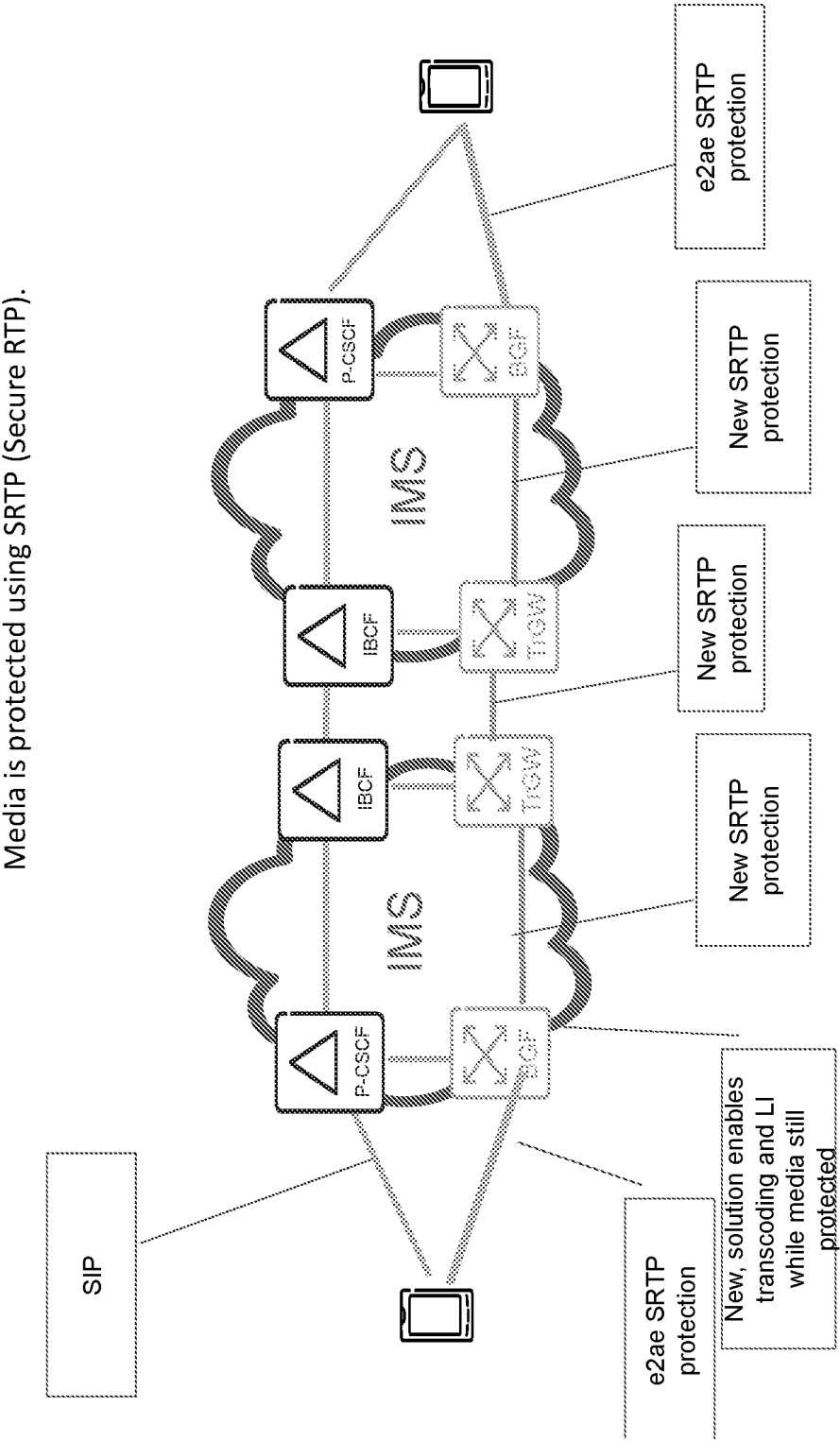


Figure 5

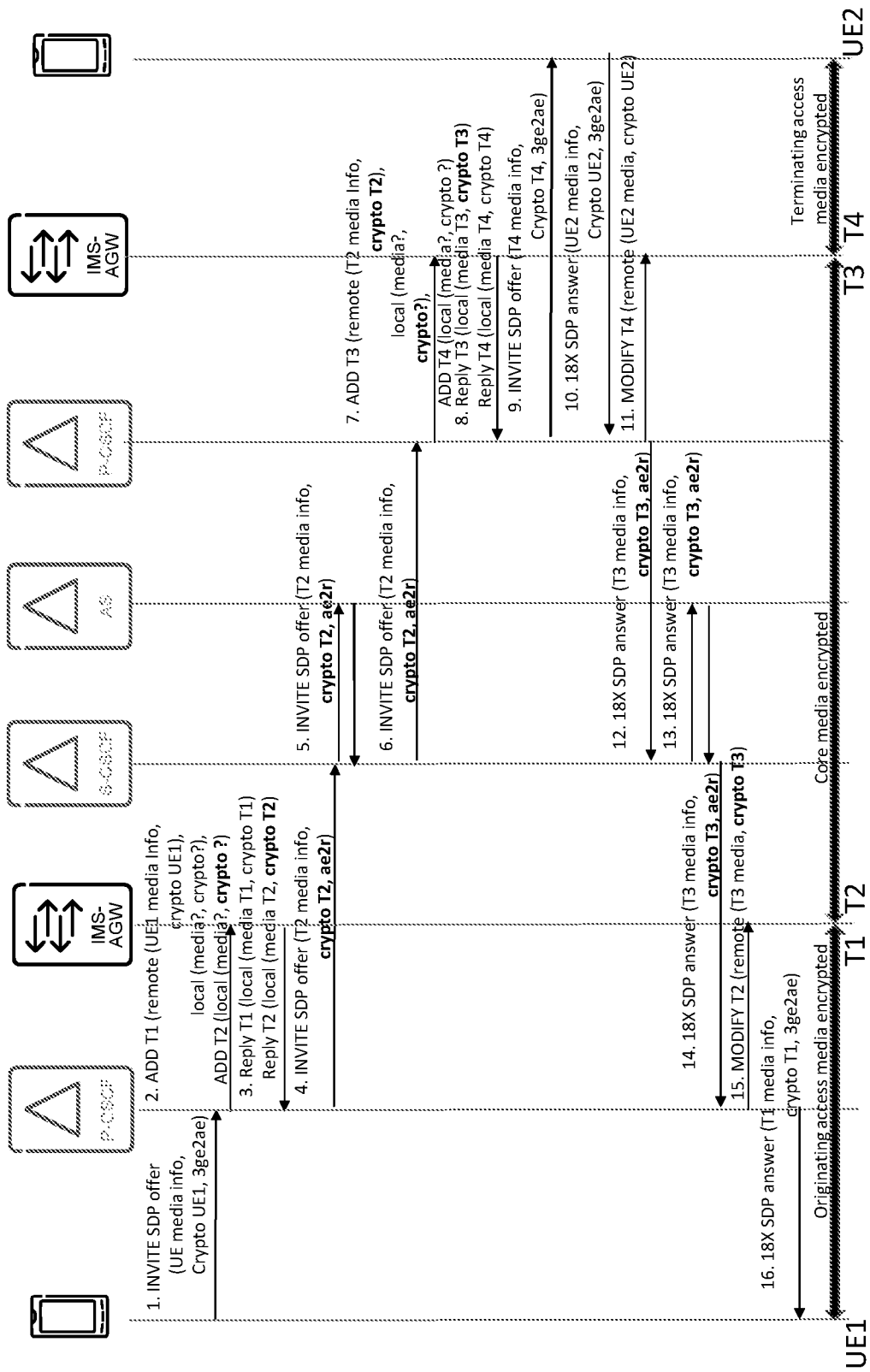


Figure 6

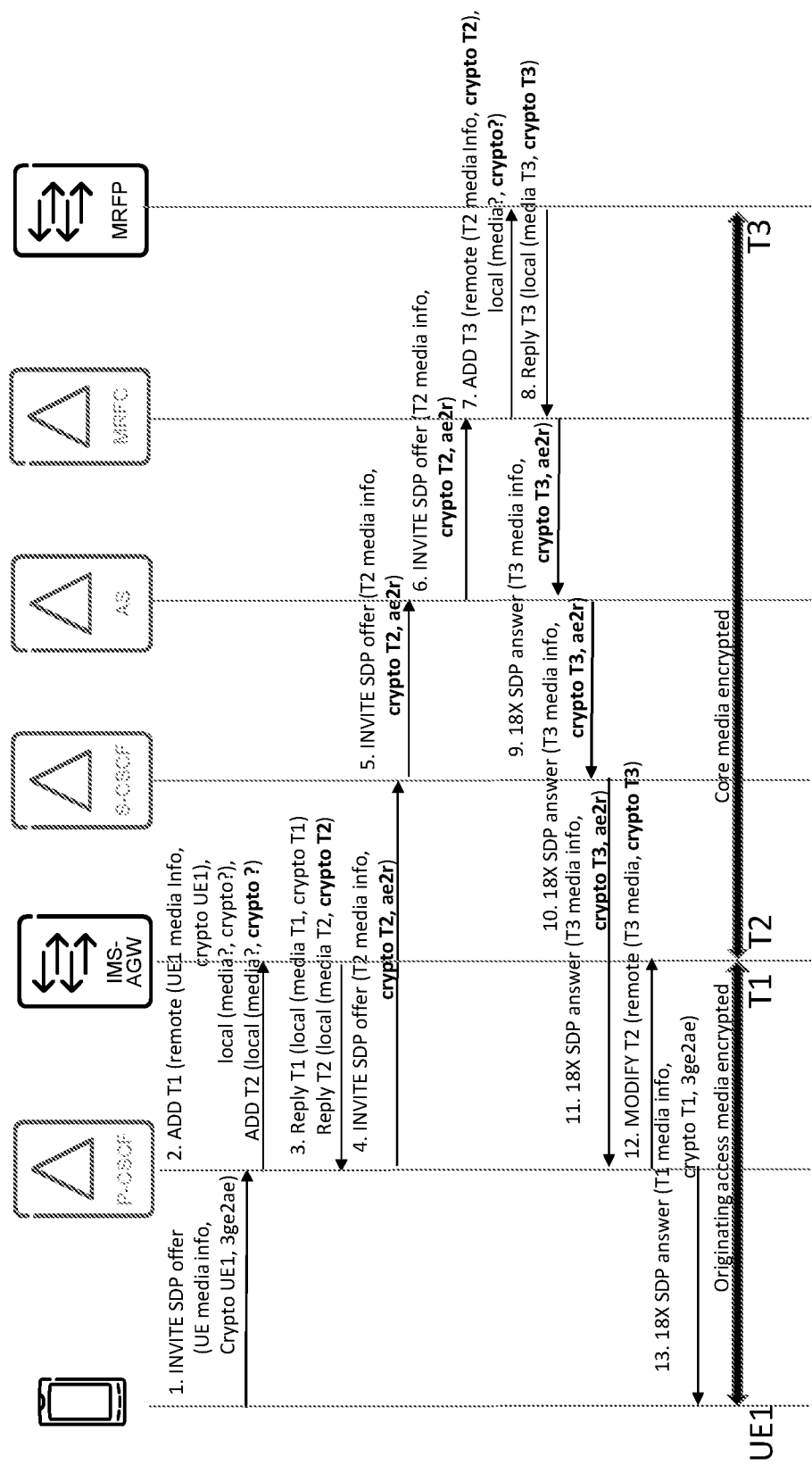


Figure 7

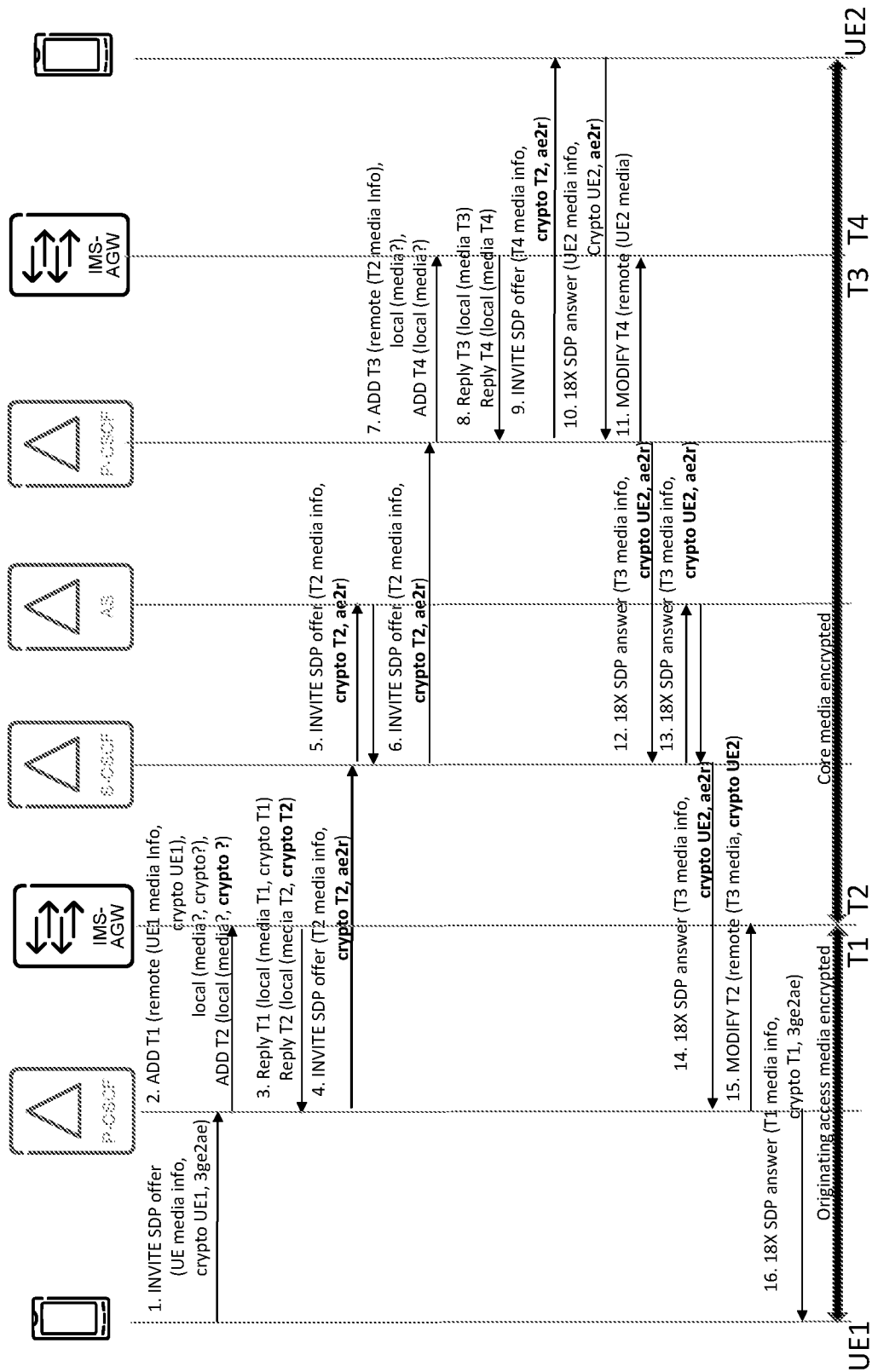


Figure 8

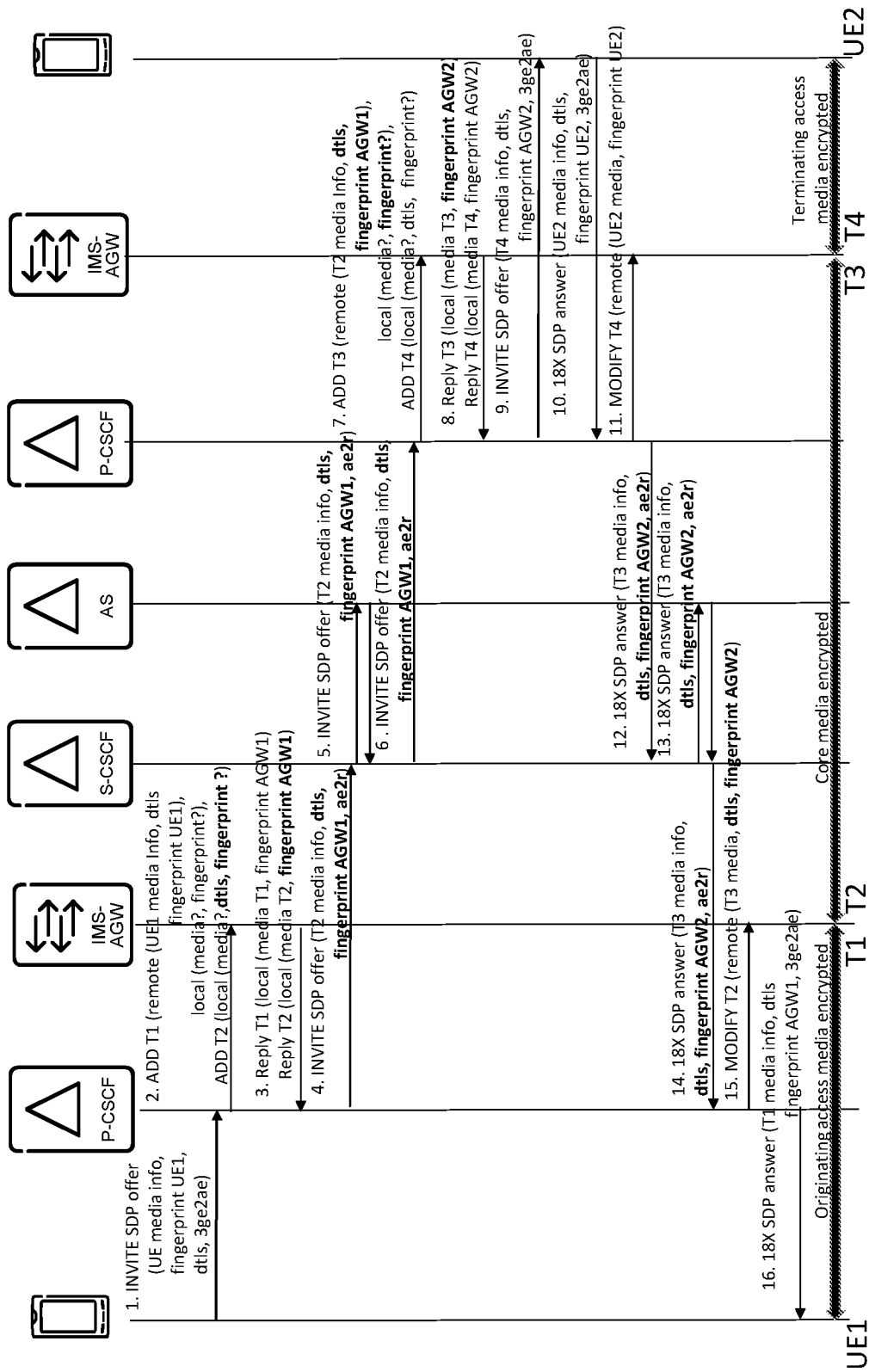


Figure 9

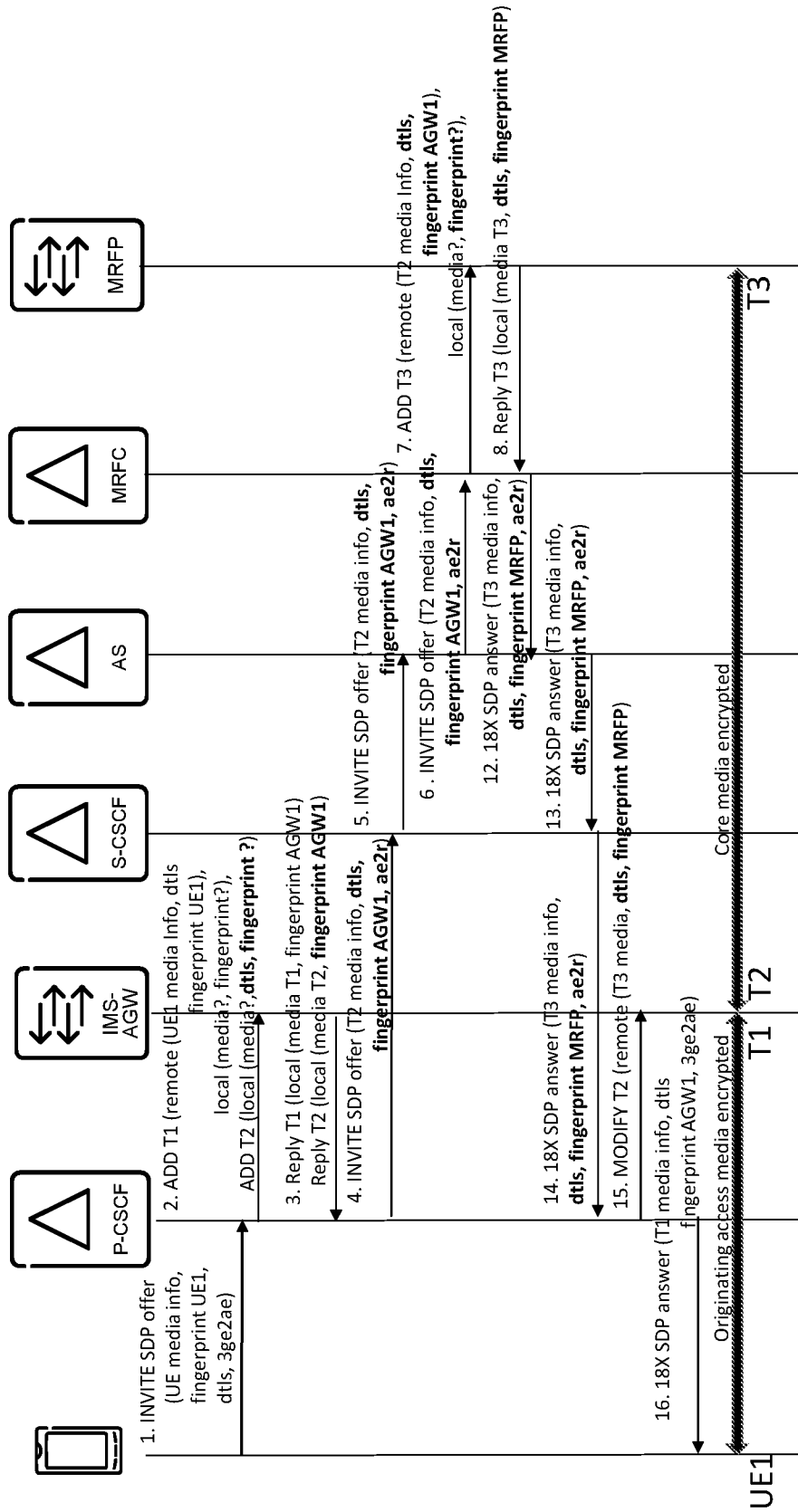


Figure 10

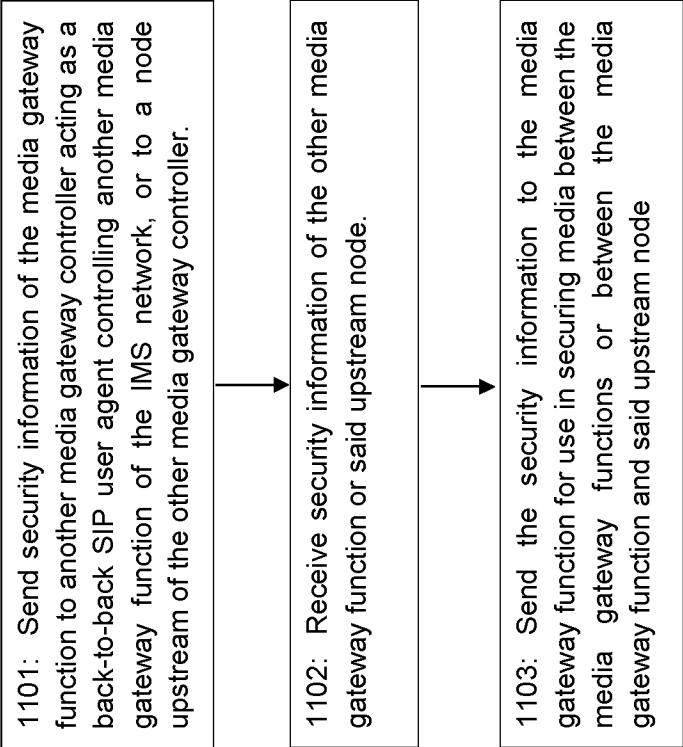


Figure 11

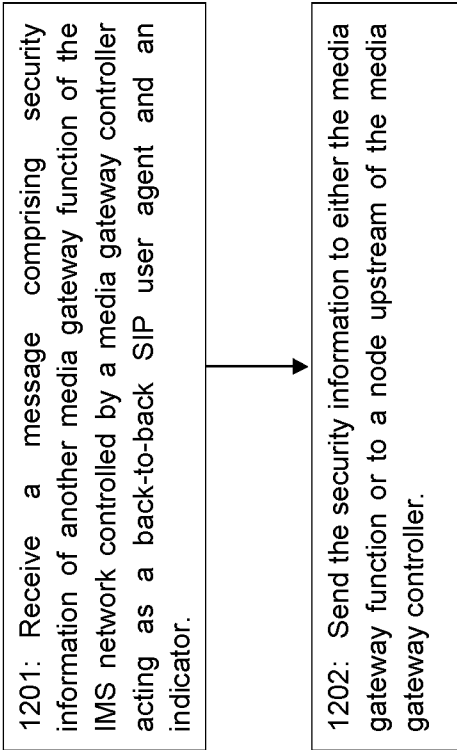


Figure 12

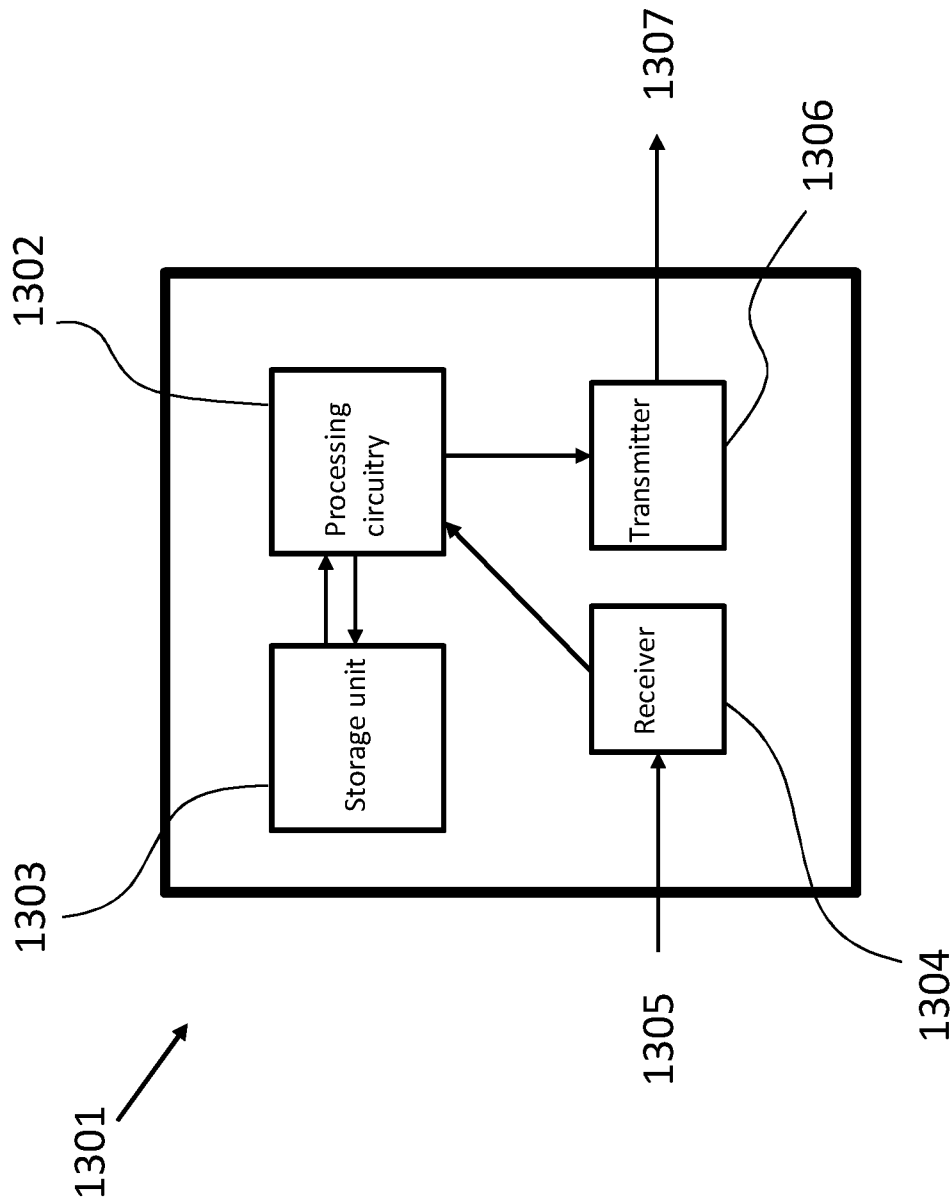


Figure 13

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2017/050648

A. CLASSIFICATION OF SUBJECT MATTER

IPC: see extra sheet

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L, H04W

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

SE, DK, FI, NO classes as above

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

EPO-Internal, PAJ, WPI data, COMPENDEX, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 20090220091 A1 (HOWARD PETER THOMAS), 3 September 2009 (2009-09-03); abstract; figure 4 --	1-21
A	WO 2016126246 A1 (NOKIA SOLUTIONS & NETWORKS OY ET AL), 11 August 2016 (2016-08-11); abstract; figure 4 --	1-21
A	US 20130268681 A1 (BARRIGA LUIS ET AL), 10 October 2013 (2013-10-10); abstract; figure 1 --	1-21
A	US 20120198527 A1 (NAESLUND MATS ET AL), 2 August 2012 (2012-08-02); abstract; figures 1,2 -- -----	1-21

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

* Special categories of cited documents:	"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
"A" document defining the general state of the art which is not considered to be of particular relevance	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"&" document member of the same patent family
"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	

Date of the actual completion of the international search 12-03-2018	Date of mailing of the international search report 12-03-2018
Name and mailing address of the ISA/SE Patent- och registreringsverket Box 5055 S-102 42 STOCKHOLM Facsimile No. + 46 8 666 02 86	Authorized officer Anders Edlund Telephone No. + 46 8 782 28 00

Continuation of: second sheet

International Patent Classification (IPC)

H04L 29/06 (2006.01)

H04L 9/00 (2006.01)

H04L 29/08 (2006.01)

H04W 12/06 (2009.01)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/SE2017/050648

US	20090220091 A1	03/09/2009	EP	1946479 B1	26/11/2014
			ES	2526703 T3	14/01/2015
			US	8705743 B2	22/04/2014
			WO	2007023286 A1	01/03/2007
WO	2016126246 A1	11/08/2016	CN	107431731 A	01/12/2017
			EP	3254451 A1	13/12/2017
			KR	20170115578 A	17/10/2017
			US	20180013880 A1	11/01/2018
US	20130268681 A1	10/10/2013	CA	2706335 A1	04/06/2009
			CN	101878631 B	12/10/2016
			CN	106850526 A	13/06/2017
			EP	2229760 A2	22/09/2010
			IL	205878 A	29/08/2013
			JP	2011505736 A	24/02/2011
			JP	2014197856 A	16/10/2014
			JP	5881949 B2	09/03/2016
			JP	5870156 B2	24/02/2016
			US	8549615 B2	01/10/2013
			US	20110010768 A1	13/01/2011
			US	8832821 B2	09/09/2014
			WO	2009068985 A2	04/06/2009
US	20120198527 A1	02/08/2012	US	8539564 B2	17/09/2013
			WO	2010099823 A1	10/09/2010