ETSI TS 133 328 V18.2.0 (2024-10)

Universal Mobile Telecommunications System (UMTS);
LTE;
IP Multimedia Subsystem (IMS) media plane security
(3GPP TS 33.328 version 18.2.0 Release 18)

Reference
RTS/TSGS-0333328vi20

Keywords
LTE,UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under https://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

With Common IMS it has become possible to use IMS over a wide variety of access networks. These access networks provide security of varying strengths, or, in some cases, no security at all. It is therefore desirable to have a standard for IMS media plane security, which provides uniform protection of IMS media against eavesdropping and undetected modification across access networks. Furthermore, media transport in the core network, although generally less vulnerable than in the access network, may also be realised in varying ways with different guarantees of protection. It is therefore also desirable to have a standard for IMS media plane security, which guarantees protection of IMS media against eavesdropping and undetected modification in an end-to-end (e2e) fashion between two terminal devices.

1 Scope

The present document presents IMS media plane security for RTP and MSRP based media, IMS data channels (i.e., SCTP over DTLS) as well as security for BFCP as used in IMS conferencing. The security mechanisms are designed to meet the following three main objectives:

1) to provide security for media usable across all access networks

2) to provide an end-to-end (e2e) media security solution for RTP and data channel-based media to satisfy major user categories

3) to provide end-to-end (e2e) media security for important user groups like enterprises, National Security and Public Safety (NSPS) organizations and different government authorities who may have weaker trust in the inherent IMS security and/or may desire to provide their own key management service.

The media plane security for RTP based media is based on the well-established protocol SRTP. Key management solutions for SRTP are defined in this specification.

The media plane security for MSRP, used in session-based messaging, is based on TLS. TLS is also used to protect BFCP. Key management solutions for MSRP and BFCP security are defined in the present document. The media plane security for IMS data channels, i.e., SCTP over DTLS, is based on DTLS.

Two normative Annexes to the present document address IMS media plane security for immediate messaging and conferencing, respectively. The media plane security for session-based messaging is addressed in the main body of this specification.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.002: "Network architecture".

[3] 3GPP TS 23.228: "IP Multimedia (IM) Subsystem".

[4] 3GPP TS 33.203: "3G Security; Access security for IP-based services".

[5] 3GPP TS 33.210: "3G Security; Network domain security; IP network layer security".

[6] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic bootstrapping architecture".

[7] IETF RFC 1035: "DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION".

[8] IETF RFC 2616: "Hypertext Transfer Protocol -- HTTP/1.1".

[9] IETF RFC 3711: "The Secure Real-time Transport Protocol (SRTP)".

[10] IETF RFC 3550: "RTP: A Transport Protocol for Real-Time Applications".

[11] IETF RFC 3830: "MIKEY: Multimedia Internet KEYing".

[12] IETF RFC 4567: "Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP)".

[13] IETF RFC 4568: "Session Description Protocol (SDP) Security Descriptions for Media Streams".

[14] IETF RFC 6043: "MIKEY-TICKET: Ticket-Based Modes of Key Distribution in Multimedia Internet KEYing (MIKEY)".

[15] IETF RFC 4771: "Integrity Transform Carrying Roll-Over Counter for the Secure Real-time Transport Protocol (SRTP)".

[16] Otway, D. and Rees, O. 1987: "Efficient and timely mutual authentication." *SIGOPS Oper. Syst. Rev.* 21, 1 (Jan. 1987), 8-10.

[17] Void

[18] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP)".

[19] 3GPP TS 24.109: "Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details".

[20] 3GPP TS 29.162: "Interworking between the IM CN subsystem and IP networks ".

[21] IETF RFC 4975: "The Message Session Relay Protocol (MSRP)".

[22] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[23] Void

[24] IETF RFC 6714: "Connection Establishment for Media Anchoring (CEMA) for the Message Session Relay Protocol (MSRP)".

[25] 3GPP TS 24.147: "Conferencing using the IP Multimedia (IM), Core Network (CN) subsystem".

[26] IETF RFC 4575: "A Session Initiation Protocol (SIP) Event Package for Conference State".

[27] GSM Association, Rich Communication Suite 5.1 Advanced Communications Services and Client Specification, Version 1.0, August 2012.

[28] 3GPP TS 24.247: "Messaging service using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".

[29] IETF RFC 5365: "Multiple-Recipient MESSAGE Requests in the Session Initiation Protocol (SIP)".

[30] Void

[31] IETF RFC 5652: "Cryptographic Message Syntax (CMS)".

[32] IETF RFC 5083: " Cryptographic Message Syntax (CMS) Authenticated-Enveloped-Data Content Type".

[33] IETF RFC 3565: "Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS)".

[34] ITU-T recommendation T.38 (09/2010): "Procedures for real-time Group 3 facsimile communication over IP networks".

[35] 3GPP TS 26.114: "IP Multimedia Subsystem (IMS); Multimedia telephony; Media handling and interaction".

[36] IETF RFC 6347: "Datagram Transport Layer Security Version 1.2".

[37] IETF RFC 7325:"UDP Transport Layer (UDPTL) over Datagram Transport Layer Security (DTLS)".

[38] Void

[39] IETF RFC 8826: "Security Considerations for WebRTC".

[40] IETF RFC 5763: "Framework for Establishing a Secure Real-time Transport Protocol (SRTP) Security Context Using Datagram Transport Layer Security (DTLS)".

[41] IETF RFC 5764: "Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)".

[42] IETF RFC 8832: " WebRTC Data Channel Establishment Protocol".

[43] IETF RFC 8851: "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification".

[44] IETF RFC 8855: "The Binary Floor Control Protocol (BFCP)".

[45] IETF RFC 8866: "SDP: Session Description Protocol".

[46] IETF RFC 7714: "AES-GCM Authenticated Encryption in the Secure Real-time Transport Protocol (SRTP)".

[47] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[48] IETF RFC 8841: "Session Description Protocol (SDP) Offer/Answer Procedures for Stream Control Transmission Protocol (SCTP) over Datagram Transport Layer Security (DTLS) Transport".

[49] IETF RFC 8842: "Session Description Protocol (SDP) Offer/Answer Considerations for Datagram Transport Layer Security (DTLS) and Transport Layer Security (TLS)".

[50] IETF RFC 8831: "WebRTC Data Channels".

[51] IETF RFC 8864 : "Negotiation Data Channels Using the Session Description Protocol (SDP)".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

End-to-access edge security: This term refers to media protection extending between an IMS UE and the first IMS core network node in the media path without being terminated by any intermediary.

End-to-end security: This term refers to media protection extending between two IMS UEs without being terminated by any intermediary.

IMS User Equipment: User equipment used for IMS media communications over access networks. Use of such equipment for IMS media communications over any 3GPP access network shall require presence of a UICC.

KMS User Identity: A KMS user identity is derived from a user's public SIP-URI and it is the NAI-part of the SIP URI.

3.2 Symbols

Void

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

BFCP	Binary Floor Control Protocol
DCSF	Data Channel Signalling Function
DTLS	Datagram Transport Layer Security
DTLS-SRTP	DTLS Extension to Establish Keys for SRTP
e2ae	End-to-access edge
e2e	End-to-end
e2DCe	End-to-Data-Channel edge
GW	Gateway
IMS-ALG	IMS Application Level Gateway
IMS AS	IMS Application Server
IMS UE	IMS User Equipment
KMS	Key Management Service
MF	Media Function
MIKEY	Multimedia Internet KEYing
MSRP	Message Session Relay Protocol
NAF	Network Application Function
RTP	Real-time Transport Protocol
SRTP	Secure Real-time Transport Protocol
TEK	Traffic Encryption Key
TGK	TEK Generation Key
TLS	Transport Layer Security
WebRTC	Web Real-Time Communication

4 IMS media plane security overview

4.1 Introduction

4.1.1 General

IMS media plane security for RTP is composed of several more or less independent key management solutions. DTLS-SRTP is for e2ae media protection. SDES, is for e2ae and for e2e media protection. These solutions relies on the security of the SIP infrastructure and in particular on SIP signalling security.

The KMS solution is for e2e protection and aims for high security, independent of the signalling and transport network. It is based on use of a Key Management Service (KMS) and a ticket concept. The security offered is anchored in the KMS including the functionality used for user authentication and key generation towards the KMS.

Irrespectively of key management solution used, SRTP [9] is used as the security protocol to protect RTP based traffic. Specifically, the key(s) provided by this specification are used as the so called SRTP master key.

TLS is used to protect MSRP based traffic. Key management for e2ae protection of MSRP relies on exchanging certificates and transmission of the fingerprints of these certificates over SDP. E2e protection can be achieved through the same KMS and ticket concept that is used for RTP traffic. The established key is used to setup a TLS-PSK tunnel between the two parties.

IMS media plane security also includes the security of IMS Data Channels (TS 23.228 [3]), which in turn includes two types of architectures, e2DCe (end to Data Channel edge) and e2e. DTLS is used to protect the IMS Data Channel type of traffic. The e2DCe is defined as the path from the IMS UE to the Data Channel Media Function (MF). The IMS e2e

is defined as the path from an IMS UE to another IMS UE or from an IMS UE to an IMS Data Channel Application server.

Editor´s Note: Using the certificate fingerprint mechanism to provide e2e protection is ffs

4.1.2 Overview of key management solutions for IMS media plane security

4.1.2.1 SDES based solution

SDES (Session Description Protocol Security Descriptions for Media Streams, cf. RFC 4568 [13]), is a simple key management protocol for media streams, which are to be secured by means of SRTP [9]. SDES defines a Session Description Protocol (SDP) RFC 8866 [45] cryptographic attribute for unicast media streams. The attribute describes a cryptographic key and other parameters that serve to configure security for a unicast media stream in either a single message or a roundtrip exchange. The attribute can be used with a variety of SDP media transports, and RFC 4568 [13] defines how to use it for the SRTP unicast media streams. The SDP crypto attribute requires the services of a data security protocol to secure the SDP message. For the use of SDES in IMS, the SIP signalling security mechanisms defined for IMS shall be used, for more details cf. clause 5.5.

SDES basically works as follows: when an offerer A and an answerer B establish a SIP session they exchange cryptographic keys for protection of the ensuing exchange of media with SRTP. A includes the key, by which the media sent from A to B is protected, in a SIP message to B, and B responds with a SIP message including a second key, by which the media sent from B to A is protected.

In this specification, SDES is used for two modes of operation: e2ae mode and e2e mode. For the e2ae mode, SDES is run between an IMS UE and a SIP edge proxy, i.e. a P-CSCF (IMS-ALG). In the originating network, he P-CSCF (IMS-ALG) evaluates and subsequently deletes SDES cryptographic attributes that are passed to it from the IMS UE in SIP messages, and creates SDES cryptographic attributes and passes them to the IMS UE in SIP messages. This is done similarly in the terminating network. The resulting SRTP session is then established between the IMS UE and the media node controlled by the P-CSCF (IMS-ALG), i.e. the IMS Access Gateway (GW). This means that, for the e2ae mode, media is protected only over the access part of the network. The purpose of the e2ae mode is to provide access protection, i.e. guarantee protection of IMS media against eavesdropping and undetected modification in a uniform manner across heterogeneous access networks with various strengths of link layer protection. Access protection on the originating side is provided independently of access protection on the terminating side.

For the e2e mode, SDES is run between two IMS UEs, and the resulting SRTP session is then established between the two IMS UEs. This e2e media plane security solution should be suitable for anyone for whom the security level, with which SIP signalling messages are protected, is sufficient.

When used in e2e mode SDES has minor requirements on the network infrastructure. When used in e2aemode, the requirements on the network infrastructure can be seen from clause 4.2.2.

Wordings like “e2e security using SDES” as used in the following refer to security for RTP based media, as SDES does only apply to protecting RTP.

4.1.2.2 KMS based solution

The KMS based solution is an e2e security solution which protects media from one IMS UE all the way to another IMS UE not allowing any network entity access to plaintext media. It is designed to rely on a well defined and limited set of entities that have to be trusted, simplifying the task of evaluation and assessment of offered security level.

This solution is based on use of a KMS and a "ticket" concept. A high level and simplified description of the solution is as follows: The initiator of a call requests keys and a ticket from the KMS. The ticket contains the keys in a protected format. The initiator then sends the ticket to the recipient. The recipient presents the ticket to the KMS and the KMS returns the keys on which the media security shall be based. All these message exchanges are authenticated and sensitive parts are encrypted. The solution is based on MIKEY-TICKET [14].

Users served by different KMS's may establish connections with media plane security enabled, provided that the operators of the KMS's have a cooperation agreement and that the operators have established a secure and authenticated channel for message exchange between the KMS's.

The KMS based solution allows implementation of per user policies regarding use of secure connections in general and key handling in particular. System specific policies can easily be defined and enforced by the KMS. Access to the KMS is granted based on user authentication and authorization. User authentication may be based on GBA [6] with the KMS taking the role of a NAF.

The KMS based solution specified here also solves the so called forking problem as it includes a mechanism which gives each individual recipient end-point in a forking scenario a unique key. These end-point unique keys cannot be recreated by any other end-point (except for the initiator) and in particular not any other end-point to which the call was forked. At the same time the solution offers SIP security independent mutual identity verification of caller and answering user.

This KMS based solution includes three features aiming to off-load the KMS from receiving ticket requests. The first feature is that tickets may be reused. This means that a user may request a ticket for another user and then for a specified time period use this ticket to protect calls to the other user. The second feature is that it is possible to generate tickets that can be used to establish secure connections to any user in a defined set of users. Such tickets are called group tickets. The third feature is that, if allowed by the local policy, the initiator may create tickets by itself, without contacting the KMS. This feature is supported by MIKEY-TICKET [14] and mimics the signalling flows of the Otway-Rees protocol [16].

Note that use of tickets combining these three features may significantly reduce the number of ticket requests that the KMS has to handle. Note also that the use of tickets carrying keys will allow a design of the KMS with no requirements to hold per user state.

4.1.2.3 Certificate fingerprints based solution for e2ae TLS/DTLS

Key management solution for e2ae protection of MSRP, DTLS-SRTP, WebRTC data channel based media are based on the cipher suites and session keys negotiated via the TLS/DTLS handshake between the UE and the IMS Access Gateway (GW). The TLS/DTLS record protocol secures the actual media. Mutual authentication during the TLS/DTLS handshake is achieved using certificates, with the certificate fingerprints being transmitted using the SDP fingerprint attribute in the SDP offer-answer exchange between the UE and the P-CSCF (IMS ALG).

This approach is specified in RFC 4975 [21]. "TCP/TLS/MSRP" is used as the protocol identifier in the m-line of the SDP, and the "a=fingerprint" attribute is used to provide the fingerprint of the certificate. The same approach is specified in RFC 8841 [48] and RFC 8842 [49], where "UDP/DTLS/SCTP" is used as the protocol identifier in the m-line of the SDP, "a=fingerprint" attribute is used to provide the fingerprint of the certificate, and "a=tls-id" provides the DTLS instance identification to handle DTLS restart scenarios.

TLS/DTLS profile considerations discussed in annex M of this specification shall be followed to support IMS media plane security.

4.1.2.4 Certificate fingerprints based solution for e2DCe DTLS

The key management solution for e2DCe protection of IMS data channel-based media is based on the cipher suites and session keys negotiated via the DTLS handshake between the UE and MF/MRF. The DTLS record protocol secures the actual media. Mutual authentication during the DTLS handshake is achieved using certificates, with the certificate fingerprints being transmitted using the SDP fingerprint attribute in the SDP offer-answer exchange between the UE and the MF/MRF via the P-CSCF, S-CSCF, IMS AS.

This approach is specified in RFC 8841 [48] and RFC 8842 [49], where "UDP/DTLS/SCTP" is used as the protocol identifier in the m-line of the SDP, "a=fingerprint" attribute is used to provide the fingerprint of the certificate, and "a=tls-id" provides the DTLS instance identification to handle DTLS restart scenarios.

DTLS profile considerations discussed in annex M of this specification shall be followed to support IMS media plane security.

4.1.2.5 Certificate fingerprints based solution for e2e DTLS

The key management solution for e2e protection of IMS data channel-based media is based on the cipher suites and session keys negotiated via the DTLS handshake between the UE and the peer. This peer can be either the peer UE or a WebRTC-enabled network server. The DTLS record protocol secures the actual media. Mutual authentication during the DTLS handshake is achieved using certificates, with the certificate fingerprints being transmitted using the SDP fingerprint attribute in the SDP offer-answer exchange between the UE and the P-CSCF (DCSF, IMS AS).

This approach is specified in RFC 8841 [48] and RFC 8842 [49], where "UDP/DTLS/SCTP" is used as the protocol identifier in the m-line of the SDP, "a=fingerprint" attribute is used to provide the fingerprint of the certificate, and "a=tls-id" provides the DTLS instance identification to handle DTLS restart scenarios.

DTLS profile considerations discussed in annex M of this specification shall be followed to support IMS media plane security.

4.2 IMS media plane security architecture

4.2.1 General

This clause describes the impact of IMS media plane security on the IMS architecture. Five cases need to be distinguished. The IMS UEs are impacted in all five cases. The network impact varies with the cases.

1. E2ae security: here the P-CSCF (IMS-ALG), the IMS Access GW, and the Iq interface between them are impacted.
2. E2e security using SDES: minor impact on the network infrastructure (see TS 29.162 [20] for details).
3. E2e security using KMS: here, the network infrastructure needs to be enhanced with a Key Management Server, which, in turn, relies on a GBA [6] infrastructure, or an infrastructure to provide corresponding services, to be in place. Otherwise, there is minor impact on the network infrastructure (see TS 29.162 [20] for details).
4. E2DCe IMS Data Channel media plane security: The P-CSCF as well as other network functions such as S-CSCF, IMS AS, and the related interfaces Mw, ISC, DC2 are impacted. The IMS Data Channel media plane security is established between the UE and MF/MRF.
5. E2e IMS Data Channel media plane security: The IMS Data Channel media plane security is established between two UEs or between a UE and a Data Channel Application Server.

A pre-requisite for support of e2e security is that media packets are forwarded transparently by any nodes present in the media path (SRTP packets in case of secure RTP, TLS packets in case of secure MSRP, and DTLS packets carrying SCTP in case of IMS Data Channel). This implies that transcoding of RTP streams is no longer possible.

These prerequisites apply irrespective of whether the SRTP session was established by means of SDES or KMS.

NOTE: The lawful interception architecture is outside the scope of this TS.

4.2.2 E2ae security

For e2ae security, the P-CSCF (IMS-ALG) shall always include the IMS Access GW in the media path even if the involvement of the IMS Access GW would otherwise not be needed, e.g. if traffic was to be routed only between two terminals in the same IMS domain.

The P-CSCF (IMS-ALG) needs to be enhanced to be able to terminate the key management protocol (DTLS-SRTP or SDES for SRTP and TLS for MSRP), as well as handle indications, which are specific to e2ae security and are inserted in SIP messages. The IMS Access GW needs to be enhanced to be able to terminate SRTP streams, TLS protecting MSRP, and DTLS protecting SCTP. The Iq interface between P-CSCF (IMS-ALG) and IMS Access GW needs to be enhanced to be able to transport parameters related to the management of SRTP and TLS/DTLS cryptographic contexts. There is no impact on other parts of the network infrastructure. This is depicted in Figure 1. Details can be found in clauses 6.2.1.3, 7.2.1 and 7.3.1.

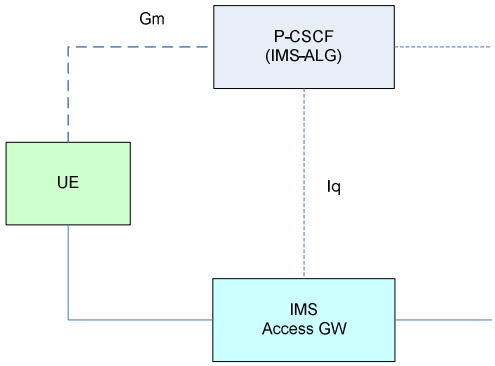


Figure 4.2.2-1: IMS signalling and media plane entities relevant to e2ae security

4.2.3 E2e security using SDES

When used in e2e mode SDES has minor requirements on the network infrastructure, see clause 4.2.1.

4.2.4 E2e security using KMS

The objective of the KMS based solution is to establish e2e media plane security between IMS UE's.

A simple network model of the entities involved in the key management for the KMS based solution is shown in Figure 2. The architecture follows the Generic Bootstrapping Architecture (GBA) [6]. GBA is used for KMS user authentication and establishment of a shared key for protection of message exchanges over Ua.

NOTE: Instead of GBA other systems offering corresponding services can be used. The used system has to provide user authentication, a shared security association between KMS and IMS UE and an identity for the security association which can be used to reference the security association. The security association can also define the user associated KMS user identities (see 6.2.3.2). The system can be based on any type of user credentials deemed to be secure enough for the intended application relying on the media plane security.

The IMS UE's may be served by different KMS's, e.g. when they belong to different IMS operator domains. Therefore, a new reference point, Zk, for message exchange between two KMS's is introduced. Zk is used when one KMS gets a request to resolve a ticket which only can be resolved by another KMS. The end-points using Zk shall be mutually authenticated and messages shall be integrity and confidentiality protected.

The media plane interface and the SIP signalling interface (Gm) is not shown in the reference model as these interfaces are in principle not changed. The required new functionality is implemented by modifications in SIP/SDP.

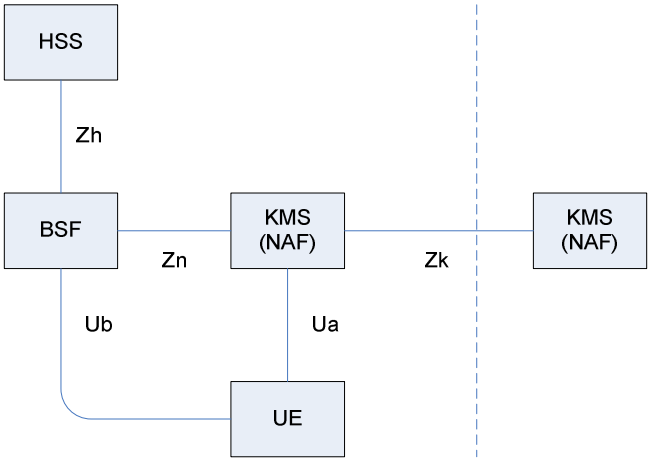


Figure4.2.4-1 : Reference model for key management for the KMS based solution

Further information on entities and reference points in the reference model is given in the following list:

- For HSS definitions refer to [2].
- For GBA and BSF definitions including the Zh, Zn and Ub reference points refer to TS 33.220 [6].
- For how to secure Zh and Zn also refer to TS 33.220 [6].
- The KMS acts as a NAF when GBA is used for user authentication and establishment of a key shared between the KMS and an IMS UE.
- Reference point Ua uses HTTP [8] for transport of MIKEY-TICKET [14] messages. The procedures are defined in Annex A.
- Protocol details for reference points Ua and Ub are provided in TS 24.109 [19].
- Reference point Zk also uses HTTP [8] for transport of MIKEY-TICKET [14] messages. The procedures are according to Annex A with the restriction that Request-URI only can contain "requesttype" equal to "ticketresolve”. Network domain Security [5] shall be used for authentication of endpoints and protection of messages.

4.2.5 E2DCe security

For e2DCe security, and for IMS Data Channels that terminate in the MF/MRF, the IMS Access GW is not needed in the media path for security purposes.

The interface between IMS AS and the Data Channel Media Function (DC2) or MRF (Mr’/Cr) needs to be able to transport parameters related to the management of DTLS cryptographic contexts. There is no impact on other parts of the network infrastructure. This is depicted in Figure 4.2.5-1. Details can be found in clauses 6.2.4, 7.2.4 and 7.3.3.

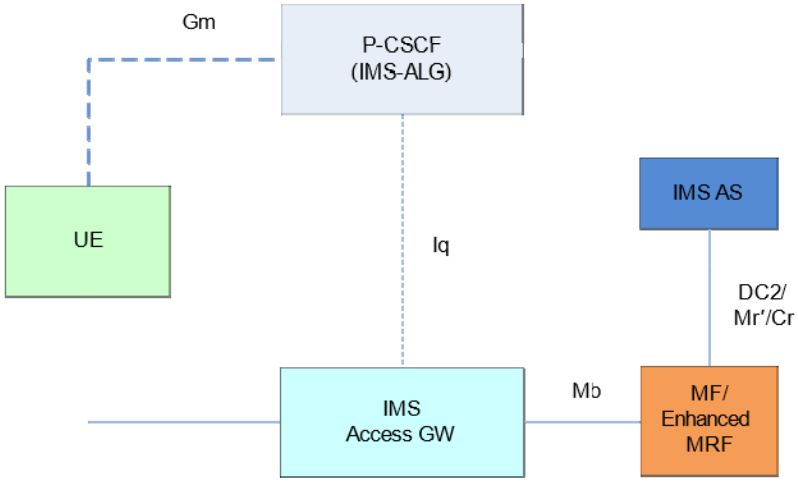


Figure 4.2.5-1: IMS signalling and media plane entities relevant to e2DCe security

4.2.6 E2e security for IMS Data Channels

The end-2-end IMS Data Channel media plane security is established between two UEs or between a UE and a Data Channel Application Server. Details can be found in clauses 6.2.5, 7.2.5 and 7.3.4.

5 IMS media plane security features

5.1 General

The support for IMS media plane security mechanisms and procedures is optional in IMS UEs and its support in the IMS core network is also optional. The support of IMS data channel media is optional. If IMS data channel media is supported, DTLS shall be supported and the following clauses related to IMS data channel media apply..

For the protection of real-time traffic, an IMS UE may support DTLS-SRTP based media plane security mechanism, SDES based media plane security mechanisms, and/or KMS based media plane security mechanism. DTLS-SRTP is only used for e2ae. When an IMS UE supports SDES media plane security mechanisms it shall support procedures for e2ae IMS media plane security and it may support e2e IMS media plane security.

For e2ae protection of MSRP, an IMS UE may support the TLS based media plane security mechanism as defined in section 4.1.2.3

For e2DCe IMS Data Channel media plane security, an IMS UE shall support the DTLS-based media plane security mechanism for IMS data channel as defined in clause 4.1.2.4.

For e2e protection of MSRP, an IMS UE may support the KMS based media plane security mechanism.

For e2e IMS Data Channel media plane security, an IMS UE shall support the DTLS-based media plane security mechanism as defined in clause 4.1.2.5.

5.2 Media integrity protection

The support for IMS media integrity protection is mandatory in an IMS UE supporting IMS media plane security and mandatory in IMS core network elements (i.e., IMS Access Gateway) supporting DTLS-SRTP based, SDES based and/or TLS (MSRP) e2ae IMS media plane security.

The support for IMS media integrity protection is mandatory in an IMS UE supporting IMS media plane security and mandatory in IMS core network elements (i.e., Data Channel Media Function) supporting e2DCe IMS Data Channel media plane security.

The support for IMS media integrity protection is mandatory in an IMS UE and in IMS network elements, supporting e2e IMS Data Channel media plane security.

The use of IMS media integrity protection for RTP is optional, except that RTCP shall be integrity protected using SRTCP, in accordance with RFC 3711 [9].

The use of IMS media integrity protection for MSRP is optional.

The use of IMS media integrity protection for IMS data channel is recommended.

5.3 Media confidentiality protection

The support for IMS media confidentiality protection is mandatory in an IMS UE supporting media plane security and mandatory in IMS core network elements (i.e., IMS Access Gateway) supporting e2ae IMS media plane security.

The support for IMS media confidentiality protection is mandatory in an IMS UE supporting IMS data channel media and mandatory in IMS core network elements (i.e., Data Channel Media Function) supporting e2DCe IMS Data Channel media plane security.

The support for IMS media confidentiality protection is mandatory in an IMS UE supporting IMS data channel media and mandatory in IMS core network elements supporting e2e IMS Data Channel media plane security.

When IMS media plane security is used, SRTP transforms with null encryption should not be used.

When TLS/DTLS is used for IMS media plane security TLS/DTLS profile considerations discussed in annex M of this specification shall be followed.

5.4 Authentication and authorization

5.4.1 Authentication and authorization for e2ae protection

E2ae security implies that no other IMS core network nodes, apart from P-CSCF (IMS-ALG) and IMS Access GW will terminate IMS media security.

The IMS UE and the P-CSCF (IMS-ALG) rely on SIP signalling security to authenticate each other. This is consistent with the fact that the security of the use of SDES and the TLS based solutions entirely rely on SIP signalling security, cf. clause 5.5.

The P-CSCF (IMS-ALG) on the terminating side tells the IMS UE by an explicit indication, cf. clause 7.3.1, that e2ae security is provided, i.e. that the IMS UE shares the media keys with the P-CSCF (IMS-ALG) and not with some other entity. For the originating side see Note 3 in clause 7.2.1. Provided the IMS UE trusts SIP signalling security it can rely on this explicit indication for the following reasons: the IMS UE knows from registration that the P-CSCF (IMS-ALG) is capable of e2ae security, and that such a P-CSCF (IMS-ALG) will remove any such indication if inserted by another party, cf. clauses 7.2.1 and 7.3.1.

In the SDES solution the IMS UE and the IMS Access GW authenticate each other by means of implicit key authentication: the IMS UE believes that only the IMS Access GW can have the media keys to protect the media because it trusts the P-CSCF (IMS-ALG) to give the keys only to the IMS Access GW. Similarly, the IMS Access GW trusts the P-CSCF (IMS-ALG) that the keys are shared only with this IMS UE.

In the DTLS-SRTP and TLS/DTLS solution, mutual authentication between the IMS UE and the IMS Access GW relies on secure transport of certificate fingerprints using SIP signalling integrity protection. If the fingerprints of the certificates used for the TLS/DTLS handshake match the fingerprints transmitted via SIP signalling, then the TLS/DTLS endpoints can be sure that TLS/DTLS is really established between the nodes that exchanged the SIP signalling.

The IMS UE implicitly authorizes the P-CSCF (IMS-ALG) and the IMS Access GW to perform e2ae security by indicating support for e2ae security during the registration in line with the IMS UE's policy, cf. clause 7.1.

Conversely, an IMS UE is always authorized to participate in e2ae security if the network policy allows e2ae security, cf. clause 7.1.

5.4.2 Authentication and authorization for e2e protection using SDES

The originating IMS UE and the terminating IMS UE rely on SIP signalling security to authenticate each other. This is consistent with the fact that the security of the use of SDES entirely relies on SIP signalling security, cf. clause 5.5.

In particular, under the assumption of secure SIP signalling, the originating IMS UE can be assured that the media key it sent reaches only the intended recipient of the SIP messages, except in forking or re-targeting situations where also the endpoints to which the call is forked or re-targeted will see the media key sent by the originating IMS UE. The terminating IMS UE gets different degrees of assurance about the identity of the originating IMS UE it shares a key with, depending on whether the originating IMS UE resides in the same trust domain or not. If it does then the network can assert the sender's identity to the terminating IMS UE, otherwise there will be no such assurance.

Furthermore, if both the originating and the terminating IMS UE are in IMS they know from the absence of indications relating to e2ae security that no IMS network node terminates IMS media security. If one of the UEs is outside the IMS there will be no such assurance.

The originating and the terminating IMS UE implicitly authorize each other to engage in e2e security by sending SDES crypto attributes to each other. Also, in case the originating IMS user chooses anonymity for a session, the terminating IMS UE will not learn the originating user's identity, and vice versa, in case the terminating IMS user chooses anonymity for a session, the originating IMS UE will not learn the terminating user's identity.

In forking and re-targeting scenarios, when the IMS user that finally terminates the session chooses anonymity, the originating IMS user may have no indication to which terminating IMS user the session has been established or even whether the call has been forked or re-targeted at all.

NOTE: An IMS UE can apply certain policies to enhance security in forking and re-targeting scenarios. For example, an IMS UE receiving an answer to an INVITE can check the P-Asserted-Identity field to verify whether the answering user is the called one, and if this is not the case, cancel the current session (and possibly establish a new session directly with the answering user, using new keys). Moreover, an IMS UE can alert the user in case the user has triggered the establishment of a media session using e2e security but the identity of the answering party is not asserted to the IMS UE.

5.4.3 Authentication and authorization for e2e protection using KMS

User authentication and authorization shall be performed as described in Clause 6.2.3.

The KMS can perform policy control regarding e.g. who is allowed to set up connections with secured media to whom. Other ticket features defined in MIKEY-TICKET [14] such as reuse of tickets, forking key generation and terminating side authentication can also be controlled by the KMS.

Authorization of ticket requests to the KMS is based on an authenticated user identity carried in the request message. The user may request a specific type of ticket but the KMS can control the actual settings in the issued ticket.

When the terminating side requests the KMS to resolve a ticket and return the keys to be used, the KMS checks that the terminating user is authorized to resolve the ticket. This authorization is based on information about allowed recipients carried in the ticket and the authenticated identity of the requesting user carried in the request message.

When user authentication is based on GBA, the IMS UE uses its GBA B-TID [6] as authenticated identifier. The NAF-key identified by the B-TID is used for protection of the message exchange.

Mutual authentication between initiating and terminating users is achieved based on trust in the KMS. The terminating side will be assured of the initiating IMS UE identity as its KMS UID, defined in clause 6.2.3.2, will be included in the ticket and ticket integrity will be verified by the KMS and reported back to the requestor. The initiator will get assurance about the identity of the terminating user when receiving the TRANSFER_RESP message. The response message will include a KMS UID representing the entity requesting the KMS to resolve the ticket. The response message is authenticated with a key guaranteeing the authenticity of the KMS UID.

As the KMS based solution only provides e2e security there is no need for control and policing regarding the scope of media protection.

If there is a need in the network to detect that KMS based security solution is used it can be done by inspecting the SDP parts of the SIP signalling, in particular the SDP attribute a=key-mgmt which if present indicates use of MIKEY-TICKET [14] and implicitly then use of the KMS based IMS media plane security functionality.

5.4.4 Authentication and authorization for e2DCe protection

E2DCe security implies that the UE and Data Channel Media Function/MRF terminate IMS Data Channel media security.

In the DTLS solutions for IMS data channels, mutual authentication between the IMS UE and the Data Channel Media Function/MRF relies on secure transport of certificate fingerprints using SIP signalling integrity protection. If the fingerprints of the certificates used for the DTLS handshake match the fingerprints transmitted via SIP signalling, then the DTLS endpoints can be sure that DTLS is really established between the nodes that exchanged the SIP signalling.

The IMS UE implicitly authorizes the P-CSCF (IMS-ALG) and the Data Channel Media Function/MRF to perform e2DCe security by indicating support for e2DCe security during the registration in line with the IMS UE's policy, cf. clause 7.1.

Conversely, an IMS UE is always authorized to participate in e2DCe security if the network policy allows e2DCe security, cf. clause 7.1.

5.4.5 Authentication and authorization for e2e protection using DTLS

E2e security implies that no IMS core network nodes will terminate IMS media security.

In the DTLS solution for IMS data channels, mutual authentication between the originating and terminating IMS UE as well as the originating UE and terminating IMS Data Channel Application Server, relies on secure transport of certificate fingerprints using SIP signalling integrity protection. If the fingerprints of the certificates used for the DTLS handshake match the fingerprints transmitted via SIP signalling, then the DTLS endpoints can be sure that DTLS is really established between the nodes that exchanged the SIP signalling.

An IMS UE is always authorized to participate in e2e security if the network policy allows e2e security using DTLS.

5.5 Security properties of key management, distribution and derivation

5.5.1 General security properties for protection using SDES

SDES requires SIP messages carrying SDES crypto attributes to be secured as SDES provides no security mechanism of its own. Under the assumption that the protocol for securing media, SRTP, is secure the use of SDES provides the same level of security for IMS media where media protection is applied as provided for SIP signalling. In other words, the user may place the same degree of trust in media security as in signalling security.

In IMS, SIP messages are secured in a hop-by-hop fashion. Several alternatives are available for securing SIP messages between the IMS UE and the P-CSCF (IMS-ALG). In particular, IPsec and TLS, as defined in TS 33.203 [4] are specified in 3GPP. Within the IMS core network, security is provided by IPsec or TLS, cf. clause 6.2.

Outside the IMS, at least hop-by-hop TLS as in RFC 3261 is likely to be supported. IMS has no control over how non-IMS SIP providers secure the interfaces between their SIP proxies. This makes SDES appear less secure in a non-IMS environment. On the other hand, service level agreements may give sufficient assurance here.

On the SIP proxies, the keys transported with SDES become visible in plaintext. Therefore, compromise of these proxies will allow not only signalling security, but also media security, to be compromised. However, it should be noted that, even if media security was not applied at all, the proxies would need to be protected anyway to secure SIP signalling for its own sake as SIP signalling security is an important requirement for operators and users. Therefore, the SIP proxies may be assumed to be trusted for this purpose anyhow.

5.5.2 Additional security properties for e2ae protection using SDES

For the e2ae case, there are additional security properties.

The trust in all SIP proxies in the signalling path is required for SDES. However, assuming that strong SIP signalling security, e.g. TLS or IPsec, is used between IMS UE and P-CSCF (IMS-ALG), this difference plays no role for the case of e2ae protection as explained below.

By definition of e2ae protection, the media keys need to be available in the P-CSCF (IMS-ALG) and IMS Access GW in the clear, irrespective of the key management scheme used. And by the assumption of strong SIP signalling security and the fact that there is no SIP proxy between the IMS UE and the P-CSCF (IMS-ALG), no attacker can obtain the media keys by eavesdropping on the interface between the IMS UE and the P-CSCF (IMS-ALG) nor any intermediate SIP proxy, again irrespective of the key management scheme used. Therefore, the attacks relating to compromised intermediate signalling nodes that may apply to the use of SDES for e2e security do not apply to the use of SDES for e2ae security.

When SDES is used for e2ae protection then, in addition to SIP signalling security, also the Iq interface for signalling between the P-CSCF (IMS-ALG), and the media node terminating SRTP towards the UE, i.e. the IMS Access GW, needs to be secured, cf. clause 6.2.1.3.

5.5.3 Security properties for e2e protection using KMS

Key management, distribution and derivation shall be performed as described in Clause 6.2.3. It is performed in accordance with MIKEY-TICKET [14]. In particular the key derivation functions of MIKEY in RFC 3830 [11] are reused.

MIKEY-TICKET [14] extends the concepts from MIKEY in RFC 3830 [11] to cover ticket based key management. The basic exchanges between a user and the KMS used in this specification are security-wise modelled after MIKEY PSK and exhibit the same security properties. These exchanges are performed over HTTP [8] and the security is based on the message security offered by MIKEY-TICKET [14].

The ticket transfer exchange is also modelled after MIKEY PSK but instead of directly using shared keys for message protection and protection of TGKs/TEKs, these keys are carried in the ticket and made available to the users from the KMS. Assuming that the KMS is secure this will render this exchange the same security properties as MIKEY PSK.

Access to KMS is a single source of failure in the system and depending on service requirements, back-up solutions should be considered. It would be possible to replicate the KMS functionality and e.g. use multiple addresses for access.

The KMS and the BSF are critical components in the system and their availability should be protected. Measures to protect against denial of service attacks should be installed.

5.5.4 Security properties for e2ae protection using TLS/DTLS

Based on secure mutual authentication leveraged by the integrity protection of the SIP signalling messages (cf. clause 5.4.1), TLS/DTLS provides secure derivation of session keys to protect the media.

Similarly as for e2ae protection using SDES, in addition to SIP signalling security, also the Iq interface for signalling between the P-CSCF (IMS-ALG), and the media node terminating MSRP/TLS towards the UE, i.e. the IMS Access GW, needs to be secured, cf. clause 6.2.1.3.

TLS/DTLS profile considerations discussed in annex M of this specification shall be followed to support IMS media plane security.

5.5.5 Security properties for e2ae protection using DTLS-SRTP

Based on secure mutual authentication leveraged by the integrity protection of the SIP signalling messages (see clause 5.4.1), DTLS provides secure derivation of session keys to protect the media.

Similarly as for e2ae protection using SDES, in addition to SIP signalling security, also the Iq interface for signalling between the P-CSCF (IMS-ALG), and the media node terminating SRTP towards the UE, i.e. the IMS Access GW, needs to be secured, see clause 6.2.1.3.

DTLS profile considerations discussed in annex M of this specification may be followed to support IMS media plane security.

5.5.6 Security properties for e2DCe protection using DTLS

Based on secure mutual authentication leveraged by the integrity protection of the SIP signalling messages (see clause 5.4.4), DTLS provides secure derivation of session keys to protect the media.

In addition to SIP signalling security, also the Mw, ISC interfaces for signalling between the P-CSCF (IMS-ALG), and the media node terminating the IMS Data Channel towards the UE, i.e. the MF/MRF, needs to be secured. Also, the DC2 or Mr'/Cr interface for signalling between the IMS AS and the Data Channel Media Function or MRF, respectively, needs to be secured, see clause 6.2.4.

DTLS profile considerations discussed in annex M of this specification may be followed to support IMS media plane security.

6 Security mechanisms

6.1 Media security mechanisms

6.1.1 Media security mechanisms for real-time traffic

In this specification, protection for real-time traffic means protection for IMS traffic using the Real-Time Transport Protocol (RTP) or the RTP Control Protocol (RTCP), cf. RFC 3550 [10].

The integrity and confidentiality protection for IMS traffic using RTP shall be achieved by using the Secure Real-Time Transport Protocol (SRTP), RFC 3711 [9]. The integrity and confidentiality protection for IMS traffic using RTCP shall be achieved by using the Secure RTCP protocol (SRTCP), RFC 3711 [9].

A compliant implementation shall support the default transforms and key derivation functions defined in SRTP [9] Additional transforms and key derivation functions may be supported. Annex C and Annex O provide further profiling of SRTP for compliant implementations.

Key management mechanisms for SRTP and SRTCP, as used in this specification, are described in clause 6.2. The key management mechanisms shall provide SRTP master key(s) and master salt(s).

6.1.2 Media security mechanisms for session based messaging (MSRP)

In this specification, protection for session based messaging means protection for IMS traffic using the Message Session Relay Protocol (MSRP) as defined in RFC 4975 [21] and RFC 6714 [24].

The integrity and confidentiality protection for IMS traffic using MSRP is achieved by TLS protection.

Key management mechanisms for MSRP, as used in this specification, are described in clause 6.2.

6.1.3 Media security mechanisms for IMS data channels

In this specification, integrity and confidentiality protection for IMS data channels means protection for IMS traffic using UDP, protected by DTLS, carrying SCTP streams, as defined by RFC 8831 [50], RFC 8841 [48], and RFC 8842 [49].

Key management mechanisms for IMS data channel, as used in this specification, are described in clause 6.2.

6.2 Key management mechanisms for media protection

6.2.1 Key management mechanisms for e2ae protection

6.2.1.1 Endpoints for e2ae protection

The P-CSCF (IMS-ALG) shall handle signalling related to e2ae protection. In particular, the P-CSCF (IMS-ALG) shall terminate the key management protocol and communicate the agreed security context parameters to the IMS Access GW over the Iq interface.

The IMS Access GW shall terminate the protocol for media confidentiality and integrity protection towards the UE as requested by the P-CSCF (IMS-ALG). The IMS Access GW shall send unprotected packets to and receive unprotected

packets from the network, unless other protection mechanisms have been configured to be used in the direction towards the network according to the policies of the operator.

For IMS real-time traffic, the IMS Access GW shall send SRTP and SRTCP packets to and receive SRTP and SRTCP packets from the UE as requested by the P-CSCF (IMS-ALG). The IMS Access GW shall send RTP and RTCP packets to and receive RTP and RTCP packets from the network.

For IMS session based messaging traffic, the IMS Access GW shall send TLS protected MSRP packets to and accept TLS protected MSRP packets from the served UE as requested by the P-CSCF (IMS-ALG). The IMS Access GW shall send MSRP packets to and accept MSRP packets from the network – whether these packets are specifically protected by TLS is up to the policies of the operator.

NOTE: From the IMS access gateway in the direction towards the network, plain TCP may be used on the next hops, assuming that the interfaces are protected e.g. using IPsec or physical protection. Optionally, TLS may be used. The IMS access gateway relays between the TLS connection towards the originating IMS UE and the connection in the direction towards the terminating IMS UE. Usage of TLS from the IMS access gateway towards the network is not covered by this specification.

For the definition of the IMS Access GW cf. TS 23.228 [3].

6.2.1.2 Key management protocol for e2ae protection

The key management protocol for e2ae protection for real-time traffic shall be the DTLS-SRTP as defined in [41] or SDP Security Descriptions (SDES) as defined in [13]. If an IMS UE supports e2ae protection of RTP based media, it shall support SDES, and may support the DTLS-SRTP.

The secure use of the SDP crypto attribute defined in DTLS-SRTP and SDES requires the services of a data security protocol to secure the SDP message. For the use of SDES in IMS, these security services are provided by the SIP signalling security mechanisms applied between the UE and the P-CSCF (IMS-ALG) as defined in TS 33.203 [4]. SIP messages between the UE and the P-CSCF (IMS-ALG) shall be confidentiality-protected either by the confidentiality mechanisms of IPsec or TLS as defined in TS 33.203 [4], or by confidentiality provided by the underlying access network.

The key management mechanism for e2ae protection of MSRP traffic shall be based on certificates and the transmission of certificate fingerprints as defined in RFC 4975 [21].

6.2.1.3 Functional extension of the Iq interface for e2ae protection

6.2.1.3.1 Functional extension of the Iq interface for e2ae protection for RTP

For each RTP media stream to be set-up, the P-CSCF (IMS-ALG) shall send the parameters contained in two specific DTLS-SRTP protection profiles or SDES crypto attributes, cf. RFC 4568 [13], over the Iq interface to the IMS Access GW. On the originating side of the session, these are the DTLS-SRTP protection profile or SDES crypto attribute selected by the P-CSCF (IMS-ALG) from the ones received from the IMS UE in the SDP Offer and the DTLS-SRTP protection profile or SDES crypto attribute generated and inserted by the P-CSCF (IMS-ALG) in the SDP Answer sent to IMS UE, cf. clause 7.2.1. On the terminating side of the session, these are the DTLS-SRTP protection profile or SDES crypto attribute selected by the UE from the ones generated and inserted by the P-CSCF (IMS-ALG) in the SDP Offer sent to IMS UE and the DTLS-SRTP protection profile or SDES crypto attribute received from the IMS UE in the SDP Answer, cf. clause 7.3.1. The P-CSCF (IMS-ALG) shall send the parameters contained in an DTLS-SRTP protection profile or SDES crypto attribute over Iq in such a way that the IMS Access GW is able to uniquely associate the SDES crypto attribute with a media stream.

The IMS Access GW shall, upon reception of an DTLS-SRTP protection profile or SDES crypto attribute, establish an SRTP security context (as described in RFC 4568 [13] and RFC 3711 [9]) and be prepared to convert RTP packets to SRTP packets and vice versa, using the corresponding SRTP security contexts, and send the packets to the UE or receive them from the UE, as described in clause 7.

The confidentiality of the keys sent over the Iq interface is required. The Iq interface shall be protected by NDS/IP [5]. If cryptographic protection is applied to the Iq interface then encryption shall be used.

NOTE: If the P-CSCF (IMS-ALG) and IMS Access GW are located in the same security domain then cryptographic protection is not mandated by NDS/IP. From TS 33.210 [5]: "The Zb-interface is located between SEGs and NEs and between NEs within the same security domain. The Zb-interface is optional for implementation."

6.2.1.3.2 Functional extension of the Iq interface for e2ae protection for MSRP

For each MSRP media stream to be set-up with e2ae security the P-CSCF (IMS-ALG) shall send the certificate fingerprint received from the IMS UE over the Iq interface to the IMS Access GW in a way that the IMS Access GW is able to uniquely associate the fingerprint with a media stream.

Vice versa, for each MSRP media stream to be set-up with e2ae security IMS Access GW shall send the fingerprint of its certificate over the Iq interface to the P-CSCF (IMS-ALG) in a way that the P-CSCF (IMS-ALG) is able to uniquely associate the fingerprint with a media stream.

For protection of session-based messaging traffic, the IMS Access GW shall, upon reception of a certificate fingerprint, use the certificate fingerprint (as described in RFC 4975 [21]) to verify the establishment of the TLS/DTLS session to belong to the served user. When the TLS/DTLS session has been established, the IMS Access GW shall be prepared to convert unprotected MSRP packets to protected MSRP packets and vice versa and send the packets to the UE or receive them from the UE, as described in clause 7.

The integrity of the fingerprints sent over the Iq interface is required. The Iq interface shall be protected by NDS/IP [5]. If cryptographic protection is applied to the Iq interface then integrity protection shall be used. (See also NOTE in 6.2.1.3.1.)

6.2.2 Key management mechanisms for e2e protection using SDES

SDP Security Descriptions (SDES) as defined in [13] may be used for key management for e2e protection for real-time traffic.

The secure use of the SDP crypto attribute defined in SDES requires the services of a data security protocol to secure the SDP message. For the use of SDES in IMS, these security services are provided by the SIP signalling security mechanisms applied between the UE and the P-CSCF as defined in TS 33.203 [4] and between IMS core network elements as defined in TS 33.210 [5] and, for the optional use of TLS, in TS 33.203 [4]. SIP messages between the UE and the P-CSCF shall be confidentiality-protected either by the confidentiality mechanisms of IPsec or TLS as defined in TS 33.203 [4], or by confidentiality provided by the underlying access network. SIP messages between IMS core network elements shall be confidentiality-protected by the confidentiality mechanisms of IPsec or TLS as defined in TS 33.210 [5] and TS 33.203 [4] respectively, or by confidentiality provided by the underlying core network.

NOTE: e2e protection using the key management mechanism described above may also be achieved between an IMS UE and a non-IMS SIP terminal. It is true also for this case that the services of a data security protocol to secure the SDP message are required. However, the means to provide such services in a non-IMS network are outside the scope of this specification.

6.2.3 Key management mechanisms for e2e protection using KMS

6.2.3.1 General

The KMS based security mechanism may be used for e2e protection of both real-time traffic and session based messaging (MSRP),

The key management mechanisms are defined by MIKEY-TICKET [14] and the profiling of tickets and procedures as given in this specification. Annex D specifies the default implementation of KMS based IMS media plane security and use of GBA for user authentication and establishment of a shared key between KMS and IMS UE.

MIKEY-TICKET [14] contains up to three message exchanges. The first exchange is called Ticket Request and is between the initiating user and the KMS. The second exchange is called Ticket Transfer and is between initiating and terminating users. The third exchange is called Ticket Resolve and is between the terminating user and the KMS. The exchanges and the messages in the exchanges are illustrated in Figure 3. In MIKEY-TICKET [14] the three parties involved in the message exchanges are called Initiator, KMS and Responder, respectively.

Depending on the KMS policy, some message exchanges may be omitted. For example, if the KMS policy indicates that the initiator generates the ticket without the assistance of KMS (MIKEY-TICKET mode 3, cf. [14]), the Ticket Request message exchange, i.e. the REQUEST_INIT and REQUEST_RESP messages will be omitted.

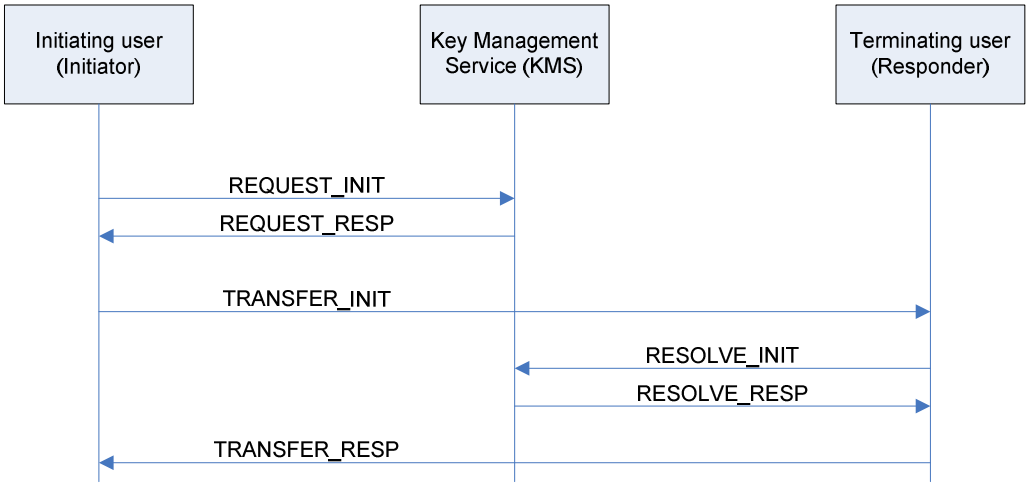


Figure 3: MIKEY-TICKET message exchanges

6.2.3.2 KMS user and user group identities

Users of the KMS based security solution shall have at least one public SIP-URI formatted identity. The NAI part (username@domain) of this identity is used for user identification and authentication in the key management system. This identity is called the KMS UID.

KMS UIDs are used to identify the user to which a ticket is issued and the allowed recipients of the ticket, i.e. the (set of) user(s) which are allowed to resolve the ticket and receive the associated keys. This information is included in the ticket.

User groups for key management purposes can be defined by wild-carding of KMS user identities. The character ? (question mark) is used as the wild card character and matches zero or more occurrences of arbitrary characters. A string formatted as a KMS UID and which includes at least one occurrence of the wild card character is called a KMS user group identity. The KMS user group identity ?.department@company.example thus defines the group of users that have a KMS user identity matching the wild-carded string and the group would include e.g. user1.department@company.example and user2.department@company.example. Another example is the group of all users which would be designated as ?@? or just ?. By appropriate assignment of public IMS UIDs varying group structures can be implemented.

6.2.3.3 IMS UE local policies

The use of the KMS based security solution is at the users' discretion; its use may be controlled by a local policy in the IMS UE and the functionality may be access protected by e.g. a password. The local policy may also control if and when reusable tickets are allowed, if and when group tickets shall be requested and which group a ticket shall be issued for. Furthermore, it may define under which conditions a received ticket shall be accepted. The local policy in the IMS UE should be in agreement with the global policy applied by the KMS.

Local policies may also control how and when warning messages are issued to the user.

6.2.3.4 Ticket data

6.2.3.4.1 Ticket format

The ticket format used in KMS based IMS media plane security is according to the base ticket format in MIKEY-TICKET [14] with the profiling defined in Annex D.

MIKEY-TICKET [14] defines a Ticket Type value (2) for 3GPP usage. Subtypes and versions of this ticket type are defined by 3GPP and shall be specified in this specification, clause 6.2.3.4.2.

6.2.3.4.2 Allocation of ticket subtype and version for ticket type 2

Table 1: Allocation of ticket subtype and versions values

Subtype	Version	Defined in
0	0	Reserved
1	1	Annex D in this specification

6.2.3.5 Authentication of public identities in REQUEST_INIT and RESOLVE_INIT

When the KMS receives a REQUEST_INIT or RESOLVE_INIT request, the KMS needs to verify that the user issuing the request is authorized to do so. This verification is based on authentication of the requesting user's KMS UID.

When GBA is used, the user issuing the request is identified according to GBA procedures by the GBA B-TID carried in the request message to the KMS. The KMS uses the B-TID to request the the NAF-Key used to protect the request and USS information containing a list of all IMPUs, which are associated with the user. The KMS then uses the list of IMPUs to derive all KMS UIDs associated with the requesting user. The KMS verifies that the KMS UID carried in the request is one of the derived identities. For RESOLVE_INIT, the KMS verifies that among the derived KMS UIDs, there is at least one (may not be the one carried in the request) matching the allowed recipient(s) identity in the ticket.

If a caller requests a ticket based on the identity of the expected responder, the call will most likely fail if the IMS network decides to divert the call to another destination. To handle call diversion it is recommended to set the allowed recipient in tickets to the wildcarded identity ?@?. This doesn't affect the security of the solution since keys returned by the KMS are always forked based on the resolver's identity.

When an alternative system for KMS user authentication and key establishment is used it shall provide authentication of the requesting user's KMS UID.

6.2.3.6 Authentication of terminating user identity

In IMS media plane security MIKEY-TICKET shall use key forking (see MIKEY-TICKET [14]) for authentication of terminating users. Key forking will provide authentication of terminating user identity. The TRANSFER_RESP message shall contain a KMS UID associated with the terminating user. The response message is authenticated with a key guaranteeing the authenticity of the KMS user identity.

6.2.3.7 Reusable tickets

Reusable tickets are allowed and their use is controlled by KMS and IMS UE local policies.

A ticket can be issued as a reusable ticket. That a ticket is reusable has two meanings. For the user that requested the ticket, it means that the user can use the same ticket for setting up multiple calls with the intended recipient, usually within a specified time period. For the ticket recipient, it means that the ticket identity and the associated keys can be stored so that the recipient does not have to request keys from the KMS each time the ticket is received. It is however not required that reusable tickets are stored. Local policy may e.g. for capacity limited devices determine not to store such tickets. It is always allowed to resolve the ticket at the time the ticket is received.

Tickets that are not reusable shall be resolved when received at the terminating side.

6.2.3.8 Signalling between KMSs

Users served by different KMSs (KMS_I, KMS_R) may establish connections that provide e2e security provided that the KMSs cooperate and that there is a trust relation between them. The KMSs shall be mutually authenticated and the signalling between them shall be integrity and confidentiality protected. If KMS_R cannot resolve a ticket, but has a trust relation with KMS_I that can resolve the ticket, KMS_R initiates a new ticket resolve exchange with KMS_I. The response message from KMS_I is then re-encoded by KMS_R and forwarded to the responder as described in Annex B. The message exchange shall be done as described in Section 10 of [14]. The exchanges and the messages in the exchanges are illustrated in Figure 4. Note that this introduces a hop-by-hop trust chain as only KMS_R authenticates the user (responder) and KMS_I will have to trust KMS_R.

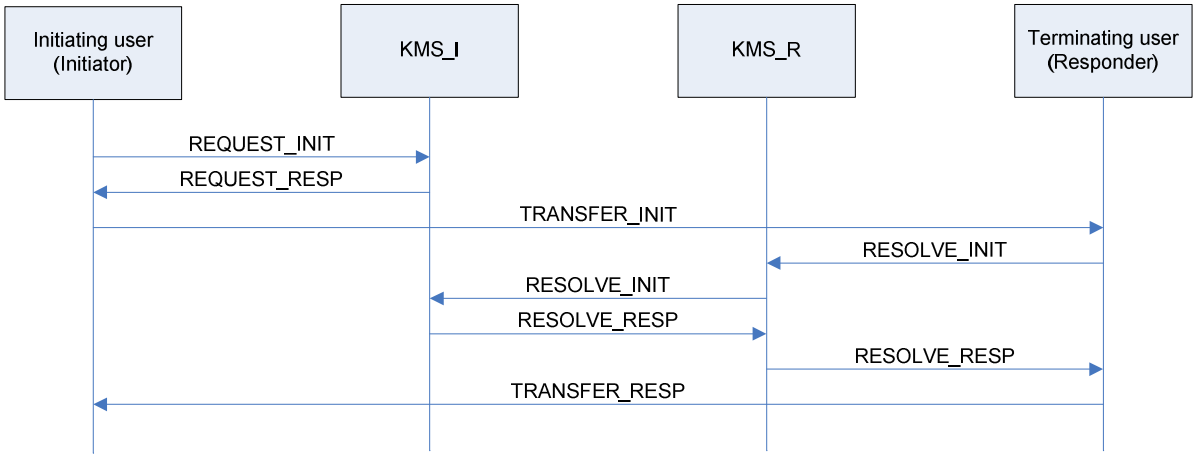


Figure 4: MIKEY-TICKET message exchanges between KMSs

6.2.4 Key management mechanisms for e2DCe protection

6.2.4.1 Endpoints for e2DCe protection

For IMS Data Channel traffic terminated by the MF/MRF, the MF/MRF shall send DTLS-protected SCTP packets to and accept DTLS-protected SCTP packets from the served UE as requested by the IMS AS via the P-CSCF.

For the definition of the Data Channel Media Function/MRF cf. TS 23.228 [3].

6.2.4.2 Key management protocol for e2DCe protection

The key management mechanism for e2DCe protection of IMS data channel traffic shall be based on certificates and the transmission of certificate fingerprints as defined in RFC 8841 [48] and RFC 8842 [49].

6.2.4.3 Functional extension of the Mw, ISC, and Mr'/Cr or DC2 interfaces for e2DCe protection

6.2.4.3.1 Functional extension of the Mw, ISC, and Mr'/Cr or DC2 interfaces for e2Dce protection for IMS data channel

For each IMS data channel media stream to be set-up with e2DCe security the P-CSCF shall send the certificate fingerprint received from the IMS UE over the Mw interface to the S-CSCF in a way that the S-CSCF is able to uniquely associate the fingerprint with a media stream. For IMS data channel media streams to be set-up with e2DCe security, the S-CSCF and IMS AS shall send the certificate fingerprint received from the IMS UE over the DC2 or Mr'/Cr or DC2 interface, respectively, to the MF/MRF in a way that the MF/MRF is able to uniquely associate the fingerprint with a media stream.

For each IMS data channel media stream to be set-up with e2DCe security the MF/MRF shall send the fingerprint of its certificate over the Mr'/Cr or DC2 interface to the S-CSCF in a way that the S-CSCF is able to uniquely associate the fingerprint with a media stream. For each IMS data channel media stream to be set-up with e2DCe security S-CSCF shall send the fingerprint of the MF/MRF certificate over the Mw interface to the P-CSCF in a way that the P-CSCF is able to uniquely associate the fingerprint with a media stream.

For protection of session-based messaging traffic and IMS data channel traffic, the MF/MRF shall, upon reception of a certificate fingerprint, use the certificate fingerprint (as described in RFC 8841 [48]) to verify the establishment of the DTLS session to belong to the served user. When the DTLS session has been established, the MF/MRF shall be prepared to convert unprotected SCTP packets to protected SCTP packets and vice versa and send the packets to the UE or receive them from the UE, as described in clause 7.

The integrity of the fingerprints sent over the Mw and Mr'/Cr or DC2 interfaces is required. The Mw and Mr'/Cr or DC2 interfaces shall be protected by NDS/IP [5]. If cryptographic protection is applied to the Mw and Mr'/Cr or DC2 interfaces then integrity protection shall be used.

NOTE: If the P-CSCF (IMS-ALG), S-CSCF and MF/MRF are located in the same security domain then cryptographic protection is not mandated by NDS/IP. From TS 33.210 [5]: "The Zb-interface is located between SEGs and NEs and between NEs within the same security domain. The Zb-interface is optional for implementation."

7 Security association set-up procedures for media protection

7.1 IMS UE registration procedures

7.1.1 Indication of support for e2ae security for RTP based media

The IMS UE performs an IMS registration according to 3GPP TS 23.228 [3], with modifications as described in the following. When performing the registration, an IMS UE supporting the mechanisms required for e2ae protection according to this specification shall include an indication "e2ae-security supported by UE" in the initial REGISTER message unless the IMS UE's policy dictates otherwise.

When receiving indication "e2ae-security supported by UE" in the initial REGISTER message from the IMS UE the P-CSCF (IMS-ALG) shall store it.

When the P-CSCF (IMS-ALG) is capable of supporting the mechanisms required for e2ae protection according to this specification, and the network policy is to prefer e2ae protection for this registration, the P-CSCF (IMS-ALG) shall include an indication "e2ae-security supported by network" in a message to the IMS UE during registration. The IMS UE shall store this indication for use with originating session set-up procedures.

NOTE 1: The names "e2ae-security supported by UE" and "e2ae-security supported by network" of the above indications are just placeholders for the purposes of this specification. Their syntax is defined in the corresponding stage 3 specification. These names refer to the RTP case only. Separate names for MSRP and BFCP are introduced from Rel-12 onwards, cf. clause 7.1.2 and Annex G of the present document.

NOTE 2: The network policy regarding e2ae protection could differ e.g. depending on the type of access network. Therefore, the policy may depend on the registration. This does not imply that the network policy depends on the individual subscription.

When an IMS UE initiates a session and both the IMS UE and the P-CSCF (IMS-ALG) have indicated support of e2ae security for RTP, then the IMS UE shall secure all RTP media streams, either e2ae or e2e. When a P-CSCF (IMS-ALG) on the terminating side receives an INVITE for an RTP stream and the P-CSCF (IMS-ALG) and the terminating IMS UE have indicated support of e2ae security for RTP, the P-CSCF (IMS-ALG) shall secure all unprotected RTP streams towards the terminating IMS UE. A request for e2ae security from an IMS UE is only allowed if both the IMS UE and P-CSCF (IMS-ALG) have indicated support of e2ae security. On the terminating side, the P-CSCF (IMS-ALG) is only allowed to initiate e2ae security if both IMS UE and P-CSCF (IMS-ALG) have indicated support of e2ae security.

NOTE 3: A session may contain a mixture of protected (e2ae and/or e2e) and unprotected media streams/sessions.

7.1.2 Indication of support for e2ae security for MSRP

Support for e2ae security for MSRP is indicated during registration in the same way as for RTP based media, cf. clause 7.1.1. It is done independently from the indication of support for e2ae security for RTP based media, and uses its own indications" e2ae- security for MSRP supported by the UE" and" e2ae-security for MSRP supported by the network" (the syntax is to be defined in the corresponding stage 3 specification).

NOTE1: The policies of the IMS UE and the network concerning the use of e2ae security for MSRP are independent from the policies concerning the use of e2ae security for RTP based media.

NOTE2: For compatibility with RCS 5.1, t he indication of support for e2ae security during registration is not a necessary prerequisite for the use of e2ae security, but it helps to avoid certain error cases, cf. Clause 7.2.1 and Clause 7.3.1.

7.1.3 Indication of support for e2DCe security for IMS data channel

Support for e2DCe security for IMS data channel is indicated during registration in the same way as for RTP based media, cf. clause 7.1.1. It is done independently from the indication of support for e2ae security for other media and uses its own indications "e2DCe-security for IMS data channel supported by the UE" and "e2DCe-security for IMS data channel supported by the network" (the syntax is to be defined in the corresponding stage 3 specification).

NOTE: The policies of the IMS UE and the network concerning the use of e2DCe security for IMS data channel are independent from the policies concerning the use of e2ae security.

7.2 IMS UE originating procedures

7.2.1 IMS UE originating procedures for e2ae

Figure 7.2.1-1 shows the originating session set-up procedures for one or more media stream(s) using e2ae security.

NOTE: The procedures shown in the figure apply to users located in their home service area. The same concepts apply to roaming users.

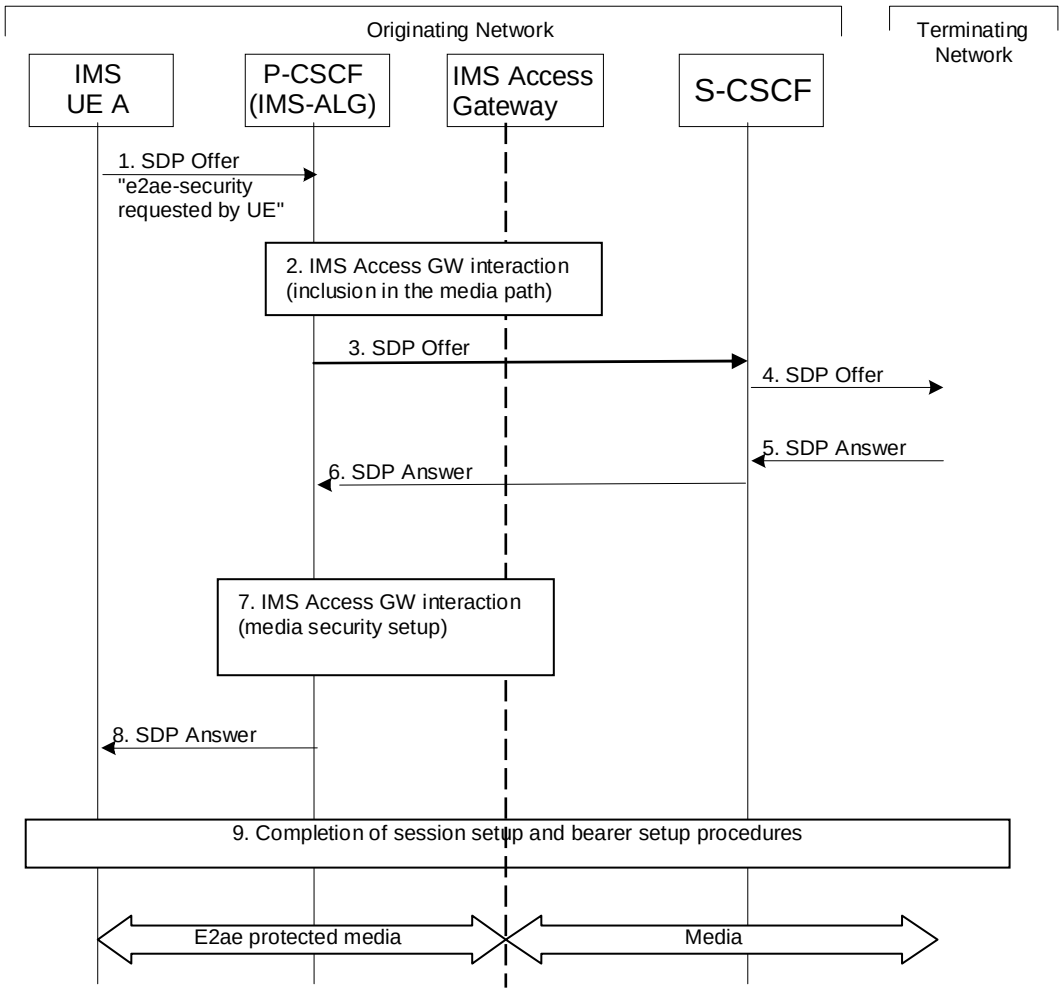


Figure 7.2.1-1: Originating call flow for e2ae case

The IMS UE A performs an IMS originating session set-up according to 3GPP TS 23.228 [3], with modifications as described in the following. If both IMS UE and network indicated support for e2ae security for RTP based traffic during registration, then the IMS UE shall request e2ae security for RTP media streams to be established as described in this clause, unless the IMS UE initiates a procedure for e2e security for a RTP media stream. If both IMS UE and network indicated support for e2ae security for MSRP during registration, then the IMS UE shall request e2ae security for

MSRP media streams to be established as described in this clause, unless the IMS UE initiates a procedure for e2e security for an MSRP media stream.

The originating procedures for establishing media streams with e2e security are described in clauses 7.2.2 (for RTP only) and 7.2.3 of this specification. The IMS UE may learn of a preference for e2e security for a particular session or media stream by explicit user action via the user interface or by the security policy implemented on the IMS UE.

The procedure in the above figure for requesting e2ae security for a media stream is now described step-by-step.

1. IMS UE A sends an SDP Offer for a media stream containing cryptographic information, together with an indication "e2ae-security requested by UE", to the P-CSCF (IMS-ALG).

   For e2ae protection of RTP using SDES, the cryptographic information contained in the SDP Offer consists of one or more SDES crypto attributes, each of these containing at least one master key K11, and other security context parameters chosen by IMS UE A in accordance with RFC 4568 [13]. The optional key lifetime field shall be omitted. For e2ae protection of DTLS-SRTP, the SDP Offer contains a setup attribute controlling DTLS roles and a fingerprint computed from UE A certificate, in accordance with RFC 5763 [40].

NOTE 1: The omission of the key lifetime field is, according to RFC 4568 [13], a way to implicitly signal the default values for the key lifetime as defined in RFC 3711 [9]. The default values are 2^48 SRTP packets and 2^31 SRTCP packets

   For e2ae protection of MSRP the cryptographic information contained in the SDP Offer consists of the fingerprint of the certificate of IMS UE A in accordance to RFC 4975 [21]. For e2ae protection of WebRTC data channel the cryptographic information contained in the SDP Offer consists of the fingerprint of the certificate of IMS UE and the TLS ID identifier, in accordance with RFC 8841 [48].

2. For each media stream that uses transport " RTP/SAVP ", "RTP/SAVPF", "TCP/TLS/MSRP", or "UDP/DTLS/SCTP", the P-CSCF (IMS-ALG) checks for the presence of the indication "e2ae-security requested by UE".

   If the indication is present and the P-CSCF (IMS-ALG) indicated support of e2ae-security for the respective protocol (RTP, and/or MSRP, and/or WebRTC data channel) during registration, the P-CSCF (IMS-ALG) allocates the required resources, includes the IMS Access GW in the media path and proceeds as specified in this clause. If the indication is not present for an SRTP media stream the P-CSCF (IMS-ALG) proceeds for this media stream as described in clause 7.2.2 or clause 7.2.3 of the present specification.

   If the indication is not present for an MSRP media stream offered with transport "TCP/TLS/MSRP", the P-CSCF (IMS-ALG) should proceed for this media stream as described in clause 7.2.3 of the present specification or in TS 23.228 [3] and skip the further steps in the present subclause. If compatibility with RCS 5.1 [27] is desired, a P-CSCF may, based on local policy, allocate the required resources, include the IMS Access GW in the media path and proceed as specified in this clause.

NOTE 1a: According to the above, an operator can choose to terminate TLS in the IMS Access GW according to the following steps for all media streams that are signalled in SIP INVITE messages with transport TCP/TLS/MSRP and a certificate fingerprint attribute, even if the UE did not indicate support for e2ae security during registration and did not indicate usage of e2ae security for the respective media streams in the INVITE. This can lead to session failures for pre-Rel-12 IMS UEs or non-IMS UEs due to a mismatch of security parameters sent by the network and expected by the UE, but on the other hand, it will ensure compatibility with RCS 5.1 [27], which specifies that TLS for MSRP is always terminated in the network. It is therefore advantageous that IMS UEs compliant to the present specification use indications if they want to establish e2ae security for MSRP rather than relying on the network to terminate TLS even if no indication is present.

NOTE 2: The inclusion of the IMS Access GW in the media path is required for the purposes of e2ae security even if it was not required otherwise.

NOTE 2a: If an indication for e2ae security for a media stream is present in an SDP offer but the support for e2ae security for the respective protocol was not successfully established during registration then this is an error case.

3. The P-CSCF (IMS-ALG) modifies the SDP offer before sending it towards the S-CSCF.

For e2ae protection of RTP using SDES, the P-CSCF (IMS-ALG) changes the transport from SRTP to RTP in the SDP Offer, selects one SDES crypto attribute and removes all received SDES crypto attributes and the indication "e2ae-security requested by UE" from the SDP Offer

For e2ae protection of MSRP, the P-CSCF (IMS-ALG) shall change the transport from "TCP/TLS/MSRP" to "TCP/MSRP" in the SDP Offer (cf., however, NOTE 4), stores the received fingerprint of the IMS UE A certificate and removes it as well as the indication "e2ae-security requested by UE" from the description of the media stream in the SDP Offer if present.

The P-CSCF (IMS-ALG) then sends the changed SDP offer towards the S-CSCF.

4. The S-CSCF performs the required procedures according to TS 23.228 [3] and forwards the SDP Offer to the terminating network.

5. The S-CSCF receives the SDP Answer from the terminating network.

6. The S-CSCF forwards the SDP Answer to the P-CSCF (IMS-ALG).

7. The P-CSCF (IMS-ALG) and the IMS Access GW exchangethe cryptographic information.

   For e2ae protection of RTP using SDES this requires that the P-CSCF (IMS-ALG) creates one SDES crypto attribute, containing at least one master key K12, and other security context parameters chosen by the P-CSCF (IMS-ALG) in accordance with RFC 4568 [13], for protecting the RTP media stream towards IMS UE A between the IMS Access GW and IMS UE A. The P-CSCF (IMS-ALG) communicates the parameters contained in the SDES crypto attribute selected in step 3 as well as those in the SDES crypto attribute created in step 7 to the IMS Access GW. The P-CSCF (IMS-ALG) instructs the IMS Access GW to check integrity / decrypt the media stream arriving from IMS UE A using K11 (and possibly further master keys), to integrity protect / encrypt the media stream arriving from the terminating network using K12 (and possibly further master keys), and to set the key lifetime to the default values as defined in RFC 3711 [9].

   For e2ae protection of MSRP the cryptographic information communicated by the P-CSCF (IMS-ALG) to the IMS Access GW consists of the fingerprint of the UE´s certificate in accordance to RFC 4975 [21]. The P-CSCF (IMS-ALG) instructs the IMS Access GW to verify during the subsequent TLS handshake with the IMS UE (see step 9) that the fingerprint of the certificate passed by the IMS UE during this TLS handshake matches the fingerprint passed by the P-CSCF (IMS-ALG) to the IMS Access GW. In turn, the IMS Access GW communicates the fingerprint of the certificate it is going to use for setting up protection for this media stream to the P-CSCF (IMS-ALG).

8. The P-CSCF (IMS-ALG) modifies the SDP Answer before sending it to the IMS UE A.

   For e2ae protection of RTP, the P-CSCF (IMS-ALG) shall change the transport from RTP to SRTP in the SDP Answer and includes the SDES crypto attribute created in step 7. The optional key lifetime field shall be omitted.

   For e2ae protection of MSRP, the P-CSCF (IMS-ALG) shall set the transport to "TCP/TLS/MSRP" , remove any fingerprint attributes in the SDP Answer, if present, and include the fingerprint of the IMS Access GW´s certificate in accordance to RFC 4975 [21].

   The P-CSCF (IMA-ALG) then sends the updated SDP Answer to IMS UE A. After receiving this message, IMS UE A completes the media security setup.

NOTE 3: The IMS UE can deduce that e2ae security is used from two facts: first, that the P-CSCF (IMS-ALG) indicated its support for e2ae security during registration, and second, that the IMS UE requested e2ae-security in the SDP Offer.

9. In case of RTP, when the full session setup has been completed, and media can be sent, the protected media stream is sent between IMS UE A and the IMS Access GW. IMS UE A integrity protects / encrypts and checks integrity / decrypts the media stream sent to and received from the network. The IMS Access GW checks integrity / decrypts the media stream arriving from IMS UE A before passing it on towards the terminating network. The IMS Access GW integrity protects / encrypts the media stream arriving from the terminating network before passing it on to IMS UE A.

   In case of MSRP, when the full session setup has been completed, the TCP and TLS connection shall be established between the IMS UE and the IMS Access GW. When subsequently media are sent from or to the IMS UE, the IMS Access GW performs the required TLS specific cryptographic operations on the media.

NOTE 4: In case cryptographic protection is also used in the core network, the IMS Access GW will also perform the necessary functions for this additional cryptographic protection. A network may have for example the policy to use TLS for MSRP also inside the core network. In this case, when e2ae security is used, TLS has to be established also from the IMS Access GW towards the core network. This may require enhancements to the procedure described above but is outside of the scope of this specification.

7.2.2 IMS UE originating procedures for e2e using SDES

Figure 7.2.2-1 shows the originating call set-up procedures for one RTP media stream using SDES based e2e security.

NOTE 1: The procedures shown in the figure apply to users located in their home service area. The same concepts apply to roaming users.

NOTE 2: E2e protected RTP sessions and/or media streams are set-up without IMS-ALG support, which means that such sessions can be set-up in networks not providing the IMS-ALG functionality in the P-CSCF.

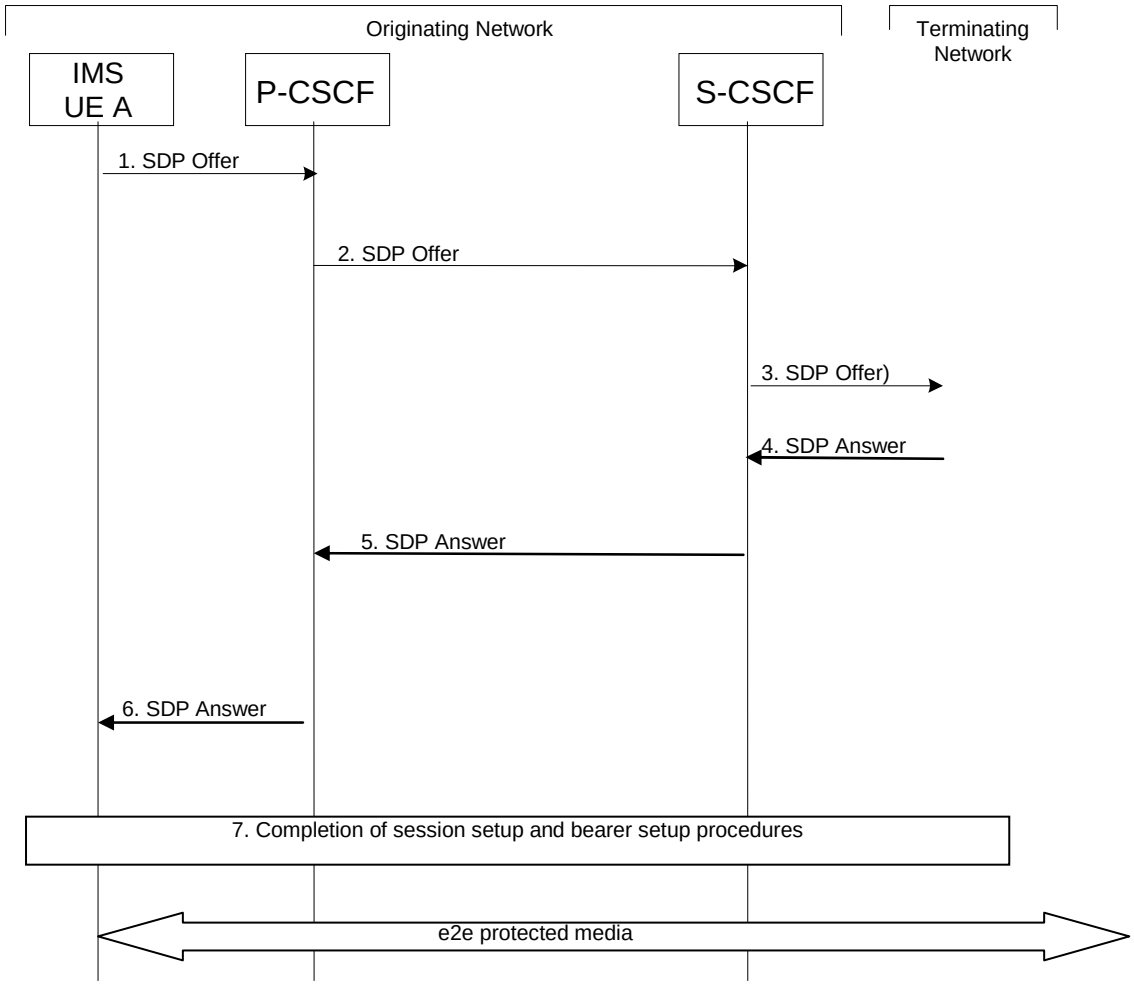


Figure 7.2.2-1: Originating call flow for e2e case using SDES

The IMS UE performs an IMS originating session set-up according to 3GPP TS 23.228 [3], with modifications as described in the following. The IMS UE may learn of a preference for e2e-security for a particular RTP media stream/session using a particular key management protocol by explicit user action via the user interface or by the security policy implemented on the IMS UE.

NOTE 3: The procedure described here is the same as for legacy UEs not fully conforming to this specification, which can also use SDES to establish e2e security.

The procedure in the above figure is now described step-by-step.

1. IMS UE A sends an SDP Offer for an SRTP stream containing one or more SDES crypto attributes to the P-CSCF. Each of these SDES crypto attributes contains at least one master key K1, and other security context parameters chosen by IMS UE A in accordance with RFC 4568 [13]. IMS UE A does not include any indication regarding the required security scope, i.e. e2e security or e2ae security.

2. If the P-CSCF supports e2ae security, the P-CSCF (IMS-ALG) checks for the presence of the indication "e2ae-security requested by UE". As the indication is not present, the P-CSCF forwards the SDP offer towards the S-CSCF. If an indication is present the P-CSCF proceeds as described in clause 7.2.1 of this specification.

3. The S-CSCF performs the required procedures according to TS 23.228 [3] and forwards the SDP Offer to the terminating network.

4. The S-CSCF receives the SDP Answer from the terminating network containing one SDES crypto attribute with at least one master key K2, and other security context parameters chosen by IMS UE B in accordance with RFC 4568 [13].

5. The S-CSCF forwards the SDP Answer to the P-CSCF.

6. The P-CSCF forwards the SDP Answer to IMS UE A. After receiving this message IMS UE A completes the media security setup.

7. When the full session setup has been completed, and media can be sent, the protected RTP media stream is sent between IMS UE A and IMS UE B. IMS UE A integrity protects / encr ypts the media stream sent towards IMS UE B using key K1 (and possibly further master keys) from the crypto attribute selected by IMS UE B and checks integrity / decrypts the media stream arriving from IMS UE B using key K2 (and possibly further master keys).

7.2.3 IMS UE originating procedures for e2e using KMS

Figure 7.2.3-1 shows the originating call set-up procedures for one RTP or one MSRP session using KMS based security.

NOTE 1: The procedures shown in the figure apply to users located in their home service area. The same concepts apply to roaming users.

NOTE 2: E2e protected RTP or MSRP sessions are set-up without IMS-ALG support, which means that such sessions can be set-up in networks not providing the IMS-ALG functionality in the P-CSCF.

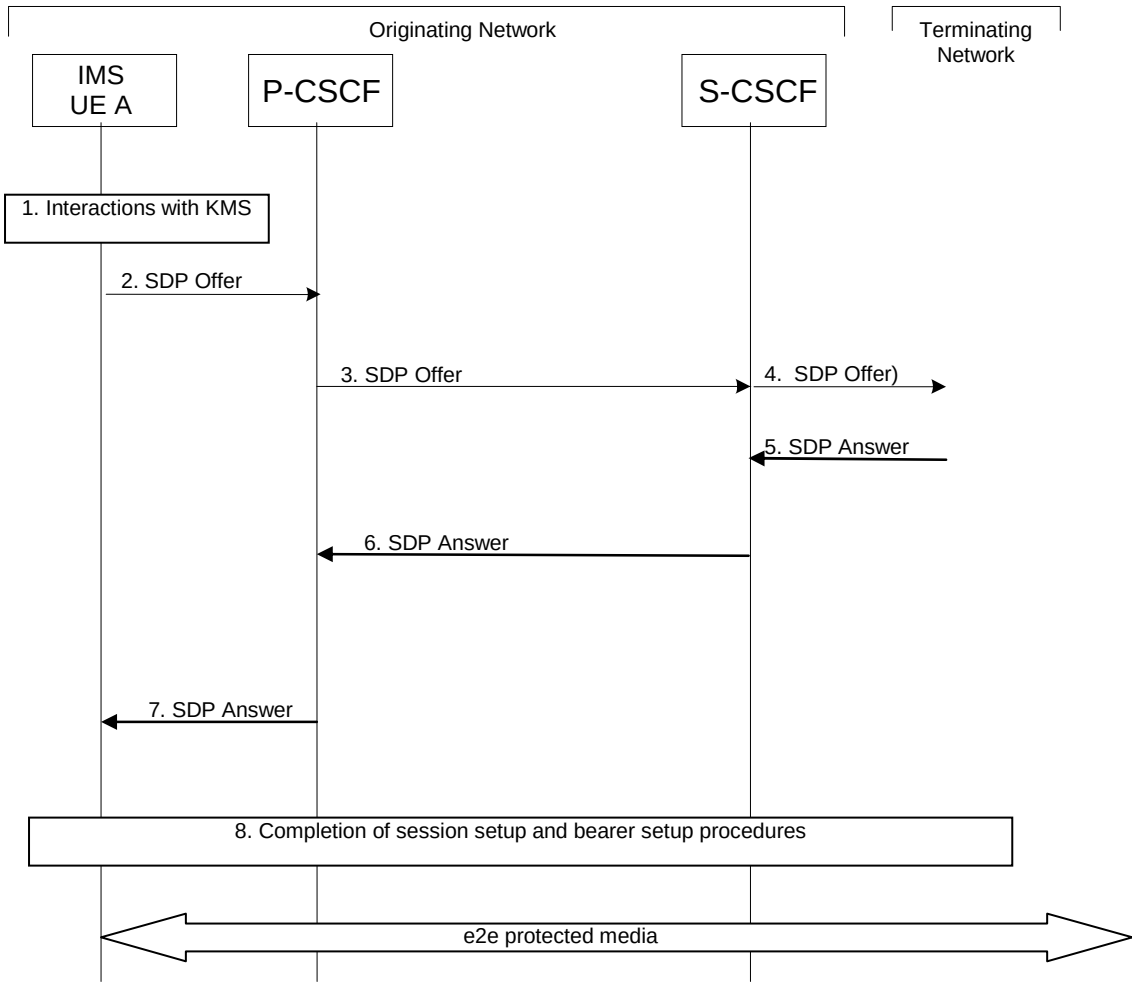


Figure 7.2.3-1: Originating call flow for e2e case using KMS

The IMS UE performs an IMS originating session set-up according to 3GPP TS 23.228 [3], with modifications as described in the following. The IMS UE may learn of a preference for e2e-security for a particular session using a particular key management protocol by explicit user action via the user interface or by the security policy implemented on the IMS UE. KMS interactions are described in clause 6.2.3.1. Details of the KMS based key management are given in Annex B.

The procedure in the above figure is now described step-by-step.

1. Depending on KMS and local policy, the IMS UE A will either interact with the KMS to obtain keys and a MIKEY-TICKET Ticket usable for IMS UE B, or it will create the ticket by itself. In the latter case, MIKEY-TICKET [14] mode 3 is used, and IMS UE A will then perform all key and ticket generation functions otherwise performed by the KMS. The ticket is protected with a key, e.g. a NAF-key that the IMS UE shares with the KMS.

2. IMS UE A sends an SDP offer for an RTP or MSRP session containing a MIKEY-TICKET offer for IMS UE B to the P-CSCF.

3. If the P-CSCF supports e2ae security, the P-CSCF (IMS-ALG) checks for the presence of the indication "e2ae-security requested by UE". As the indication is not present, the P-CSCF forwards the SDP offer towards the S-CSCF.

4. The S-CSCF performs the required procedures according to TS 23.228 [3] and forwards the SDP offer to the terminating network.

5. The S-CSCF receives the SDP answer from the terminating network containing a MIKEY-TICKET response.

6. The S-CSCF forwards the SDP answer to the P-CSCF.

7. The P-CSCF forwards the SDP answer to IMS UE A. After receiving this message the IMS UE A checks that the responder is authorized before completing the media security setup.

8. IMS UE-A derives the media session keys and initiates the media plane security. For an RTP session this means sending and receiving SRT(C)P streams and for an MSRP session this means setting up a TLS-PSK tunnel to protect the MSRP messages.

7.2.4 IMS UE originating procedures for e2DCe

Figure 7.2.4-1 shows the originating session set-up procedures for one or more media stream(s) using e2DCe security.

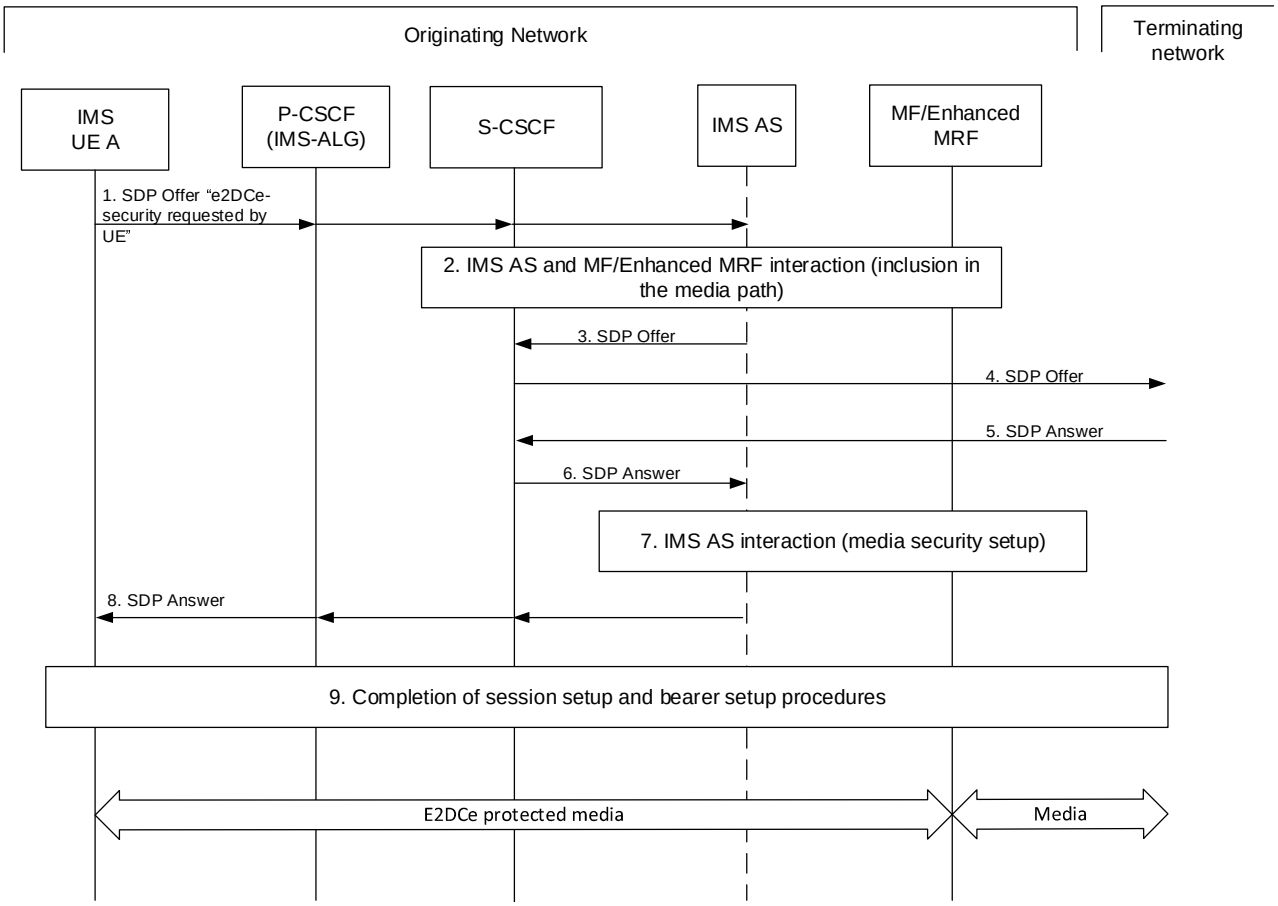


Figure 7.2.4-1: Originating call flow for e2DCe using MF/MRF case

The IMS UE A performs an IMS originating session set-up according to 3GPP TS 23.228 [3], with modifications as described in the following. If both IMS UE and network indicated support for e2DCe security for IMS data channel during registration, then the IMS UE shall request e2DCe security for IMS data channel media streams to be established as described in this clause, unless the IMS UE initiates a procedure for e2e security for an IMS data channel media stream.

The originating procedures for establishing IMS data channels with e2e security are described in clause 7.2.5 of this specification. The IMS UE may learn of a preference for e2e security for a particular session or media stream by explicit user action via the user interface or by the security policy implemented on the IMS UE.

The procedure in the above figure for requesting e2DCe security for a media stream is now described step-by-step.

1. IMS UE A sends an SDP Offer for a media stream containing cryptographic information, together with an indication "e2DCe-security for IMS data channel requested by UE", to the IMS AS via the P-CSCF .

   For e2DCe protection of IMS data channel the cryptographic information contained in the SDP Offer consists of the fingerprint of the certificate of IMS UE and the tls-id attribute, in accordance with RFC 8841 [48].

2. For each media stream that uses transport "UDP/DTLS/SCTP", the P-CSCF (IMS-ALG) checks for the presence of the indication "e2DCe-security for IMS data channel requested by UE".

   If the indication is present and the P-CSCF (IMS-ALG) indicated support of e2DCe-security for IMS data channel during registration, the P-CSCF (IMS-ALG) allocates the required resources, includes the IMS Access GW and Data Channel Media Function/MRF in the media path and proceeds as specified in this clause. If the indication is not present for an IMS data channel media stream, the P-CSCF (IMS-ALG) proceeds for this media stream as described in clause 7.2.5 of the present specification.

NOTE 1: The inclusion of the IMS Access GW and Data Channel Media Function /MRF in the media path is needed for the purposes of e2DCe security even if it was not needed otherwise.

NOTE 2: If an indication for e2DCe security for a media stream is present in an SDP offer but the support for e2DCe security for the respective protocol was not successfully established during registration then this is an error case.

3. The IMS AS sends the SDP offer towards the S-CSCF.

4. For e2DCe protection of IMS Data Channel, the S-CSCF stores the received fingerprint of the IMS UE A certificate, performs the required procedures according to TS 23.228 [3], and forwards the SDP Offer to the terminating network.

5. The S-CSCF receives the SDP Answer from the terminating network.

6. The S-CSCF sends the SDP answer towards the IMS AS.

7. The IMS AS and the Data Channel Media Function/MRF exchange the cryptographic information.

   For e2DCe protection of IMS Data Channel the cryptographic information communicated by the IMS AS to the Data Channel Media Function/MRF consists of the fingerprint of the UE's certificate and tls-id in accordance with RFC 8841 [48]. The IMS AS instructs the Data Channel Media Function/MRF to verify during the subsequent DTLS handshake with the IMS UE (see step 10) that the fingerprint of the certificate passed by the IMS UE during this DTLS handshake matches the fingerprint passed by the IMS AS to the Data Channel Media Function/MRF. In turn, the Data Channel Media Function/MRF communicates the fingerprint of the certificate it is going to use for setting up protection for this media stream to the IMS AS.

8. The S-CSCF forwards the SDP Answer to the P-CSCF (IMS-ALG).

9. The P-CSCF (IMS-ALG) sends the SDP Answer to the IMS UE A. After receiving this message, IMS UE A completes the media security setup.

NOTE 3: The IMS UE can deduce that e2DCe security is used from two facts: first, that the P-CSCF (IMS-ALG) indicated its support for e2DCe security during registration, and second, that the IMS UE requested e2DCe-security in the SDP Offer.

10. In case of IMS data channel, when the full session setup has been completed, the DTLS connection shall be established between the IMS UE and the Data Channel Media Function/MRF. When subsequently media are sent from or to the IMS UE, the UE and the Data Channel Media Function/MRF perform the required DTLS specific cryptographic operations on the media.

7.2.5 IMS UE originating procedures for e2e using TLS/DTLS certificate / fingerprint

Figure 7.2.5-1 shows the originating call set-up procedures for one IMS data channel media stream using DTLS-based e2e security.

NOTE 1: The procedures shown in the figure apply to users located in their home service area. The same concepts apply to roaming users.

NOTE 2: E2e protected IMS data channel sessions and/or media streams are set up without IMS-ALG support, which means that such sessions can be set up in networks not providing the IMS-ALG functionality in the P-CSCF.

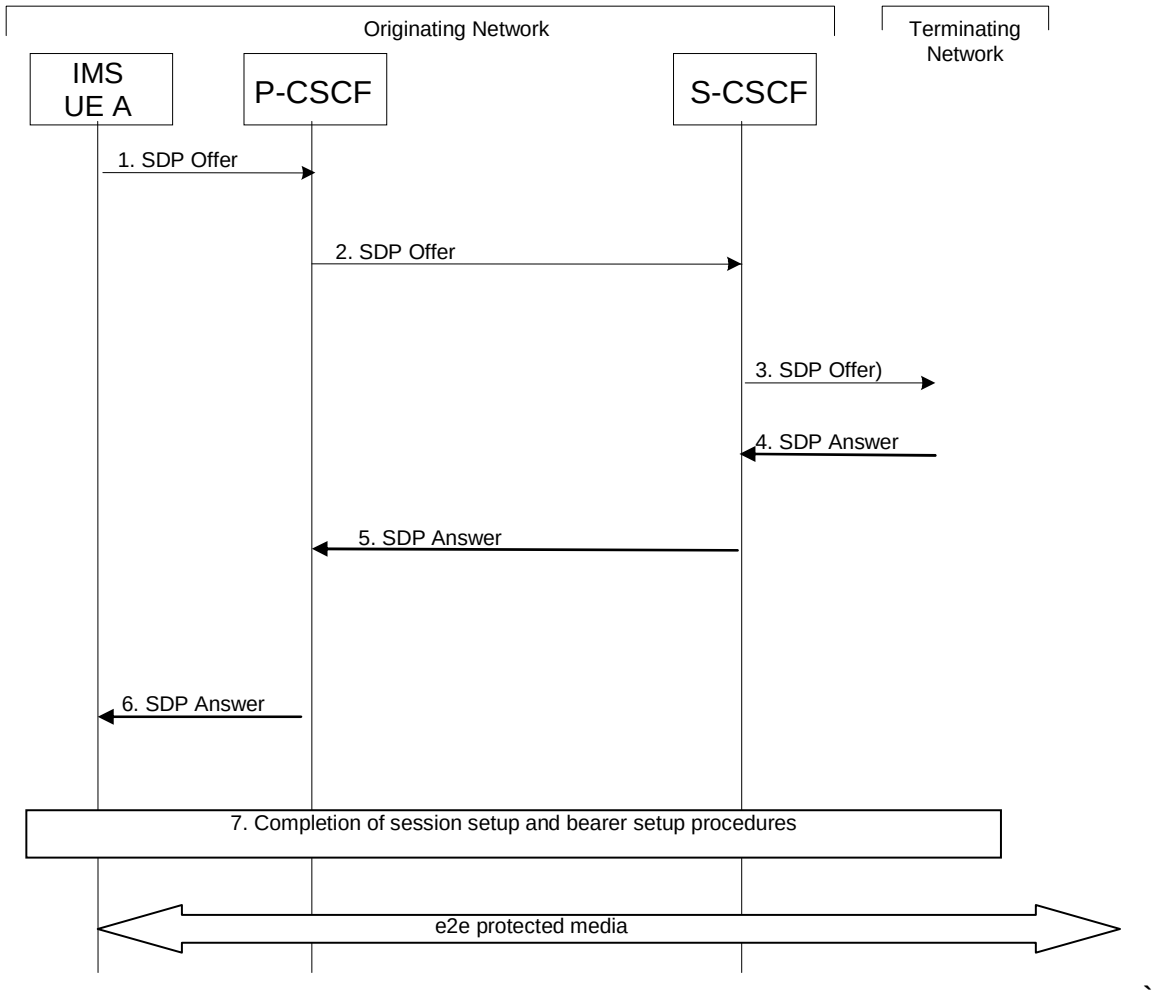


Figure 7.2.5-1: Originating call flow for e2e case using certificate / fingerprint

The IMS UE performs an IMS originating session set-up according to 3GPP TS 23.228 [3], with modifications as described in the following. The IMS UE may learn of a preference for e2e-security for a particular IMS data channel media stream/session using a particular key management protocol by explicit user action via the user interface or by the security policy implemented on the IMS UE.

The procedure in the above figure is now described step-by-step.

1. IMS UE A sends an SDP Offer for an IMS data channel stream containing fingerprint, tls-id, and setup attributes to the P-CSCF, according to RFC 8841 [48]. IMS UE A does not include any indication regarding the required security scope, i.e., e2DCe security, or e2ae security.

2. If the P-CSCF supports e2ae security and/or e2DCe security, the P-CSCF (IMS-ALG) checks for the presence of the indications "e2ae-security requested by UE" and "e2DCe-security for IMS data channel requested by UE". As neither one of the indications is present, the P-CSCF forwards the SDP offer towards the S-CSCF. If an indication is present the P-CSCF proceeds as described in clauses 7.2.1 or 7.2.4 of the present document, respectively.

3. The S-CSCF performs the required procedures according to TS 23.228 [3] and forwards the SDP Offer to the terminating network.

4. The S-CSCF receives the SDP Answer from the terminating network containing fingerprint, tls-id, and setup attributes chosen by IMS UE B in accordance with RFC 8841 [48].

5. The S-CSCF forwards the SDP Answer to the P-CSCF.

6. The P-CSCF forwards the SDP Answer to IMS UE A. After receiving this message, IMS UE A completes the media security setup by either initiating DTLS handshake (if setup attribute of the SDP Answer indicated that

UE A is DTLS client) or waiting for the peer to initiate DTLS handshake (if setup attribute of SDP Answer indicated that UE A is DTLS server), in accordance with RFC 8841 [48].

7. When the full session setup has been completed, and media can be sent, the protected IMS data channel media stream is sent between IMS UE A and IMS UE B. IMS UE A integrity protects / encrypts the media stream sent towards IMS UE B using the previously exchanged keys from DTLS handshake and checks integrity / decrypts the media stream arriving from IMS UE B using the previously exchanged keys from DTLS handshake.

7.3 UE terminating procedures

7.3.1 UE terminating procedures for e2ae

Figure 7.3.1-1 shows the terminating session set-up procedures for one or more media stream using e2ae security.

NOTE 1: The procedures shown in the figure apply to users located in their home service area. The same concepts apply to roaming users.

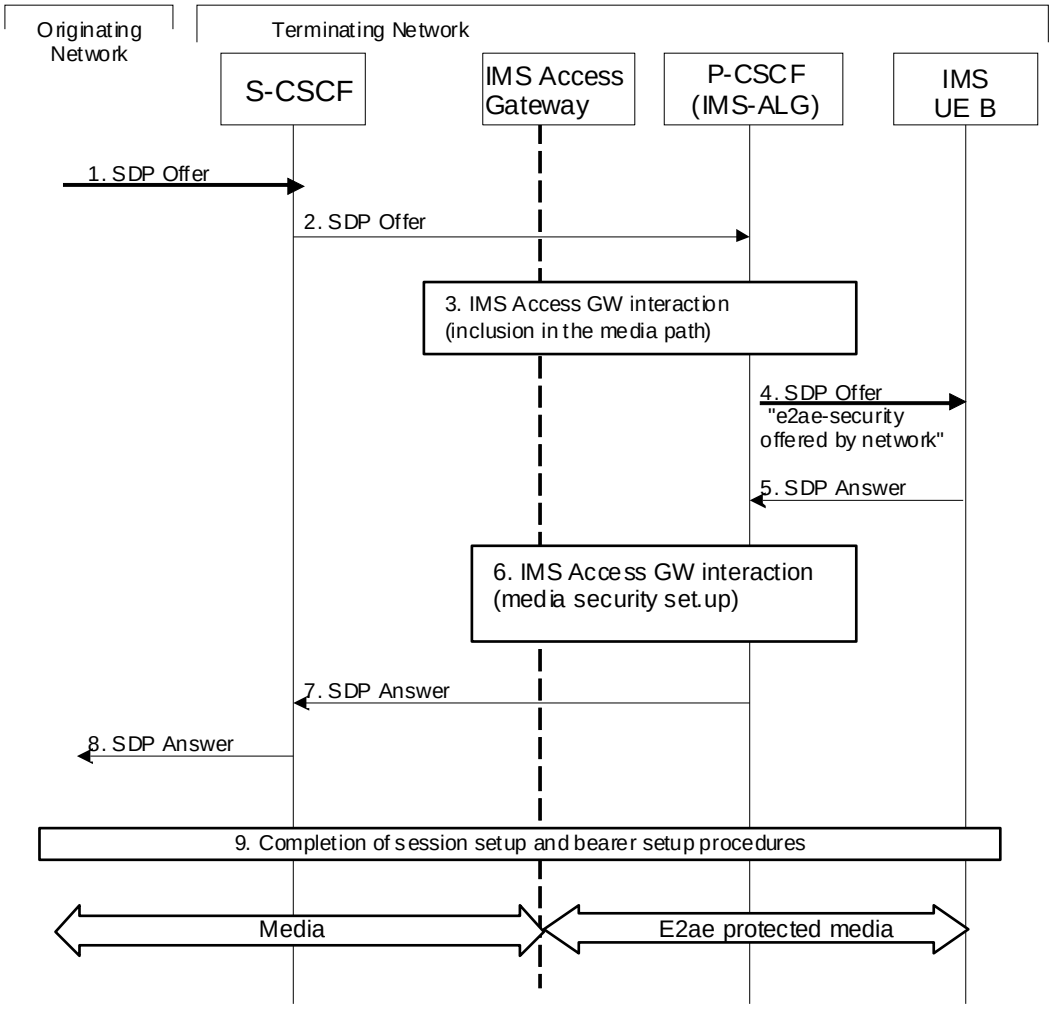


Figure 7.3.1.-1: Terminating call flow for e2ae case

The IMS UE performs an IMS terminating session set-up according to 3GPP TS 23.228 [3], with modifications as described in the following. If both IMS UE and network indicated support for e2ae-security for RTP based traffic during registration and the P-CSCF (IMS-ALG) receives an SDP Offer for an RTP media stream using transport "RTP/AVP" or "RTP/AVPF" (i.e. no SRTP) from the S-CSCF, then the P-CSCF (IMS-ALG) shall establish e2ae-

security for the RTP media stream as described in this clause. If both IMS UE and network indicated support for e2ae-security for MSRP during registration and the P-CSCF (IMS-ALG) receives an SDP Offer for an MSRP media stream using transport "TCP/MSRP" (i.e. no TLS) from the S-CSCF, then the P-CSCF (IMS-ALG) shall establish e2ae-security for the MSRP media stream as described in this clause.

NOTE 2: The P-CSCF (IMS-ALG) will not establish e2ae security for RTP based media if the SDP offer received from the S-CSCF indicates that e2e security is being offered, cf. clauses 7.3.2 and 7.3.3 for the establishment of e2e security on the terminating side.

The procedure in the above figure is now described step-by-step.

1. The S-CSCF in the terminating network receives an SDP Offer for an RTP media stream with transport "RTP/AVP" or "RTP/AVPF" or an MSRP stream with transport "TCP/MSRP" from the originating network.

2. The S-CSCF performs the required procedures according to TS 23.228 [3] and forwards the SDP Offer for the media stream to the P-CSCF (IMS-ALG).

3. The P-CSCF (IMS-ALG) checks the media streams in the SDP Offer.

   For each RTP media stream offered with transport "RTP/AVP" or "RTP/AVPF", if ,both the IMS UE and the P-CSCF (IMS-ALG) indicated support of e2ae-security during registration the P-CSCF (IMS-ALG) proceeds for this media stream as described in the present clause and allocates the required resources and includes the IMS Access GW in the media path. For each RTP media stream offered with transport "RTP/AVP" or "RTP/AVPF" where this is not the case the P-CSCF (IMS-ALG) continues as described for a call without IMS media plane security.

   For each RTP media stream offered with transport "RTP/SAVP" or "RTP/SAVPF", the P-CSCF (IMS-ALG) proceeds as described in clause 7.3.2 or 7.3.3.

   For each MSRP media stream offered with transport "TCP/MSRP",

   - if both the IMS UE and P-CSCF (IMS-ALG) indicated support for e2ae-security for MSRP during registration, the P-CSCF (IMS-ALG) proceeds for this media stream as described in this clause and allocates the required resources, includes the IMS Access GW in the media path for establishing the TLS/DTLS towards the IMS UE and retrieves from the IMS Access GW the fingerprint of the certificate the IMS Access GW is going to use for setting up security for this media stream

   - if not both the IMS UE and P-CSCF (IMS-ALG) indicated support for e2ae-security for MSRP during registration, the P-CSCF (IMS-ALG) should continue as described for media streams without IMS media plane security. If compatibility with RCS 5.1 [27] is desired, a P-CSCF may, based on local policy, proceed for this media stream as described in the preceding paragraph.

   For each MSRP media stream offered with transport "TCP/TLS/MSRP" the P-CSCF (IMS-ALG) should proceed as specified in clause 7.3.3 of the present specification or in TS 23.228 [3] or may, depending on its local policy, terminate TLS and proceed as specified in this clause.

NOTE 2a: According to the above, an operator can choose to set up e2ae security for terminating MSRP media streams according to the following steps for all MSRP media streams that would otherwise not be protected by TLS, even if the UE did not indicate support for e2ae security during registration. This can lead to session failures for pre-Rel-12 IMS UEs or non-IMS UEs that do not support MSRP over TLS with self-signed certificates and the exchange of certificate fingerprints, but on the other hand, it will ensure compatibility with RCS 5.1 [27], which recommends to always use e2ae security for MSRP on the terminating leg. Furthermore, an operator can choose to always terminate TLS when offered from the originating side, but this again can lead to session failures due to a mismatch of security parameters sent by the network and expected by the UE..

NOTE 3: The inclusion of the IMS Access GW in the media path is required for the purposes of e2ae security even if it was not required otherwise.

4. The P-CSCF (IMS-ALG) modifies the SDP Offer before sending it to the IMS UE B.

   For e2ae protection of RTP the P-CSCF (IMS-ALG) changes the transport from RTP to SRTP in the SDP Offer, includes one or more SDES crypto attributes, as well as an indication that e2ae security is offered by the

network. Each of these SDES crypto attributes contains at least one master key K21, and other security context parameters chosen by the P-CSCF (IMS-ALG) in accordance with RFC 4568 [13]. The optional key lifetime field shall be omitted.

For e2ae protection of an MSRP media stream the P-CSCF (IMS-ALG) sets the transport to "TCP/TLS/MSRP" in the SDP Offer, removes any fingerprint attributes for this media stream and include the fingerprint of the IMS Access GW´s certificate in accordance to RFC 4975 [21] as well as an indication that e2ae security is offered by the network.

The P-CSCF (IMS-ALG) then sends the updated SDP Offer to IMS UE B.

5. IMS UE B replies with an SDP Answer for a secured media stream.

   For e2ae protection of SRTP, the IMS UE B includes in the SDP Answer one of the received SDES crypto attributes containing at least one master key K22, and other security context parameters chosen by IMS UE B in accordance with RFC 4568 [13]. The optional key lifetime field shall be omitted.

   For e2ae protection of MSRP, the IMS UE B includes in the SDP Answer the fingerprint of the UE´s certificate in accordance to RFC 4975 [21].

6. The P-CSCF (IMS-ALG) communicates the cryptographic information contained in the SDP Answer to the IMS Access GW.

   For e2ae protection of RTP, this includes the parameters contained in the SDES crypto attribute selected by IMS UE B in step 5 as well as those in the SDES crypto attribute sent by IMS UE B in step 5 to the P-CSCF (IMS-ALG). The P-CSCF (IMS-ALG) instructs the IMS Access GW to check integrity / decrypt the media stream arriving from IMS UE B using K22 (and possibly further master keys), to integrity protect / encrypt the media stream arriving from the originating network using K21 (and possibly further master keys), and to set the key lifetime to the default values as defined in RFC 3711 [9].

   For e2ae protection of MSRP, the cryptographic information communicated to the IMS Access GW consists on the fingerprint of the IMS UE B certificate in accordance to RFC 4975 [21 The P-CSCF (IMS-ALG) instructs the IMS Access GW to verify during the subsequent TLS handshake with the IMS UE (see step 9) that the fingerprint of the certificate passed by the IMS UE during this TLS handshake matches the fingerprint passed by the P-CSCF (IMS-ALG) to the IMS Access GW.].

7. The P-CSCF (IMS-ALG) modifies the SDP Answer before sending it to the S-CSCF.

   For e2ae protection of SRTP, the P-CSCF (IMS-ALG) changes the transport from SRTP to RTP in the SDP Answer and removes the SDES crypto attribute.

   For e2ae protection of MSRP, the P-CSCF (IMS-ALG) changes the transport from "TCP/TLS/MSRP" to “TCP/MSRP” in the SDP Answe r (cf., however, NOTE 4) . Further, it removes the fingerprint of the IMS UE B certificate.

   The P-CSCF (IMS-ALG) then sends the SDP Answer to the S-CSCF.

8. The S-CSCF forwards the SDP Answer towards the originating network.

9. In case of RTP, when the full session setup has been completed, and media can be sent, the protected media streams are sent between the IMS UE B and IMS Access GW. IMS UE B integrity protects / encrypts and integrity check / decrypts the media streams sent to and received from the network. The IMS Access GW integrity checks / decrypts the media stream arriving from IMS UE B before passing it on towards the originating network. The IMS Access GW integrity protects / encrypts the media stream arriving from the originating network before passing it on to IMS UE B.

A P-CSCF (IMS-ALG) supporting e2ae-security shall remove any indication "e2ae-security offered by network" if inserted in a SIP message by another party.

In case of MSRP, when the full session setup has been completed, the TCP and TLS connection shall be established between the IMS UE and the IMS Access GW. When subsequently media are sent from or to the IMS UE, the IMS Access GW performs the required TLS specific cryptographic operations on the media.

NOTE 4: A network may have the policy to use TLS for MSRP also inside the core network. So TLS from the direction of the core network may be terminated at the IMS Access GW. This may require enhancements to the procedure described above but is outside of the scope of this specification.

NOTE 5: It is left to stage 3 specifications whether the IMS UE takes the role of TLS client or TLS server. These alternatives are equivalent from a security point of view.

7.3.2 IMS UE terminating procedures for e2e using SDES

Figure 7.3.2-1 shows the terminating call set-up procedures for one RTP media stream using e2e security.

NOTE 1: The procedures shown in the figure apply to users located in their home service area. The same concepts apply to roaming users.

NOTE 2: E2e protected RTP sessions and/or media streams are set-up without IMS-ALG support, which means that such sessions can be set-up in networks not providing the IMS-ALG functionality in the P-CSCF.

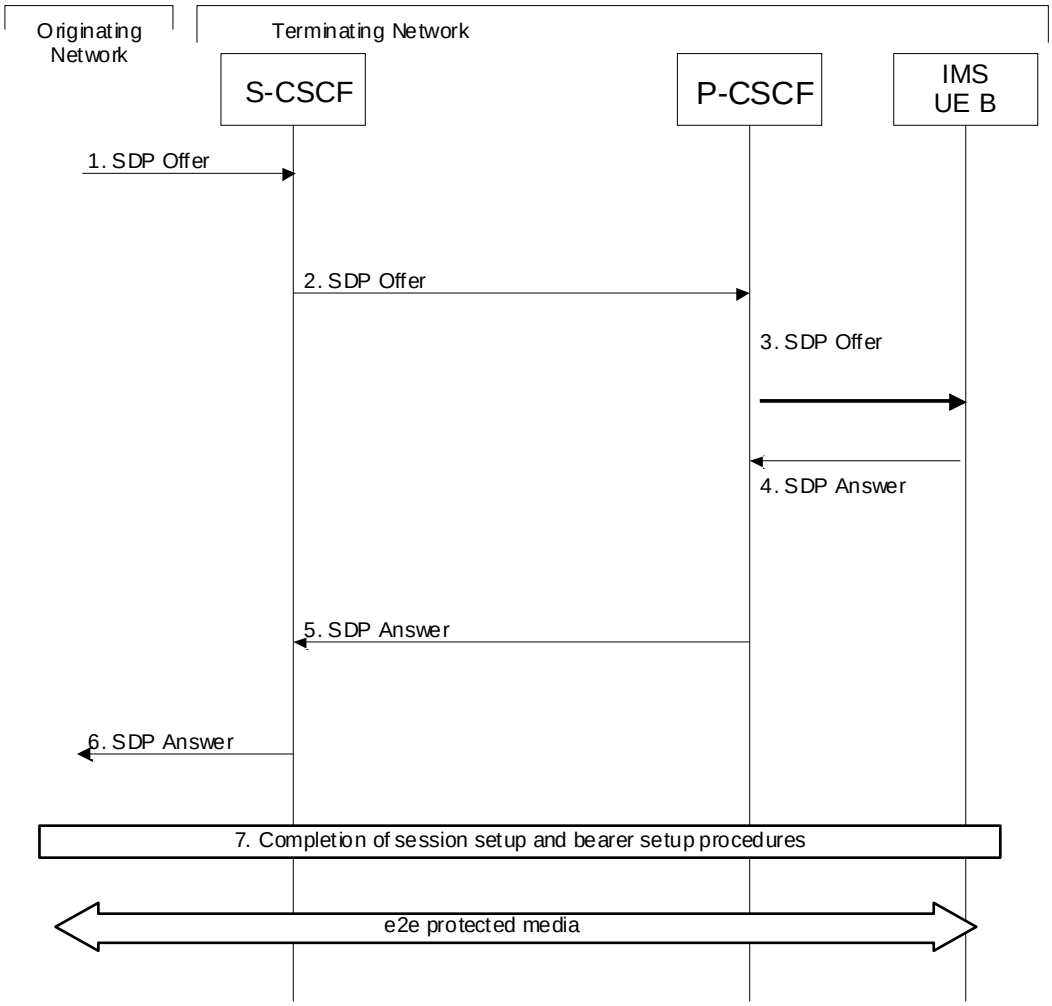


Figure 7.3.2-1: Terminating call flow for e2e case using SDES

The IMS UE performs an IMS terminating session set-up according to 3GPP TS 23.228 [3], with modifications as described in the following.

NOTE 3: The procedure described here is the same as for legacy UEs not fully conforming to this specification, which may also use SDES to establish e2e security.

The procedure in the above figure is now described step-by-step.

1. The S-CSCF in the terminating network receives an SDP Offer for an SRTP media stream including one or more SDES crypto attributes from the originating network. Each of these SDES crypto attributes contains at least one master key K1, and other security context parameters chosen by IMS UE A in accordance with RFC 4568 [13].

2. The S-CSCF performs the required procedures according to TS 23.228 [3] and forwards the SDP Offer for the SRTP media stream to the P-CSCF.

3. The P-CSCF forwards the SDP Offer for the SRTP media stream to IMS UE B.

4. IMS UE B selects one of the received SDES crypto attributes, and then replies with an SDP Answer for an SRTP media stream, including one SDES crypto attribute with at least one master key K2, and other security context parameters chosen by IMS UE B in accordance with RFC 4568 [13].

5. The P-CSCF forwards the SDP Answer to the S-CSCF.

6. The S-CSCF forwards the SDP Answer towards the originating network.

7. When the full session setup has been completed, and media can be sent, the protected RTP media stream is sent between IMS UE A and IMS UE B. IMS UE B integrity protects / encrypts the RTP media stream sent towards IMS UE A using key K2 (and possibly further master keys) and checks integrity / decrypts the RTP media stream arriving from IMS UE A using key K1 (and possibly further master keys) from the crypto attribute selected by IMS UE B.

7.3.3 IMS UE terminating procedures for e2e using KMS

Figure 7.3.3-1 shows the terminating call set-up procedures for one RTP or one MSRP session using KMS based security.

NOTE 1: The procedures shown in the figure apply to users located in their home service area. The same concepts apply to roaming users.

NOTE 2: E2e protected RTP or MSRP sessions are set-up without IMS-ALG support, which means that such sessions can be set-up in networks not providing the IMS-ALG functionality in the P-CSCF.

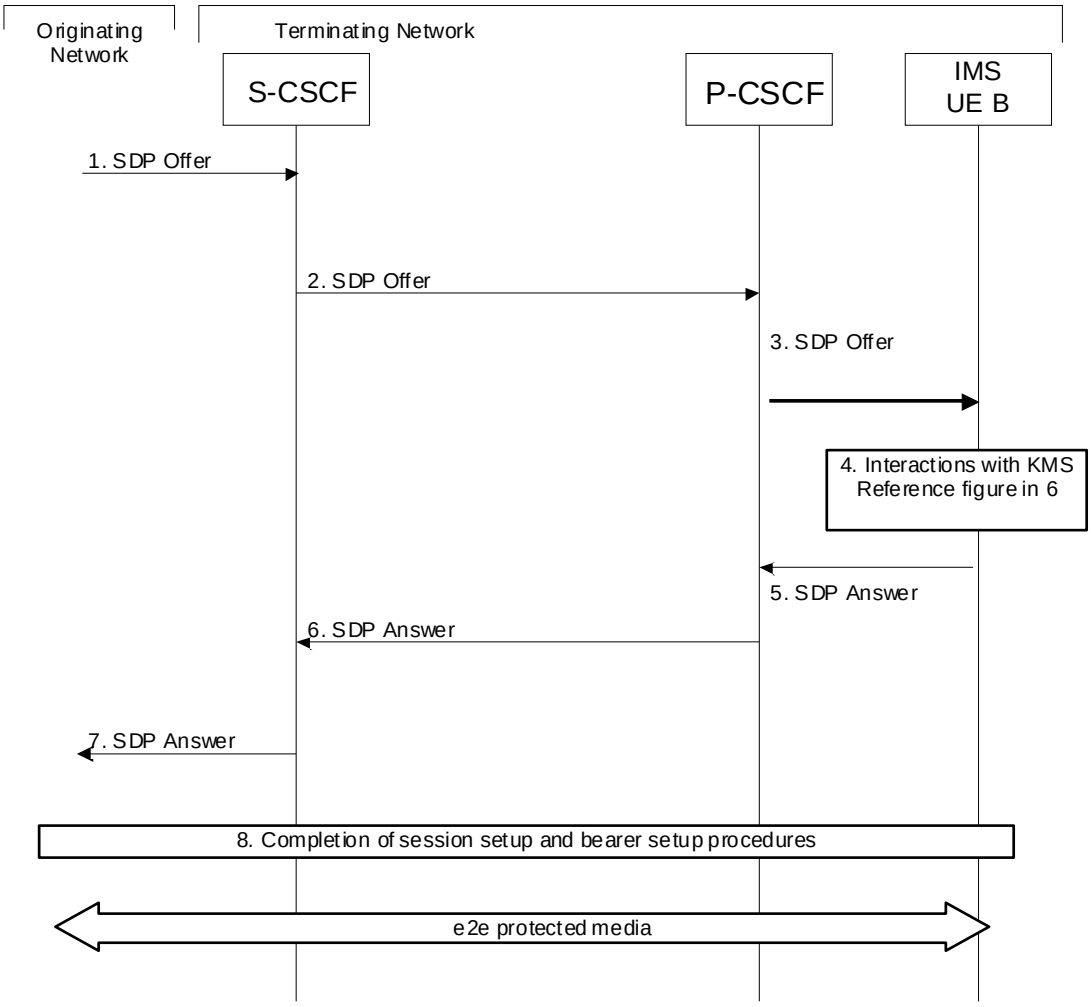


Figure 7.3.3-1: Terminating call flow for e2e case using KMS

An IMS terminating session set-up according to 3GPP TS 23.228 [3] is performed, with modifications as described in the following. KMS interactions are described in clause 6.2.3.1. Details of the KMS based key management are given in Annex B.

The procedure in the above figure is now described step-by-step.

1. The S-CSCF in the terminating network receives an SDP offer for an RTP or MSRP session containing a MIKEY-TICKET offer.
2. The S-CSCF performs the required procedures according to TS 23.228 [3] and forwards the SDP offer to the P-CSCF.
3. The P-CSCF forwards the SDP offer to IMS UE B.
4. IMS UE B checks if it is authorized to resolve the ticket and if that is the case IMS UE B interacts with the KMS to resolve the ticket and receive keys.
5. IMS UE B replies with an SDP answer for an RTP or MSRP session, including a MIKEY-TICKET response.
6. The P-CSCF forwards the SDP answer to the S-CSCF.
7. The S-CSCF forwards the SDP answer towards the originating network.

IMS UE-B derives the media session keys and initiates the media plane security. For an RTP session this means sending and receiving SRT(C)P streams and for an MSRP session this means setting up a TLS-PSK tunnel to protect the MSRP messages.

7.3.4 UE terminating procedures for e2DCe

Figure 7.3.4-1 shows the terminating session set-up procedures for one or more media streams using e2DCe security.

NOTE 1: The procedures shown in the figure apply to users located in their home service area. The same concepts apply to roaming users.

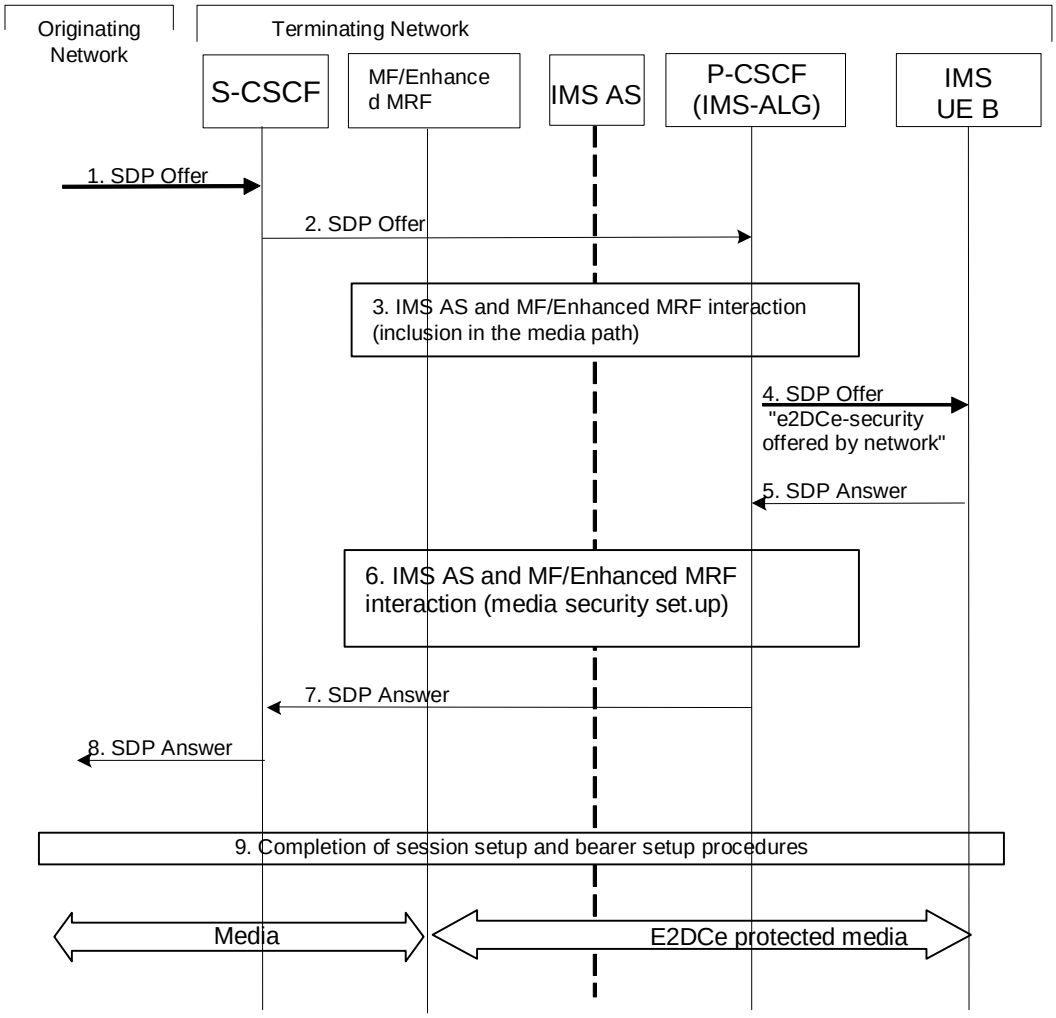


Figure 7.3.4-1: Terminating call flow for e2DCe using MF/MRF case

The IMS UE performs an IMS terminating session set-up according to 3GPP TS 23.228 [3], with modifications as described in the following. If both IMS UE and network indicated support for e2DCe-security for IMS data channel media streams during registration and the P-CSCF receives an SDP Offer for an IMS data channel media stream using "UDP/DTLS/SCTP" transport from the S-CSCF, then the P-CSCF (IMS-ALG) shall establish e2DCe-security for the IMS data channel media stream as described in this clause.

NOTE 2: The P-CSCF (IMS-ALG) will not establish e2DCe security for IMS data channel media if the SDP offer received from the S-CSCF indicates that e2e security is being offered, cf. clauses 7.3.2, 7.3.3, and 7.3.5 for the establishment of e2e security on the terminating side.

The procedure in the above figure is now described step-by-step.

1. The S-CSCF in the terminating network receives an SDP Offer for an IMS data channel stream with transport "UDP/DTLS/SCTP" from the originating network.

2. The S-CSCF performs the required procedures according to TS 23.228 [3] and forwards the SDP Offer for the media stream to the IMS AS.

3. The IMS-AS checks the media streams in the SDP Offer.

For each IMS data channel media stream offered with transport "UDP/DTLS/SCTP",

- if both the IMS UE and P-CSCF (IMS-ALG) indicated support for e2DCe-security for IMS data channel during registration, the IMS-AS and S-CSCF proceeds for the respective media stream as described in this clause and allocates the required resources, includes the Media Function/MRF in the media path for establishing the DTLS towards the IMS UE and retrieves from the Media Function/MRF the fingerprint, tls-id, and setup role of the certificate the Media Function/MRF is going to use for setting up security for this media stream

- if not both the IMS UE and P-CSCF (IMS-ALG) indicated support for e2DCe-security for IMS data channel during registration, the IMS-AS should continue using e2e security, as described in clause 7.3.5 of the present specification.

NOTE 3: The inclusion of the Media Function/MRF in the media path is required for the purposes of e2DCe security even if it was not required otherwise.

The IMS-AS modifies the SDP Offer before sending the SDP Offer back to S-CSCF.

For e2DCe protection of an IMS data channel media stream, the IMS-AS keeps the transport as "UDP/DTLS/SCTP" in the SDP Offer, conveys the fingerprint, tls-id, and setup attribute information of the MF/MRF in accordance with RFC 8841 [48] as well as an indication that e2DCe security is offered by the network to UE.

The IMS-AS then sends the updated SDP Offer to S-CSCF.

4. The S-CSCF performs the required procedures according to TS 23.228 [3] and forwards the SDP Offer for the media stream to the P-CSCF(IMS-ALG).

5. The P-CSCF (IMS-ALG) forwards the SDP Offer to the IMS UE B.

6. IMS UE B replies with an SDP Answer for a secured media stream.

For e2DCe protection of IMS Data Channel, the IMS UE B includes in the SDP Answer the fingerprint of the UE´s certificate, tls-id, and setup attributes in accordance with RFC 8841 [48].

7. The P-CSCF sends the SDP Answer to the S-CSCF.

8. The S-CSCF performs the required procedures according to TS 23.228 [3] and sends the SDP Answer to the IMS AS.

9. The IMS-AS communicates the cryptographic information contained in the SDP Answer to the Media Function/MRF, performs the required procedures according to TS 23.228 [3] and sends the SDP Answer to the S-CSCF.

For e2DCe protection of IMS Data Channel, the cryptographic information communicated to the Media Function/MRF consists of the fingerprint of the IMS UE B's certificate, tls-id, and setup attributes in accordance with RFC 8841 [48]. The S-CSCF instructs the Media Function/MRF to verify during the subsequent DTLS handshake with the IMS UE (see step 9) that the fingerprint of the certificate passed by the IMS UE during this DTLS handshake matches the fingerprint passed by the S-CSCF to the Media Function/MRF.

10. The S-CSCF forwards the SDP Answer towards the originating network.

11. In case of IMS Data Channel, when the full session setup has been completed, the DTLS connection shall be established between the IMS UE and the Data Channel Media Function/MRF. When subsequently media are sent from or to the IMS UE, the Data Channel Media Function/MRF performs the required DTLS specific cryptographic operations on the media.

NOTE 4: It is left to stage 3 specifications whether the IMS UE takes the role of DTLS client or DTLS server. These alternatives are equivalent from a security point of view.

7.3.5 IMS UE terminating procedures for e2e using TLS/DTLS certificate / fingerprint

The IMS UE terminating procedures for e2e using TLS/DTLS certificate fingerprints are expected to be similar to the corresponding originating procedures.

7.4 Session update procedures

When session update is performed, and there is a need for updating the media security context (e.g., re-keying), new security context shall be included. If the media security context does not need to be updated (e.g., the session update is due to media on hold), the previously sent security context shall be included in accordance to the offer answer procedures (see also TS 24.229 [18]).This means in particular that when an unchanged security context is received there shall be no re-initialization of the media plane protection.

Media security context update is not used with e2ae security.

7.5 Handling of emergency calls

E2ae security procedures according to clause 7.2.1 shall be applied to an emergency call set-up if and only if the registration procedure according to clause 7.1 has shown that both, IMS UE and network, support e2ae security. E2e security shall not be applied to emergency calls.

Annex A (Normative): HTTP based key management messages

A.1 General aspects

This annex specifies the HTTP based key management procedures between the KMS and the UE. It defines the following HTTP based procedures:

- KMS Ticket Request
- KMS Ticket Resolve

The KMS Ticket Resolve procedure shall also be used between KMSs when one KMS gets a request to resolve a ticket that can only be resolved by another KMS.

The Ua security protocol identifier used for GBA NAF-Key generation shall be as defined in TS 33.220 [6].

A.2 Key management procedures

The IMS UE shall send the requests to the KMS in the message-body of a HTTP POST request. The Request-URI shall indicate the type of the message. Upon successful request, KMS shall return indication of success.

The IMS UE populates the HTTP POST request as follows:

- the HTTP version shall be 1.1 which is specified in RFC 2616 [8];
- the Request-URI shall contain an URI parameter "requesttype" that shall be set to "ticketrequest" or "ticketresolve", i.e. Request-URI takes the form of "/keymanagement?requesttype=ticketrequest";
- the header field Host shall contain the full KMS URI (e.g. kms.operator.example:1234);
- the header field Content-Type shall be the MIME type of the payload, i.e. "application/mikey". The MIME type is specified in RFC 3830 [11];
- the message-body shall contain a base64 encoded MIKEY-TICKET message. Either a REQUEST_INIT or a RESOLVE_INIT message corresponding to the requesttype parameter in the Request-URI. The MIKEY-TICKET messages are specified in [14].
- the IMS UE may add additional URI parameters to the Request-URI;
- the IMS UE may add additional header fields;

The IMS UE sends the HTTP POST to the KMS. The KMS checks that the HTTP POST is valid, and extracts the request for further processing.

```
POST /keymanagement?requesttype=ticketrequest HTTP/1.1
Host: kms.operator.example:1234
Content-Type: application/mikey
Content-Length: 127
User-Agent: KMSAgent; Release-9 3gpp-gba
From: alice@operator.example
Date: Fri, 31 Dec 1999 23:59:59 GMT

Mgj4hyruihyu8568dfg543...
```

After processing, the KMS shall return the HTTP 200 OK to the IMS UE.

The KMS shall populate HTTP response as follows:

- the status code shall be 200 OK;

- the header field Content-Type shall be the MIME type of the payload, i.e. "application/mikey". The MIME type is specified in RFC 3830 [11];
- the message-body shall contain a base64 encoded MIKEY-TICKET message. Either a REQUEST_RESP or a RESOLVE_RESP message corresponding to the MIKEY-TICKET message in the HTTP POST, or a Error message specifying the error that occurred. The MIKEY-TICKET response messages are specified in [14] and the Error message is specified in RFC 3830 [11].
- the KMS may add additional header fields;

The KMS shall send the HTTP response to the IMS UE. The IMS UE shall check that the HTTP response is valid.

```
HTTP/1.1 200 OK
Date: Fri, 31 Dec 1999 23:59:59 GMT
Content-Type: application/mikey
Content-Length: 235

Mgj4hyruihyu8568dfg543...
```

A.3 Error situations

The HTTP procedures may not be successful for multiple reasons. The error cases are indicated by using 4xx and 5xx HTTP Status Codes as defined in RFC 2616 [8]. The 4xx status code indicates that the IMS UE seems to have erred, and the 5xx status code indicates that the KMS is aware that it has erred.

Annex B (Normative): KMS based key management

B.1 UE originating procedures

B.1.1 Preconditions

The following preconditions are assumed:

- The IMS UE is configured with the address to the KMS, which it shall use for ticket requests.
  The KMS address is in the form of a Fully Qualified Domain Name as defined in IETF RFC 1035 [7]
- The IMS UE is configured with GBA protocol identifier to use for MIKEY-TICKET [14] message exchange.
- The IMS UE has performed a GBA bootstrap and holds a valid B-TID and Ks.
- The IMS UE has derived the NAF-key for the KMS, which it shall use for ticket request

B.1.2 Procedures

The originating call set-up procedure is described in clause 7.2.3. Interactions with the KMS are described in clause 6.2.3.1.

The detailed originating procedures are described in the following steps

1. The initiator evaluates the local policy held in the IMS UE for calling the intended user. If the local policy determines that a fresh ticket generated by the KMS should be used then the processing continues at step 3. If the local policy determines that the IMS UE shall generate a fresh ticket then the IMS UE generates the ticket and the processing continues at step 10.

   When an IMS UE generates a ticket the NAF-Key shall be used as ticket protection key (TPK), see Annex D.4.

2. The initiator searches its local store of reusable tickets. If a reusable ticket is found having the intended recipient as an allowed recipient, and which also fulfils all other required ticket properties, then this ticket shall be reused. Next processing step is step 10.

3. The initiator prepares a REQUEST_INIT_PSK message as described in MIKEY-TICKET [14]. The payloads are generated according to the local policy for ticket requests. The IDRpsk payload is populated with the B-TID and the NAF-key is used as the pre-shared key for protection of the message.

4. The message is sent to the KMS over HTTP, as defined in Annex A.

5. The KMS receives the message. The KMS processes the message as defined in MIKEY-TICKET [14]. The KMS retrieves the B-TID and request the NAF-Key and related USS information from the BSF containing a list of all IMPUs associated with the requestor. Based on the NAF-Key, the KMS verifies the authenticity of the message. If the verification fails, the KMS returns an appropriate error message.

6. The KMS verifies that one of the IMPUs in the received USS matches, after transformation into a KMS UID format, the KMS UID is included in the ticket request as the identity of the initiator. If there is no match the processing is terminated and an appropriate error message is returned.

7. The KMS checks the requested ticket policy against its policy for the requesting user and requested allowed recipients. The KMS modifies the requested policy as needed or if that is not possible or allowed, it terminates processing and sends and appropriate error message.

8. The KMS generates the REQUEST_RESP message according to MIKEY-TICKET [14] and sends it as a response over HTTP, see Annex A, to the initiator.

9. The initiator receives the REQUEST_RESP message and checks the response according to MIKEY-TICKET [14]. The initiator also checks if the policy has been changed and if so, verifies that it still fulfils the requirements for the call. If the ticket is a reusable ticket then it is stored in the local store of reusable tickets together with the corresponding keys retrieved from the REQUEST_RESP message.

10. The initiator generates the TRANSFER_INIT message according to MIKEY-TICKET [14]. The identities of the initiator and the responder in the message shall be the KMS UIDs derived from the URI's in the To: and From: fields in the INVITE.

    In the RTP case, the number of Crypto Sessions included in the TRANSFER_INIT message should match the number of RTP streams (both incoming and outgoing) as described in RFC 4567 [12]. The protocol type in the Crypto Session shall be set to SRTP.

    In the MSRP case, a single Crypto Session is included in the TRANSFER_INIT message as described in Annex X.3. The protocol type in the Crypto Session shall be set to TLS.

    The initiator prepares the media security offer in the SDP part of the INVITE according to local policies and this specification. It inserts the TRANSFER_INIT message according to RFC 4567 [12]

11. The initiator receives the TRANSFER-RESP message in the SDP part of a 200 OK or an 18x provisional response. It verifies the message according to MIKEY-TICKET [14] and then verifies that the authenticated identity of the recipient corresponds to the policy for the call. Depending on local policy different types of user warnings may be generated if the returned identity differs from what is expected.

12. The initiator derives the media session keys and initiates the media plane security. For an RTP session this means sending and receiving SRT(C)P streams and for an MSRP session this means setting up a TLS-PSK tunnel to protect the MSRP messages.

B.2 UE terminating procedures

B.2.1 General

The terminating call set-up procedure is described in clause 7.3.3. Interactions with the KMS are described in clause 6.2.3.1.

B.2.2 Procedures for the case with one KMS domain

B.2.2.1 Preconditions

The following preconditions are assumed:

- The IMS UE is configured with the address to the KMS it shall use for ticket resolve. The KMS address is in the form of a Fully Qualified Domain Name as defined in IETF RFC 1035 [7].
- The IMS UE is configured with GBA protocol identifier to use for MIKEY-TICKET [14] message exchange.
- The IMS UE has performed a GBA bootstrap and holds a valid B-TID and Ks.
- The IMS UE has derived the NAF-key for the KMS it shall use for ticket resolve.

B.2.2.2 Procedures

The detailed terminating procedures for the case when both initiator and responder have trust relations with a common KMS are described in the following steps

1. The responder receives the TRANSFER_INIT message and makes an initial verification of the message by verifying that payloads are in accordance with the responders receive policy. In particular, the responder checks that the identity of the issuer of the ticket corresponds to the sender of the TRANSFER_INIT. As the keys used to protect the message are based on the content of the ticket no check of the authenticity of the message can be

made.

If the ticket is marked as reusable, and the Ticket Resolve exchange is not indicated as mandatory, the responder searches his local store of reusable tickets. If a match is found the next processing step is step 10.

2. The responder prepares a RESOLVE_INIT_PSK message as described in MIKEY-TICKET [14]. The payloads are generated according to the local policy for ticket resolve requests. The IDRpsk payload is populated with the B-TID and the NAF-key is used as the pre-shared key for protection of the message.

3. The message is sent to the KMS over HTTP, as defined in Annex A.

4. The KMS receives the message. The KMS processes the message as defined in MIKEY-TICKET [14]. The KMS retrieves the B-TID and request the NAF-Key and related USS information from the BSF. The USS contains a list of all IMPUs associated with the requestor. Based on the NAF-Key, the KMS verifies the authenticity of the message. If the verification fails, the KMS returns an appropriate error message.

5. The KMS verifies that one of the IMPUs in the received USS matches, after transformation into a KMS UID format, a legitimate recipient according to the ticket (policy). If there is no match the processing is terminated and an appropriate error message is returned.

6. The KMS checks the received ticket policy against its policy for the requesting user and initiator and if there is a usage conflict the processing is terminated and an appropriate error message is returned.

7. The KMS generates the RESOLVE_RESP message according to MIKEY-TICKET [14] and sends it as a response over HTTP, as defined in Annex A, to the responder.

8. The responder receives the RESOLVE_RESP message and checks it according to MIKEY-TICKET [14]. If the ticket was a reusable ticket then it is stored in the local store of reusable tickets together with the corresponding keys retrieved from the RESOLVE_RESP message.

9. The responder generates the TRANSFER_RESP message according to MIKEY-TICKET [14]. The responder prepares the media security response in the SDP part of the 200 OK or 18x provisional answer according to local policies and this specification. It inserts the TRANSFER_RESP message according to RFC 4567 [12]

10. The responder derives the media session keys and initiates the media plane security. For an RTP session this means sending and receiving SRT(C)P streams and for an MSRP session this means setting up a TLS-PSK tunnel to protect the MSRP messages.

B.2.3 Procedures for the case with two KMS domains

B.2.3.1 Preconditions

The following preconditions are assumed:

- The IMS UE is configured with the address to the KMS, KMS_R, it shall use for ticket resolve. The KMS address is in the form of a Fully Qualified Domain Name as defined in IETF RFC 1035 [7].
- The IMS UE is configured with GBA protocol identifier to use for MIKEY-TICKET [14] message exchange.
- The IMS UE has performed a GBA bootstrap and holds a valid B-TID and Ks.
- The IMS UE has derived the NAF-key for the KMS it shall use for ticket resolve.
- The ticket is issued by another KMS, KMS_I, with which KMS_R has a trust relation. Message origin authentication, and integrity and confidentiality protection between KMS_R and KMS_I is based on NDS/IP [5], see 4.2.4. Confidentiality protection is mandated (over Za) because keys are transported in the clear over Zk. Confidentiality protection may be achieved by cryptographic or other means

B.2.3.2 Procedures

The detailed terminating procedures for the case when the initiator has a trust relation with different KMSs are described in the following steps

1-5. The steps 1 to 5 are identical to steps 1–5 in clause B.2.2.2.2 with KMS replaced by KMS_R

6. KMS_R prepares a new RESOLVE_INIT_PSK message as described in MIKEY-TICKET [14]. If the IDRr payload in the received RESOLV_INIT_PSK message matched a legitimate recipient (step 5) it is reused in the new RESPOLVE_INIT_PSK, otherwise KMS_R inserts a matching KMS UID as IDRr. The TICKET payload is reused. The message is not integrity protected.

7 The message is sent to KMS_I over HTTP, as defined in ANNEX A.

NOTE: The address of KMS which can resolve the ticket is included in the Ticket.Policy Payload, subpayload IDRkms, cf. MIKEY-TICKET [14].

8. KMS_I verifies the message and that it comes from a trusted source (based on the NDS/IP protection).

9. KMS_I checks the received ticket policy against its policy for the requesting user and initiator and if there is a usage conflict the processing is terminated and an appropriate error message is returned.

10. KMS_I generates a RESOLVE_RESP message and sends it as a response over HTTP to KMS_R. The RESOLVE_RESP message itself is not protected, i.e. there is no integrity protection and the KEMAC is not enciphered.

11. KMS_R receives the RESOLVE_RESP message and checks its integrity and source (based on the NDS/IP protection).

12. KMS_R prepares a new protected RESOLVE_RESP reusing the payloads from KMS_I. The KEMAC is enciphered and the message is integrity protected. KMS_R sends the message to the responder over HTTP according to Annex A

13-14. The steps 13 and 14 are identical to steps 9 and 10 in clause B.2.2.2.2.

Annex C (Normative): SRTP profiling for IMS media plane security

An IMS UE and IMS core network entity capable of supporting IMS media plane security (SDES and/or KMS based)

- Shall support all mandatory features defined in RFC 3711 [9] except that it does not have to support key derivation rates different from zero (KDR <> 0).

- May support RFC 4771, "Integrity Transform Carrying Roll-Over Counter for the Secure Real-time Transport Protocol (SRTP)" [15] for SDES based media plane security. RFC 4771 shall be supported and used for KMS based media plane security RFC 4771 defines functionality that is essential to simplify late entry in group communications and broadcasting sessions.

Annex D (Normative): MIKEY-TICKET profile for IMS media plane security

D.1 Scope

The profiling given in this Annex is with respect to MIKEY-TICKET [14]. The profiling is for the default implementation of KMS based IMS media plane security using GBA for user authentication and establishment of a shared key between KMS and IMS UE.

The profiling is based on what is needed to support SRTP as defined in RFC 3711 [9] and enhancements in terms of new SRTP transforms using 256 bit keys.

D.2 General

A KMS based IMS media plane security default implementation:

- Shall support MIKEY-TICKET Mode 1 and Mode 3 (cf. clause 4.1.1 in [14]).
- Does not have to support REQUEST_INIT_PK and RESOLVE_INIT_PK, i.e. it does not have to support public key based exchanges.
- Shall use the recommended payload order for all messages in the exchanges.
- Shall not add any extra payloads.

D.2A Keys, RANDs and algorithms

A KMS based IMS media plane security default implementation:

- Shall support use of keys of length 128 and 256 bit.
- Shall support use of RANDs of length 128 and 256 bit.
- Shall support the PRF-HMAC-SHA-256 in all HDR and TP payloads.
- May support PRFs MIKEY-1 in all HDR and TP payloads.
- Shall for KEMAC protection support AES-CM-128 and AES-CM-256 encryption algorithms and the NULL authentication algorithm.
- Shall support HMAC-SHA-256-256 as authentication algorithm in V payloads.
- May support HMAC-SHA-1-160 as authentication algorithm in V payloads.

D.3 Exchanges

D.3.1 Ticket Request

A KMS based IMS media plane security default implementation:

- Shall support timestamp of type NTP-UTC-32 and COUNTER.
- Shall populate payloads in REQUEST_INIT_PSK as defined here:

- IDRi: shall contain the Initiator’s KMS user identity.
- IDRkms: optional, URI for target KMS.
- TP: shall specify (IDRr), i.e. the intended recipients of the requested ticket. IDRapp shall be set to"IMS-MEDIASEC". In order to be able to handle call diversion (CDIV) scenarios, it is recommended to use the wildcarded identity ?@?.
- IDRpsk: B-TID.

- Shall populate payloads in REQUEST_RESP_PSK as defined here:
  - IDRkms: optional, URI for responding KMS.

D.3.2 Ticket Transfer

A KMS based IMS media plane security default implementation:

- Shall support timestamp of type NTP-UTC-32.
- Shall use CSB ID map type of type GENERIC-ID.
- Shall populate payloads in TRANSFER_INIT as defined here:
  - IDRi: shall be present. Contains initiator's KMS UID.
  - IDRr: shall be present. Contains KMS UID or KMS group identity.
- Shall populate payloads in TRANSFER_RESP as defined here:
  - RANDRr: shall be present.
  - RANDRkms: shall be present (used in key forking).
  - IDRr: shall be present (used in key forking).

D.3.3 Ticket Resolve

A KMS based IMS media plane security default implementation:

- Shall support timestamp of type NTP-UTC-32 and COUNTER.
- Shall populate payloads in RESOLVE_INIT_PSK as defined here:
  - IDRr: shall contain the Responder’s KMS UID.
  - IDRkms: optional, URI.
  - IDRpsk: shall contain B-TID.
- Shall populate payloads in RESOLVE_RESP_PSK as defined here:
  - IDRkms: optional, URI.
  - RANDRkms: shall be present (used in key forking).

D.4 Profiling of tickets

The default ticket for KMS based IMS media plane security

- Shall support use of keys of length 128 and 256 bit.
- Shall support use of RANDs of length 128 and 256 bit.

- Shall for KEMAC protection support AES-CM-128 and AES-CM-256 as encryption algorithm and the NULL Authentication algorithm.
- Shall support HMAC-SHA-256-256 as authentication algorithm in V payloads.
- May support HMAC-SHA-1-160 as authentication algorithm in V payloads.
- Shall support timestamps of type NTP-UTC-32.

The TP payload (section 6.10 in [14]) in the default ticket for KMS based IMS media plane security shall be populated as defined here:

- Has ticket type value 2 (defined in MIKEY-TICKET).
- Has subtype value 0 (zero) and version value 0 (zero).
- E flag shall have value 1 due to forking.
- F flag shall have value 1 due to forking.
- G flag shall have value 1.
- H flag shall have value 1.
- I flag shall have value 1 prescribing forking.
- L flag shall have value 0.
- M flag shall have value 0.
- N flag shall have value 1 prescribing that no extensions are used.
- O flag shall have value 1 prescribing that no extensions are used.
- All sub-payloads specified shall be present.

The ticket data of the Ticket payload (Appendix A in [14]) in the default ticket for KMS based IMS media plane security shall be populated as defined here:

- THDR: the first 48bits of the THDR Data shall contain a globally unique identifier of the issuing KMS.
- IDRpsk: shall contain B-TID if the ticket is generated by the initiator. If the KMS generates the ticket it is implementation specific.

Annex E (normative): Profiling of SDES

The present Annex contains a complete list of parameters that may be contained in an SDES crypto attribute, according to RFC 4568.

The following short-hand notation is used:

- "mandatory / optional to support / use" means: "This parameter shall / may be supported / used in implementations conforming to 3GPP specifications."

The default use is that the sender omits the parameters that are optional to use.

CRYPTOGRAPHIC ALGORITHMS

cryptosuite: mandatory to support and use

In addition to mandating the support and use of the parameter "cryptosuite" in an SDES crypto attribute, the cryptosuite "AES_CM_128_HMAC_SHA1_80", as defined in RFC 4568, is mandatory to support.

"KEY PARAMETERS" (ONE OR MORE TIMES):

key: mandatory to support and use

salt: mandatory to support and use

key lifetime: optional to support and use for e2e security, shall not be used for e2ae security (cf. clauses 7.2.1 and 7.3.1 of this specification).

Master Key Index (MKI): optional to support, mandatory to use if more than one set of key parameters is contained in the crypto attribute, otherwise optional to use. If only one master key is used, an MKI is not recommended to be used.

NOTE: It is not guaranteed that implementations support more than one master key per crypto attribute. If only one master key is used, an MKI has no function as it adds to the SRT(C)P packet overhead.

Length of MKI field: optional to support, mandatory to support if MKI is supported, mandatory to use if MKI is used.

"SESSION PARAMETERS"

key derivation rate: optional to support and use

UNENCRYPTED_SRTP: mandatory to support and optional to use

UNENCRYPTED_SRTCP: mandatory to support and optional to use

UNAUTHENTICATED_SRTP: mandatory to support and optional to use

NOTE: The flags "UNENCRYPTED_SRTP" and "UNENCRYPTED_SRTCP**"** may be useful when regulations do not permit encryption, but authentication is still desired. The flag "UNAUTHENTICATED_SRTP" may be useful to reduce the packet size for e.g. voice traffic where integrity protection may not be needed, cf. the situation on 3GPP radio interfaces over which user data are not integrity-protected.

forward error correction order: not applicable

key parameters for the FEC stream: optional to support and use

window size hint: optional to support and use

Annex F (normative): IMS media plane security for immediate messaging

F.1 Void

F.2 Security for immediate messaging based on SIP signalling security

Security for immediate messaging based on IMS signalling security shall be provided by the SIP signalling protection mechanisms specified in TS 33.203 [4].

NOTE1: The usage of the "P-Asserted-Identity" header provides secure identification of the sender of a message by the receiver, unless the sender has chosen to hide its identity, in which case the receiver will not learn the sender's identity.

NOTE2: SIP messages between the UE and the P-CSCF (IMS-ALG) can be confidentiality-protected either by the confidentiality mechanisms of IPsec or TLS as defined in TS 33.203 [4], or by confidentiality provided by the underlying access network, according to clause 6.2.1.2 of the present specification. The IMS UE is aware of the established protection mechanism, but the P-CSCF takes the final decision.

NOTE3: The IMS UE can be aware of the protection mechanism for immediate messaging on the first hop only, and there is no way for the IMS UE to ensure the use of protection mechanisms on further hops. Moreover, nodes in the IMS core (in particular the P- and S-CSCF) will have access to the cleartext message content.

NOTE4: Application servers may be used for storing instant messages for a user that is currently not registered or for distributing instant messages to multiple recipients. In this solution, such application servers have access to the message content and need to be trusted.

F.3 Security for immediate messaging based on MIKEY-TICKET

F.3.1 UE sends a SIP MESSAGE

A UE prepares a protected SIP message as described in TS 24.247 [28], with the difference that S/MIME is applied for content protection. Here S/MIME refers to the pre-shared-key variant of S/MIME defined in Annex I of this TS, and not the RFC 8551 [43] definition of S/MIME. This variant of S/MIME encrypts and authenticates the MIME content using a symmetric key that is transported inside a TRANSFER_INIT message. An example of a protected MESSAGE is shown below.

```
MESSAGE sip:user2@domain.com SIP/2.0
Via: SIP/2.0/TCP user1pc.domain.com;branch=z9hG4bK776sgdkse
Max-Forwards: 70
From: sip:user1@domain.com;tag=49583
To: sip:user2@domain.com
Call-ID: asd88asd77a@1.2.3.4
CSeq: 1 MESSAGE
Content-Type: multipart/mixed;boundary="boundary1"
Content-Length: <length>

--boundary1
Content-Type: application/mikey
Content-Transfer-Encoding: base64

<Base64 encoded TRANSFER_INIT message>

--boundary1
Content-Type: application/pkcs7-mime;
```

```
    smime-type=auth-enveloped-data;
    name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m

*********************************************************
* Content-Type: text/plain                              *
*                                                       *
* All your base are belong to us.                       *
*********************************************************
```

The UE needs to ensure that the TICKET inside the TRANSFER_INIT is resolvable by all the intended recipients. Typically, the intended recipient is the URI indicated in the To header field of the request. This is true when:

- The message is sent to another user using an IMPU in the To header field. The UEs registered under that IMPU are the intended recipients of the content.
- The message is sent to a list server using a PSI (Public Service Identity) in the To header field. The PSI is the intended recipient even though it is not the final recipient. This is because the list server hosting the PSI needs to be able to re-encrypt the content before forwarding it (it is assumed that neither the sending UE nor the KMS knows the members of the list). From the KMS perspective the PSI is seen as one of the list server's identities.

The only case when the URI in the To header field is not the intended recipient of the content is when:

- The message is sent to a list server and a URI list is included in the message body. The URIs in the URI list are the intended recipients of the content but not necessarily the list server. Since the sending UE knows the identities of the final recipients the list server does not have to re-encrypt the content before forwarding it. If the list server is not included as an intended recipient, the URI list needs to be sent un-protected or protected separately using an additional S/MIME entity.

For efficiency reasons the sender may want to re-use a TICKET in several SIP MESSAGEs sent to the same or different users. This is possible as long as all recipients were listed as authorized resolvers in the ticket request. It is important to be aware though that specifying a very wide group of resolvers may impact security.

Proof-of-origin (or non-repudiation) can be provided by the sender by adding the extension payload described in Annex D to the TRANSFER_INIT message. The extension payload contains a copy of the MAC calculated over the MIME entity and since the origin of the TRANSFER_INIT message is guaranteed, the origin of the MIME entity is guaranteed as well. The downside of providing proof-of-origin is that that the receiver has to do a ticket resolve against the KMS for every message that it receives.

F.3.2 UE receives a SIP MESSAGE

Upon receipt of a protected SIP MESSAGE, the UE extracts the key in the TRANSFER_INIT and hands both the key and the protected content over to S/MIME. S/MIME in turn uses the key to verify the integrity and decrypt the content. The UE also checks if the sender identity reported back by S/MIME matches the identity contained in the From header field. In case the identities differ, the S/MIME identity takes precedence and needs to be displayed to the user. As described above, this may happen when a list server re-encrypts the content but leaves the From header field intact. The same thing happens when a list server adds its own protected content to a forwarded message (for example the identities of the other recipients). Otherwise, the handling is as described in TS 24.247 [28].

Deferred delivery with MIKEY-TICKET can be accommodated by using a replay cache for TRANSFER_INIT messages which does not enforce any message age restriction (this is not required either by MIKEY [11]), The replay cache would accept a new entry as long as the cache is not full or if the entry is more recent than the oldest entry (determined from the message timestamp). If the cache is full and the oldest entry is older, the oldest entry is deleted and the new entry is inserted. Furthermore, the size of the cache needs to be adjusted according to the expected message intensity and the offline time (i.e. the period during which the UE is unreachable). The AS can also reduce the likelihood that a valid message gets rejected by delivering all the deferred messages in order, starting with the oldest one. However, even with the increased cache size, in case of high volume of messages or extended offline time the UE may run out of memory and has to start dropping messages.

F.3.3 List server forwards a SIP MESSAGE to multiple recipients using a PSI

A protected SIP MESSAGE that includes a PSI in the request URI is forwarded by the list server to all the entries in the associated URI list as specified in TS 24.247 [28]. The only difference is that the protected content in the incoming message needs to be re-encrypted before it is copied to the outgoing message. When the list server decrypts the content it needs to verify that the sender identity reported by S/MIME matches the identity in the To header field of the incoming message. Provided the verification is successful, the list server re-encrypts the content and sets the MIKEY-TICKET in the TRANSFER_INIT to be resolvable by all the entries in the predefined URI list. The re-encrypted content is then copied to all of the outgoing messages.

F.3.4 List server forwards a SIP MESSAGE to multiple recipients using a URI-list

A protected SIP MESSAGE with a URI-list included in the multipart body is forwarded by the list server to all the entries in the list as specified TS 24.247 [28]. There is no need to re-encrypt the protected content since the TICKET inside the TRANSFER_INIT is resolvable by the final recipients. Note that the list server forwards both the S/MIME content and the TRANSFER_INIT message.

If the list server includes a URI-list in the outgoing SIP message, as described in RFC 5365 [29], it should be protected using S/MIME. It is recommended to encrypt the URI-list once and copy it to all the outgoing messages by using a TICKET that is resolvable by all the recipients.

Annex G (normative): IMS media plane security for conferencing

G.1 General aspects

A conference server may send and receive cryptographically protected media streams to and from participants as specified in clauses G.2 and G.3. In doing so, the conference server shall use individual keys per participant (and per media stream).

NOTE: This means the conference server does not use group keys. This way, a participant is only able to decrypt media sent to him during his presence in the conference (but not media sent out by the media server to other participants, e.g. before the participant joined or after he left the conference).

Once the conference URI has been created, the participants (including the conference creator himself) join the conference using one of the methods specified in TS 24.147 [25]:

- The participant sends a SIP INVITE directly to the conference URI (how the participant learns of the SIP URI is out of scope)
- The conference creator or conference focus sends a SIP REFER to participant which triggers the participant to send a SIP INVITE to the conference URI
- The conference creator instructs the conference focus (either via SIP REFER or via the external interface) to send a SIP INVITE to the participant

Regardless of the method chosen the end result is always that a SIP INVITE is sent from the participant to the conference URI or vice versa. From a media security perspective, this situation is no different from a point-to-point call between two UEs.

The conference creator or a conference participant may subscribe to the conference event package as described in RFC 4575 [26] using the stored conference URI. Whenever there is a change to the conference state the subscription service will notify the subscribers by sending a NOTIFY request.

G.2 Security for conferencing based on SIP signalling security

Two cases are considered in this subclause: e2ae security between UE and IMS Access GW and e2e security between UE and conference server.

e2ae security:

When participating in conferences, IMS UEs may use e2ae security for RTP based traffic and/or for MSRP, as specified in the main body of the present document, and/or for BFCP, as specified in the following.

For BFCP that may be used in conferences, e2ae security shall be supported in the same way as for MSRP, as specified in the main body of the present document. The only differences are:

1) e2ae security for BFCP uses individual indications "e2ae-security for BFCP supported by the UE" and "e2ae-security for BFCP supported by the network" during registration (the syntax is to be defined in the corresponding stage 3 specification); compare clause 7.1.2 .

2) In the SDP, security for a BFCP media stream is specified by using the transport “TCP/TLS/BFCP”,

NOTE 1: Application of e2ae security for RTP, MSRP and/or BFCP is not visible to the conference server, which has therefore no assurance on how the communication is secured over the access networks. The conference server itself is assumed to be an MRF that is part of the IMS core network. Protection of the interfaces of the conference server to other entities of the IMS core can therefore rely on the security provided inside the IMS core (e.g. by means of IPsec).

e2e security:

The conference server may support e2e security using SDES for RTP based media between IMS UE and conference server as specified in clauses 7.2.2 and 7.3.2 of the present document. Usage of this type of security by the conference server, i.e. accepting it when offered in incoming SDP offers (dial-in case) and offering it in outgoing SDP offers (dial-out case) is subject to the policies of the conference server.

NOTE 2: e2e security between IMS UE and conference server does not imply e2e security between two IMS UEs.

It is outside the scope of the solution in the present clause whether the conference server supports TLS for MSRP according to RFC 4975 [21] and/or for BFCP according to RFC 8855 [44].

NOTE 3: The conference server can request TLS for MSRP and/or for BFCP in SDP offers it sends in outgoing SDP offers (dial-out case) and accept and perform TLS when it is specified in incoming SDP offers (dial-in case). This depends on the policies of the conference server. If the conference server is configured not to use TLS, then MSRP and/or BFCP can still be protected by TLS over the access network between an IMS Access GW and a participant according to clause 7 and/ or the present clause of the present document, if the participant and the network have negotiated using this protection over the access network.

NOTE 4: When the conference server uses SRTP/SDES for RTP based media, it has no assurance where this protection is terminated and how the communication is secured on the subsequent hops.

By means of the “P-Asserted-Identity” header, the conference server has assurance about the identity of the participants. A conference server may reject users trying to dial-in anonymously. In the dial-out case, by means of re-targeting an INVITE by the conference server may be answered by a user different from the invited user. The conference server may cancel the invitation of a participant if this participant’s identity is not revealed, or if the participant is not allowed to join the conference according to the conference policies.

G.3 Security for conferencing based on MIKEY-TICKET

G.3.1 Conference creation and policy control

The KMS based conferencing solution relies on an external interface between the conference creator and the AS/MRFC for creating and managing conferences. The interface should enable the conference creator to create new conference URIs, set and update the list of authorized conference participants, and change other conference settings. It may also be possible to allow other conference participants to change the conference policy. The interface is not considered part of IMS and will not be standardized. It would typically be implemented as a web page or as a specific application on the UE.

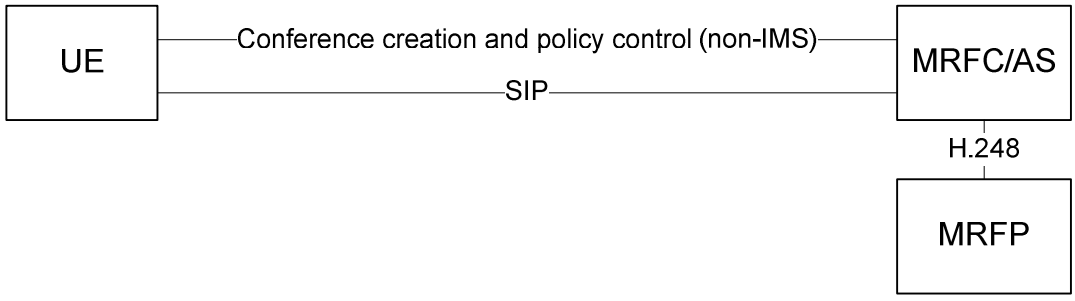


Figure Y1: Conference creation and policy control via external interface

G.3.2 User joining a secure conference

RTP and MSRP traffic shall be protected using MIKEY-TICKET in the same way as specified in Clause 7.2.3 and 7.3.3. The only difference being that one of the UEs is replaced by the conference focus. BFCP traffic shall be protected in the same way as MSRP traffic, i.e. using a TLS tunnel established with MIKEY-TICKET. In the SDP, security for BFCP is specified by using the transport “TCP/TLS/BFCP”.

The conference focus shall verify that the UE identity (KMS UID) specified in the MIKEY-TICKET exchange is authorized to join the conference.

G.3.3 Subscribing to conference event package

Upon receipt of a SUBSCRIBE request, the conference notification service shall verify that the sender is an authorized conference participant and, provided the verification is successful, establish the subscription to the conference state information. The state information carried in NOTIFY requests shall be confidentiality and integrity protected using the pre-shared key variant of S/MIME as described in Annex I.

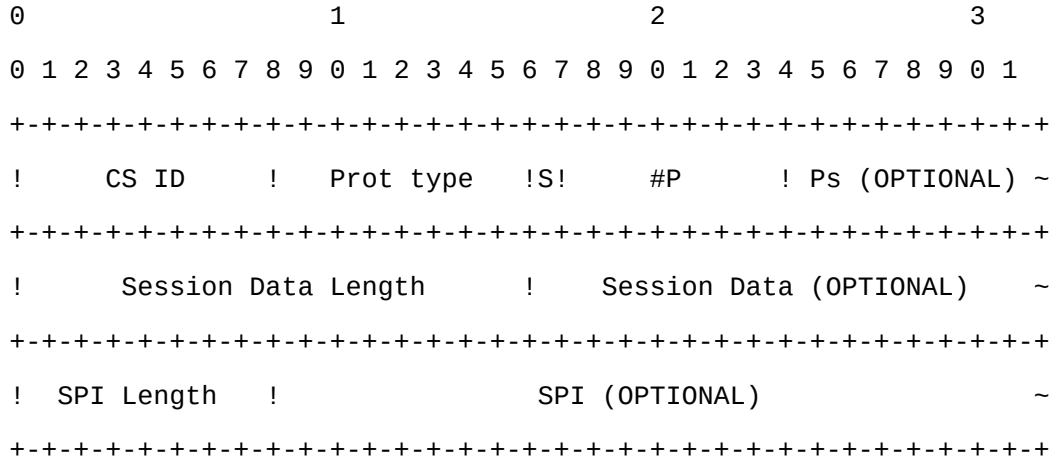
NOTE: S/MIME offers only limited protection to the conference state information. An attacker will still be able to delay, re-order or delete state information carried in the NOTIFYrequests. This could for example lead to a situation where conference participants incorrectly believe that a certain user has not yet joined the conference.

Annex H (normative): Setup of TLS-PSK using MIKEY-TICKET

Although MIKEY-TICKET [14] only specifies how to establish key data and algorithm settings for the SRTP protocol, it can easily be extended to carry the security parameters needed for setting up almost any kind of security protocol. This Annex describes how MIKEY-TICKET is used to establish a PSK to be used in a TLS-PSK handshake.

H.1 The TLS Prot Type

A Crypto Session (CS) in MIKEY-TICKET defines a security association for a specific security protocol, and contains all the required security parameters, such as key data and algorithm settings. Each CS is represented by an entry in the CS ID map info field of the HDR payload. Such an entry has the following format (assuming the GENERIC-ID map type is used):



- CS ID (8 bits): defines the CS ID to be used for the crypto session
- Prot Type (8 bits): defines the security protocol to be used for the crypto session. Shall be set to TLS.
- S (1 bit): flag that MAY be used by the Session Data. This flag is not used for the Prot Type TLS. The value needs to be set to '0', but shall be ignored by the receiver.
- #P (7 bits): indicates the number of security policies provided for the crypto session. For the Prot Type TLS, this value shall be set to 0. No security policy is required since negotiation of parameters is included in the TLS handshake.
- Ps (variable length): lists the policies for the crypto session. Since #P=0 for the Prot Type TLS, this field is omitted.
- Session Data Length (16 bits): the length of Session Data (in bytes). For the Prot Type TLS, the length shall be set to 0 as no additional session data is required.
- Session Data (variable length): contains session data for the crypto session. Since length is 0 for the Prot Type TLS, this field is omitted.
- SPI Length (8 bits): the length of SPI (in bytes). For the Prot Type TLS, the length can be set arbtrarily.
- SPI (variable length): the SPI corresponding to the session key to be used for the crypto session. The SPI identifies a specific TGK/GTGK that is used to derive the TEK for the crypto session (the SPI could also identify a TEK directly).

Editor's note: Setting #P=0 in both the init and response message is not allowed according to RFC 6043. There are two possible ways to get around this problem. Either we ignore the restriction in RFC 6043 (which really doesn't matter) or we specify a dummy Security Policy for TLS which does not contain any values.

Editor's note: The Prot Type TLS must be registered with IANA and the value is therefore TBD.

H.2 Establishing a TLS connection

A CS with Prot Type TLS contains the necessary parameters to perform a TLS-PSK handshake and establish a TLS connection over a reliable transport association (such as a TCP connection). It is assumed that the transport association can be used to identify the CS (e.g. a TCP connection maps to a certain m line in the SDP which in turn maps to a CS). The parameters that need to be input to the TLS implementation are the following:

- TLS client/server role: the role of each peer is negotiated by means outside of MIKEY-TICKET (e.g. as part of the establishment of the transport association in SDP). Typically, the client (server) in the transport protocol assumes the role of client (server) in the TLS protocol.
- The TLS ciphersuites shall be of type TLS_PSK and TLS shall be profiled as specified in TS 33.310 Annex E [AA] with the exception that ciphersuites using Diffie-Hellman shall not be used.
- PSK identity: this value is not used. The PSK identity is set to the empty string by the client and is ignored by the server.
- PSK identity hint: this value is not used. The identity hint is an optional value provided by the server in the server hello message.
- PSK: The PSK is the TEK associated with the CS. The SPI in the CS points to a TGK or GTGK from which the TEK is derived using the CS ID (and some other parameters). The SPI could also point to a TEK directly.

H.3 Usage with SDP

The TLS CS defined above can be used to establish a TLS connection using the PSK-TLS ciphersuite. The only piece missing is to show how an m-line using a protocol of the form X/TLS/Y (e.g., TCP/TLS/MSRP or TCP/TLS/BFCP) is mapped to such a CS.

RFC 4567 [12] describes how the key-mgmt attribute is used to perform a MIKEY-TICKET exchange in SDP and how an m-line can be mapped to set of SRTP CSs (one for each SSRC). If the key-mgmt attribute is used at session level then the MIKEY-TICKET exchange contains CSs for all the m-lines in the SDP and the mapping is based on the order of the m-lines. If the key-mgmt attribute is used at the media level then the CSB only contains the CSs for that m-line. Mixing of session and media level attributes is allowed by RFC 4567 [12] but the expected behaviour is not well defined. Another restriction is that the offerer needs to know how many SSRCs that the answerer will use for a particular m-line.

The mapping between an X/TLS/Y m-line and a TLS CS is done in the same way as the mapping between and SRTP m-line and a set of SRTP CSs. The only difference is that there is exactly one CS per m-line.

Annex I (normative): Pre-shared key MIME protection

Secure/Multipurpose Internet Mail Extensions (S/MIME), defined in IETF RFC 5751 [30], is a standard for encryption and signing of MIME encoded data. S/MIME uses Cryptographic Message Syntax (CMS), defined in IETF RFC 5652 [31], to cryptographically protect MIME entities. Unfortunately, S/MIME was designed for public key cryptography and does not specify how a MIME entity can be encrypted and authenticated using a pre-shared key. However, extending S/MIME to support symmetric crypto is not a major issue since CMS already defines the necessary message constructs and algorithms.

I.1 The smime-type parameter

S/MIME defines the application/pkcs7-mime media type that is used to carry different types of CMS content types. Information about the applied security and the CMS content type (EnvelopedData, SignedData, CompressedData) can be indicated via the optional "smime-type" parameter. To add support for pre-shared key MIME protection an additional smime-type parameter is defined:

Table I.1: smime-type (addition)

Name	CMS Type	Inner Content
auth-enveloped-data	AuthEnvelopedData	id-data

Editor's note: Whether we can continue using the MIME type application/pkcs7-mime when the new smime-type parameter is introduced is FFS. It might be necessary to register a new MIME type application/X with IANA (in the vendor tree where vendor is 3GPP). The new MIME type would have the same semantics as application/pkcs7-mime but would also include the smime-type auth-enveloped-data.

I.2 The Auth-Enveloped S/MIME type

I.2.1 General

AuthEnvelopedData is a CMS type defined in IETF RFC 5083 [32] and is intended to be used with authenticated encryption modes, such as AES-CCM and AES-GCM. These algorithms allow arbitrary data to be both authenticated and encrypted using a single key. IMS clients compliant with this this specification shall support the authenticated encryption algorithms in Table I.2.

Table I.2: Authenticated encryption algorithms

Algorithm name	Key size
AES-CCM	128, 256
AES-GCM	128, 256

The content-authenticated-encryption key is generated at random and is sent alongside the protected data in the RecipientInfo field of AuthEnvelopedData. The format of this field varies depending on the key management technique. IMS clients implementing this specificiation shall support the KEKRecipientInfo type where the content-authenticated-encryption key is encrypted using a previously distributed symmetric key. Table I.3 shows the key encryption algorithms that the IMS client shall support (see RFC 3565 [33]).

Table I.3: Key encryption algorithms

Algorithm name	Key size
AES-WRAP	128, 256

The data to protect (a MIME entity) shall be prepared as in standard S/MIME before it is passed on to CMS for encryption and authentication. The encrypted data shall be included in the EncryptedContent field and the ContentType shall be set to id-data (i.e., the plaintext is treated as arbitrary octet data by CMS).

I.2.2 Creating an Auth-Enveloped message

This Clause describes how a MIME entity is protected using the auth-envoloped S/MIME type. With the exception of the second step, the process is identical to the creation of an Enveloped-Only message in S/MIME [43].

a) The MIME entity to be protected is prepared according to Section 3.1 in S/MIME [43].

b) The MIME entity and other required data is processed into a CMS object of type AuthEnvelopedData. The key for the desired content-authenticated-encryption algorithm is generated at random and is sent encrypted in a KEKRecipientInfo. The previously distributed key encryption key is identified via a KEK identifier.

c) The AuthEnvelopedData object is wrapped in a CMS ContentInfo object.

d) The ContentInfo object is inserted into an application/pkcs7-mime MIME entity.

The smime-type parameter for auth-enveloped messages is "auth-enveloped-data". The file extension for this type of message is ".p7m". An example message is shown below.

```
Content-Type: application/pkcs7-mime;
    smime-type=auth-enveloped-data;
    name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m

*******************************************************
* Content-Type: text/plain                            *
*                                                     *
* All your base are belong to us.                     *
*******************************************************
```

I.3 Transferring KEK using MIKEY-TICKET

MIKEY-TICKET shall be used to transfer the S/MIME key encryption key (KEK) to the remote recipient. The KEK shall be included in a TRANSFER_INIT message which in turn shall be added to the SIP message using the application/mikey media type.

The KEK (which corresponds to a TEK in MIKEY-TICKET) is identified by its SPI and shall be derived from the TGK carried inside the TICKET payload of the TRANSFER_INIT message.

In order to ensure that the receiver has access to the KEK when the S/MIME message is processed, it is recommended to send the TRANSFER_INIT message and S/MIME message in the same SIP message. As shown in the example below, this can be appomplished by using the multipart/mixed media type and including the TRANSFER_INIT message at the top.

```
Content-Type: multipart/mixed;boundary="boundary1"
Content-Length: <length>

--boundary1
Content-Type: application/mikey
Content-Transfer-Encoding: base64

<Base64 encoded TRANSFER_INIT message>

--boundary1--
Content-Type: application/pkcs7-mime;
    smime-type=auth-enveloped-data;
    name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m

*******************************************************
* Content-Type: text/plain                            *
*                                                     *
* All your base are belong to us.                     *
*******************************************************
```

By default a KEK shall only be used once. This together with the fact that TRANSFER_INIT messages are replayed protected imply that the S/MIME message is replayed protected as well. Other types of security policies are outside the scope of this document.

Optionally, proof-of-origin (or non-repudiation) can be achieved by adding the extension payload defined in Annex X to the TRANSFER_INIT message and including a copy of the MAC value calculated over the MIME entity. Since the origin of the TRANSFER_INIT message can be guaranteed (Initiator Data in the TICKET payload is authenticated with a key known only to the sender and the KMS), the origin of the MIME entity can be guaranteed as well. The downside of providing non-repudiation is that the receiver has to do a ticket resolve against the KMS for every message that it receives (there is no point of caching the results of a ticket resolve since the TICKET payload always changes).

I.4 MIKEY-TICKET profile for pre-shared key MIME protection

The MIKEY-TICKET profile for pre-shared key MIME protection is the same as the profile for IMS Media Plane security (see Annex D) except for a few minor differences. These differences are explained below.

The Ticket Request exchange is unchanged except that IDRapp in the Ticket Policy (TP) payload shall be set to the string "PSK/MIME".

The Ticket Transfer exchange is half-roundtrip and consists only of the TRANSFER_INIT message. This message is constructed as in IMS Media Plane security, except for the following changes:

- The HDR payload shall contain a single Crypto Session (CS) of type PSK/MIME. A CS of this type has no associated Security Policy (#P=0) and no Session Data. The CS SPI field shall be set to the SPI of the TGK carried in the TICKET (see below). Furthermore, as no answer is expected, the V flag in the HDR payload shall be set to 0.

  The extension payload defined in Annex X needs to be included if proof-of-origin is required for the MIME entity. The value of the extension payload is the MAC calculated in the authenticated encryption algorithm. Note that proof-of-origin requires that Initiator Data is included in the TICKET payload which in turn requires that forking is enabled (I flag in the Ticket Policy is set to 1).

The Ticket Resolve exchange is unchanged

Tickets are generated in the same way as in the IMS Media Plane security profile except for the changes indicated below.

- The F flag shall be set to 0 indicating that TRANSFER_RESP should not be sent
- The G shall be set to 0 indicating that the Responder should not generate RANDRr
- The I shall be set to 0 (no-forking) unless proof-of-origin is required for the MIME entity
- The KEMAC payload in the TICKET shall contain a single TGK with the SPI field set to the value of S/MIME key encryption key identifier. No salt or key validity period shall be included.

Editor's note: No Security Policy is required for a CS of type PSK/MIME since all the algorithms, key lengths, etc are specified by S/MIME. However, it is currently unclear if it is allowed to omit the Security Policy payload (#P=0) from a TRANSFER_INIT message.

Editor's note: Proof-of-origin requires that Initiator Data is included in the TICKET payload which in turn requires that forking is enabled. However, forking was originally intended to be used in the cases where the responder is able to send a TRANSFER_RESPONSE, and the MIKEY-TICKET was written with this in mind. It might be therefore be necessary to add some text explaining why forking still works.

Editor's Note: This Annex was added to enable other clauses to refer to it. It will be filled with text later.

Annex J (normative): IANA considerations

J.1 IANA assignments

This clause defines several new values for the namespace Prot Type defined in IETF RFC 3830 [11]. IANA is requested to record the assignments in Table X to the namespace Prot Type in the MIKEY payload registry. The Prot Types can be used by any MIKEY mode.

Table J: Prot Type (Additions)

Type	Value	Comments
TLS	TBD1	TLS-PSK
PSK S/MIME	TBD2	See Annex I
Application Specific	TBD3	Application Specific

TLS: This Prot Type provides a pre-shared key (TEK) to be used in pre-shared key ciphersuites for (D)TLS as specified in Annex H.

PSK S/MIME: This Prot Type provides a pre-shared key (TEK) to be used to protect MIME content as specified in Annex I.

Application Specific: This Prot Type provides pre-shared key(s) to be used in an application specific security protocol. Security policies (SP payloads) shall not be associated with the Crypto Session (CS).

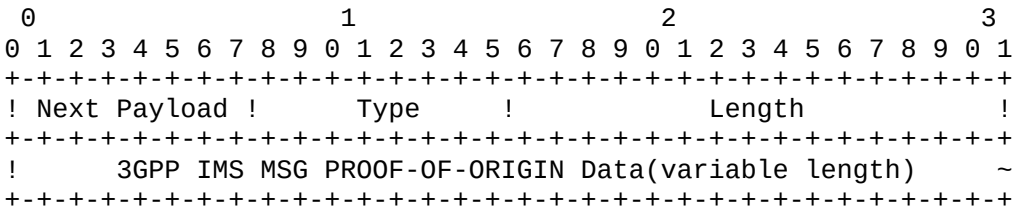
Editor's note: The values TBD1, TBD2, and TBD3 will later be replaced with values assigned by IANA.

Annex K (normative): MIKEY general extension payload for message proof-of-origin

This clause specifies a new MIKEY General Extension Payload to provide proof-of-origin for an arbitrary message. It is intended to be used together with the pre-shared key MIME protection defined in Annex I where the MAC of the MIME entity is copied to a TRANSFER_INIT message. Since the origin of the TRANSFER_INIT message is guaranteed, the origin of the MIME entity will be guaranteed as well (the receiver compares the MAC value of the MIME entity to the MAC value in the extension payload).

K.1 Payload format

The 3GPP IMS MSG PROOF-OF-ORIGIN Type (Type TBD) formats the MIKEY General Extension payload as follows:



- Next Payload and Length are defined in Section 6.15 of MIKEY [11]
- Type (8 bits) identifies the type of the General Extension Payload (see Section 6.15 of MIKEY [11]). This Annex adds a new type. It specifies the use of Type TBD for 3GPP IMS MSG PROOF-OF-ORIGIN.
- 3GPP IMS MSG PROOF-OF-ORIGIN Data (variable length): contains the data whose origin needs to be asserted. The interpretation of the data is application/context specific (data could for example be the hash of a much longer message, where the hash algorithm is defined by the application/context)

Editor's note: The 3GPP IMS MSG PROOF-OF-ORIGIN type must be registered with IANA

Annex L (normative): IMS media plane security for T.38 fax

L.1 Introduction

The transmission of fax over IP networks is specified in the ITU-T recommendation T.38 [34] and uses either TCP or UDP for transport. T.38 allows transmission of fax over IP networks in real time and allows interworking with the legacy PSTN T.30 fax protocol. For the TCP transport, IFP (Internet Fax Protocol) is encapsulated in TPKT. For the UDP transport, IFP data is encapsulated in either UDPTL (UDP Transport Layer) or RTP. The purpose of UDPTL and RTP is to provide sequence numbering and packet redundancy (to cope with packet loss).

UDPTL (UDP Transport Layer) is the predominant means for transporting T.38. For IMS, a profile of T.38 fax is specified in Annex L of TS 26.114 [35]. This profile only supports UDPTL/UDP transport. The packet structure for UDPTL based T.38 fax is shown in Figure L-1.

Figure L–1: Packet structure for UDPTL based T.38 fax transmission [34]

A T.38 fax call is established in SIP/SDP similar to how an audio or messaging session is established. Figure L-2 shows how the SDP media line is constructed in case of UDPTL/UDP transport.

```
m=image 49170 udptl t38
a=...
```

Figure L-2: Example SDP offer forT.38 fax transmission using UDPTL/UDP transport (non-relevant parts of the SDP offer have been excluded)

L.2 Use cases

As fax has a special legal status in many countries and enjoys continuing support, specification of secure fax is important. As most faxes are still connected to PSTN, the primary use case is seen as a fax call between an IMS UE and a PSTN/CS fax terminal. In order to support this use case media protection needs to start at the IMS UE and be terminated before or at the PSTN GW. Fax calls between two IMS UEs is another possibility but is not as common, and in this case there exist other alternatives like attaching the fax in an email or instant message using ITU-T recommendation T.37.

L.3 e2ae security for T.38 fax using DTLS

T.38 fax using UDPTL/UDP transport shall be secured e2ae between IMS UE and IMS-AGW by usage of DTLS (IETF RFC 6347 [36]). DTLS shall be profiled as defined in Annex M of the present document. The transport protocol identifier "UDP/TLS/UDPTL" and the usage of UDPTL over DTLS are defined in IETF RFC 7345 [37].

The solution leverages IMS control plane security by using self-signed certificates and exchanging the certificate fingerprints via SIP/SDP. Usage of the "P-Asserted-Identity" header provides secure identification of the other endpoint. The solution is almost identical to MSRP e2ae security specified in this document, but uses DTLS instead of TLS for confidentiality and integrity protection.

Support for e2ae security for T.38 shall be indicated during registration in the same way as specified for RTP and MSRP based media. The indication shall be be done independently from the indication of support for e2ae security for RTP or MSRP based media, and shall use its own indications "e2ae-security for T.38 supported by the UE" and "e2ae-security for T.38 supported by the network" (the syntax is to be defined in the corresponding stage 3 specification).

The originating IMS UE shall set the transport identifier to "UDP/TLS/UDPTL" and include the SDP fingerprint attribute in the SDP offer. Moreover, the IMS UE adds an SDP attribute "e2ae-security requested by UE" indicating the

request for e2ae security to the description of the T.38 fax call. The network shall insert the IMS access gateway into the media path and properly terminate DTLS, using its own certificate (the fingerprint of this certificate is returned to the originating IMS UE in the SDP answer). From the IMS access gateway in the direction towards the terminating IMS UE, plain UDP may be used on the next hops, assuming that the interfaces are protected.

Annex M (normative): TLS profile for IMS media plane security

M.1 General

TLS shall be supported as specified in annex E of 3GPP TS 33.310 [22] with the additions/modifications outlined below Since DTLS is based on TLS and functions more or less in an identical way, the same option shall be applied to both DTLS and TLS. In the rare cases where there is a difference, this will be pointed out. .

TLS cipher suites without encryption should not be used;

Pre-shared keys shall not be used for e2ae media security. E2ae media security shall be based on the cipher suites and session keys negotiated via the TLS handshake.

Editor's note: TLS certificate profile and validation is missing. A starting point is TS 33.203, O.5.

Annex N (normative): IMS media plane security interworking for WebRTC access to IMS and IMS data channels

N.1 General

This annex describes the additional IMS media plane security features that are necessary to support WebRTC IMS Clients access to IMS as well as IMS data channels.

N.2 Media security for RTP

N.2.1 General

According to IETF RFC 8826 [39], all RTP traffic generated or received by a WebRTC client shall be protected with SRTP, using DTLS-SRTP [40, 41] as the key management protocol. This means that if a WebRTC IMS Client is supposed to be able to communicate with existing IMS endpoints (e.g. IMS UE or PSTN GW), DTLS-SRTP and SRTP shall be terminated at an intermediate node.

This clause describes the additional procedures and interface extensions required to support end-to-access-edge (e2ae) security for RTP using DTLS-SRTP and SRTP.

N.2.2 e2ae security for RTP using DTLS-SRTP

E2ae protection of RTP using DTLS-SRTP is similar to e2ae protection of MSRP using TLS/TCP and the session establishment procedures are therefore largely the same. In both cases certificate fingerprints need to be exchanged over SDP and the media has to be anchored in IMS by inserting a gateway on the media path. Similarly as for e2ae protection using SDES and TLS, the signalling path between the WebRTC IMS Client and the eP-CSCF needs to be secured.

Figure N.2.2-1 shows the originating procedure for e2ae protection of RTP using DTLS-SRTP. The terminating procedure is similar and is not shown here. Note that no assumption is made on the interface between the WebRTC IMS client and the eP-CSCF except that it is SDP based and integrity protected.

Since only e2ae security is supported at the moment, the WebRTC IMS Client is required to include the indication "e2ae-security requested by UE" in every offer it creates.

It is assumed that the eP-CSCF is aware of the fact the IMS UE is a WebRTC IMS Client and automatically applies e2ae security for terminating calls. Therefore, unlike the existing e2ae security for RTP and MSRP, there is no need for the IMS UE to explicitly indicate support of e2ae security during registration.

NOTE: Void

The DTLS-SRTP profile to use is described in Annex O of this document.

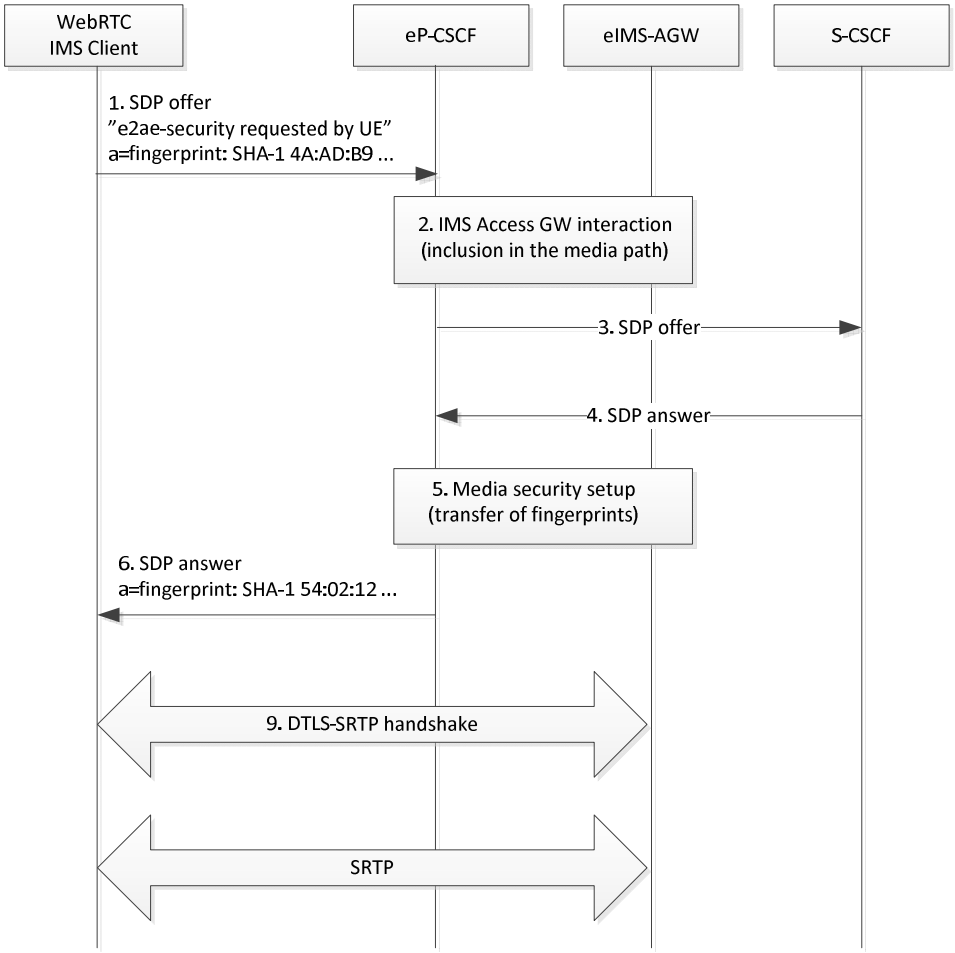


Figure N.2.2-1: E2ae protection of RTP based on DTLS-SRTP

N.3 Media security for WebRTC and IMS data channels

N.3.1 General

This clause describes how end-to-access-edge (e2ae) and end-to-end (e2e) security is achieved for WebRTC Data Channels (see IETF RFC 8831 [50], IETF RFC 8841 [48], and IETF RFC 8864 [51]). In addition the end-to-DC-edge (e2DCe) security is specified. The end-to-DC-edge (e2DCe) is defined to be the path between the UE and MF.

WebRTC-compatible browsers use SCTP over DTLS as transport protocol for peer-to-peer data. A WebRTC Data Channel is defined as two unidirectional SCTP streams, one in each direction, which are managed together as a single entity (see IETF RFC 8831 [50]). The application protocol which runs on top of the WebRTC Data Channel is not specified and the JavaScript is free to implement any protocol it requires.

The application protocols that a WebRTC IMS Client may need to support are MSRP, BFCP, T.140, and T.38. A DCMTSI IMS Client [35] also supports the unspecified application protocol approach used by WebRTC Data Channel with, for example, a related web page and JavaScript handling the needed transmission and protocol format actions.

Figure N.3.1-1 shows the common protocol stack and the required protocol translation for a WebRTC IMS Client, where the WebRTC Data Channel stack is not used in IMS core network or towards the peer. The transport protocol that the IMS-AGW applies on the remote side (marked X in the figure) depends on the application protocol. For MSRP and BFCP X=TCP, for T.140 X=RTP/UDP, and for T.38 X=UDPTL/UDP. In general, the IMS-AGW will forward the application protocol messages transparently. The only exception is MSRP messages which contain IP address information and therefore needs to be re-written by the IMS-AGW. This can however be avoided if both endpoint support the MSRP CEMA extension [24].

T.140 (real-time text) and T.38 (fax) are included here for sake of completeness. These are legacy protocols and are not expected to be commonly used.

Editor's Note: The final list of supported application protocols (e.g., MSRP, BFCP, T.140, and T.38) is to be decided by CT groups.

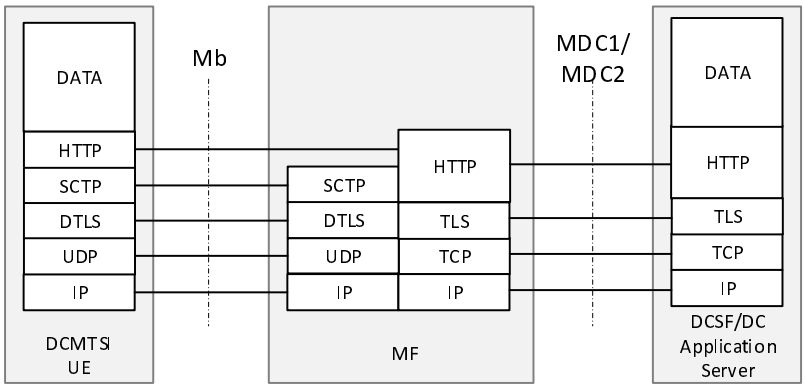


Figure N.3.1-1: Protocol stack for WebRTC IMS Client (WIC) Data Channels

Figures N.3.1-2 and N.3.1-3 are based on TS 23.228 [3] and show two examples of the protocol stack used by DCMTSI [35] Clients. Figure N3.1-2 shows a protocol stack for the HTTP proxy configuration mode for the Bootstrap Data Channel or Application Data Channel in case MF is anchoring DTLS.

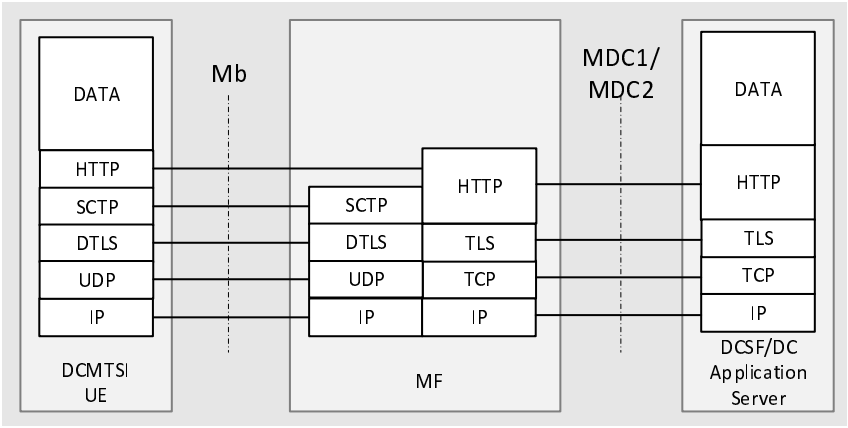


Figure N.3.1-2: Protocol stack for IMS bootstrap data channels (TS 23.228[3])

Figure N.3.1-3 shows protocol stack for the UDP proxy configuration mode for the Application Data Channel case, providing a Person2Application/Application2Person/Person2Person Data Channel Application.

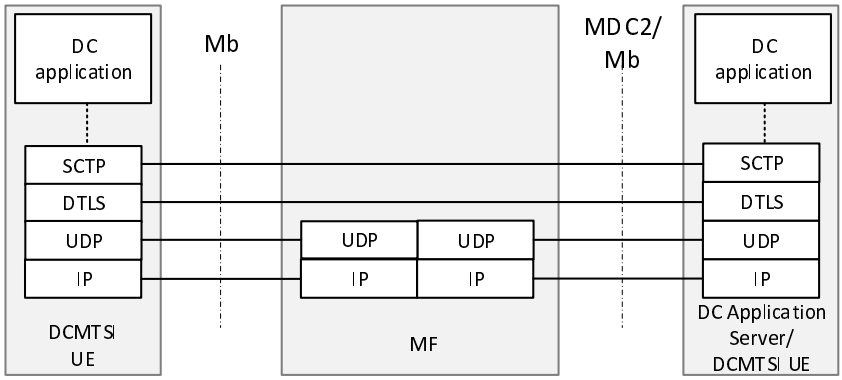


Figure N.3.1-3: Protocol stack for P2P/P2A/A2P IMS application data channels without MF (TS 23.228[3])

N.3.2 e2ae security for WebRTC data channels

E2ae security for WebRTC Data Channels for a WebRTC IMS Client (WIC) is achieved in the same way as e2ae security for MSRP over TLS/TCP. In both cases certificate fingerprints need to be exchanged over SDP and the media has to be anchored in IMS by inserting a gateway on the media path. To ensure the integrity of the certificate fingerprint the signalling path is assumed to be protected.

Figure N.3.2-1 shows the originating procedure for e2ae protection of WebRTC Data Channels. The terminating procedure is similar and is not shown here. Note that no assumptions are made on the interface between the WebRTC IMS Client and eP-CSCF except that it is SDP-based and integrity protected.

Since only e2ae security is supported at the moment for WebRTC IMS Client (WIC), the WebRTC IMS Client is required to include the indication "e2ae-security requested by UE" in every offer it creates.

It is assumed that the eP-CSCF is aware of the fact the IMS UE is a WebRTC IMS Client and automatically applies e2ae security for terminating calls. The P-CSCF is aware of a DCMTSI client, based on the IMS data channel media feature tag used by the DCMTSI client during registration. Therefore, unlike the existing e2ae security for MSRP over TLS/TCP, there is no need for the IMS UE to indicate support of e2ae security during registration.

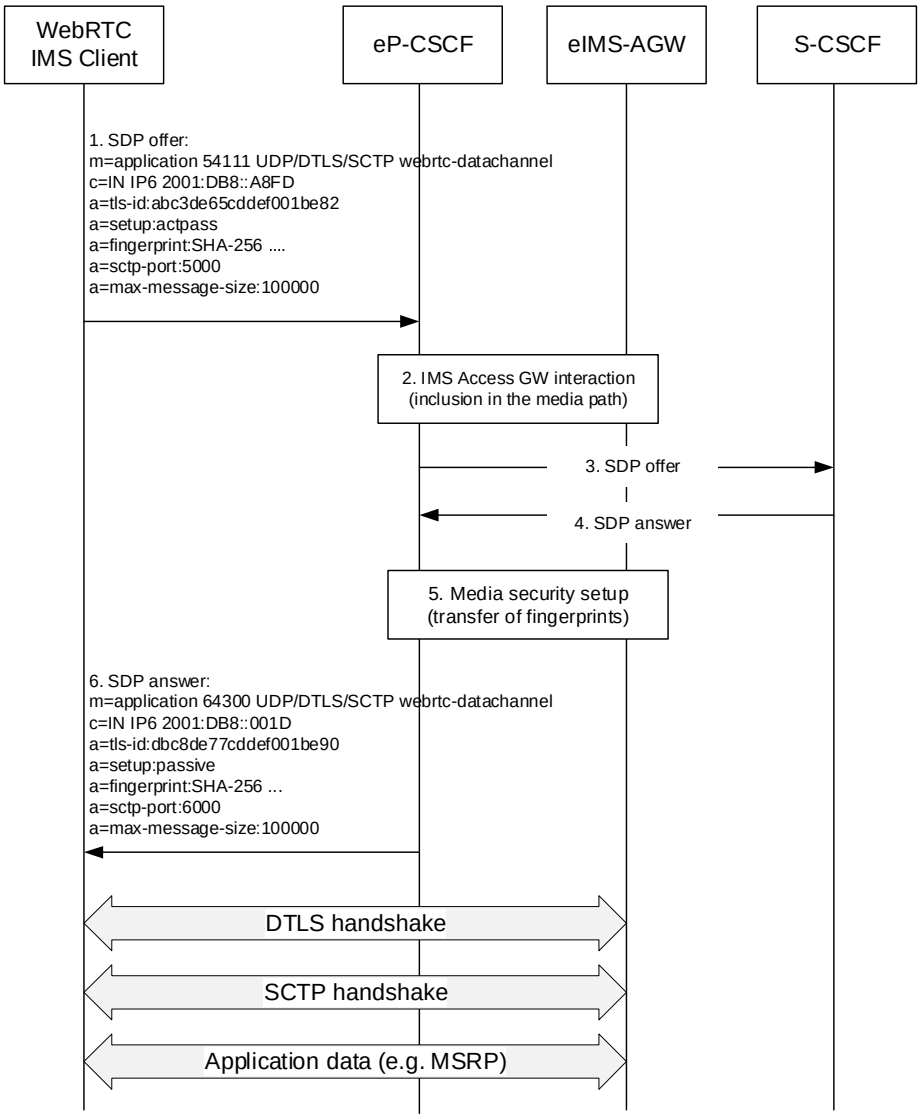


Figure N.3.2-1: E2ae protection of WebRTC Data Channels

NOTE 1: The method for negotiating the application protocol (e.g. MSRP) and configuring the WebRTC Data Channel (e.g. setting stream identifiers, choosing between reliable or unrealiable transmission, etc) is defined in the corresponding stage 3 specification, e.g., based on IETF RFC 8832 [42] or IETF RFC 8864 [51].

NOTE 2: From a security perspective, it is safe to multiplex several WebRTC Data Channels (e.g. one for MSRP and one for BFCP) on top of a single SCTP association and DTLS connection. However, there may be other, non-security related reasons that prevent this option.

NOTE 3: IMS Data Channel (DCMTSI) clients use a=dcmap lines from IETF RFC 8864 [51] in SDP, in addition to the SDP lines indicated above, while WebRTC clients do not. See also Figure N.3.4-1.

N.3.3 e2DCe security for IMS data channels

For DCMTSI clients using IMS data channel media, e2DCe security is achieved by anchoring DTLS in Data Channel Media Function (MF) while IMS Access GW is anchoring UDP but transparently letting through layers above UDP, to avoid unnecessary DTLS decryption/encryption operations, but otherwise handling certificates and fingerprints as above. See Figure N.3.1-2.

For IMS data channel (DCMTSI) clients, both e2DCe and e2e security shall be supported for IMS data channels and e2DCe security support may be included in SDP offers and answers.

N.3.4 e2e security for IMS data channels

E2e security for IMS Data Channels for DCMTSI clients is achieved in a similar way as for e2DCe security. See clause N.3.3. In both cases, certificate fingerprints need to be exchanged over SDP between the peers and certificates are exchanged through DTLS handshake in-band on the media path. The media may be anchored in IMS by inserting a gateway on the media path. To ensure the integrity of the certificate fingerprint, the signalling path is assumed to be protected.

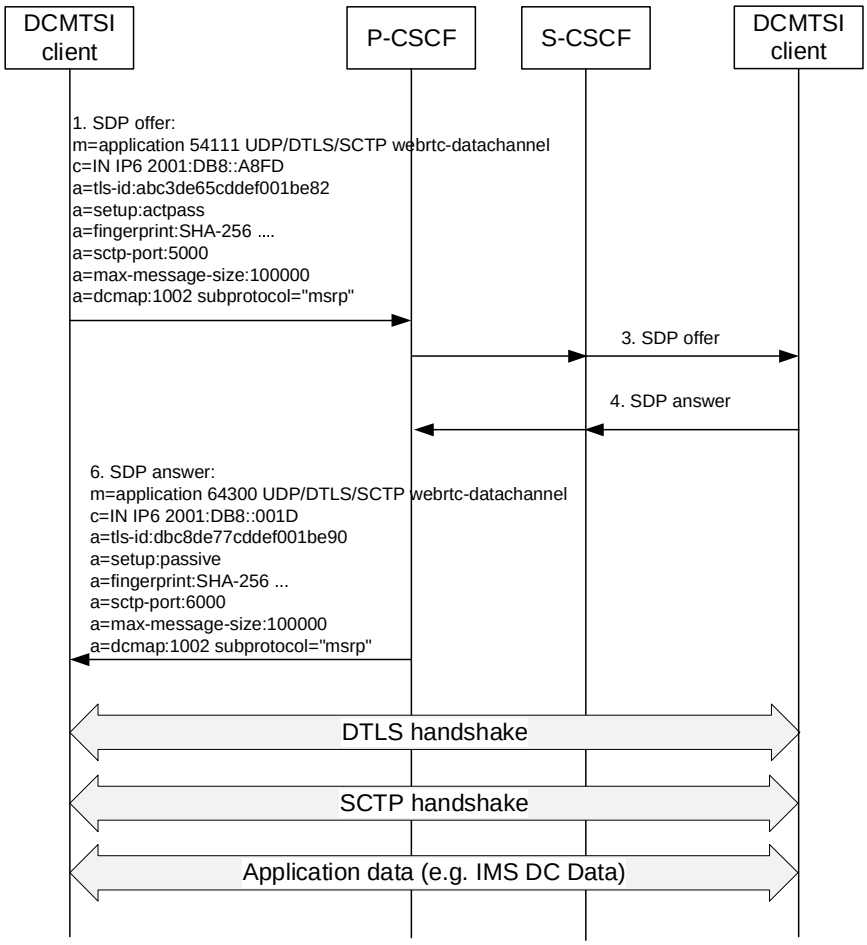


Figure N.3.4-1: E2E protection of IMS Data Channels

NOTE: SDP is not exchanged between the S-CSCF and the DC Application Server. The DC3 and DC4 interfaces are not specified in TS 23.228[3].

Annex O (normative): Profiling of DTLS-SRTP

The present Annex contains a list of parameters that may be contained in the use_srtp extension in the DTLS extended client hello, according to RFC 5764 [41]. The rest of the DTLS profile is as defined in Annex M of this document.

SRTP Protection Profiles:

The SRTP protection profile "AES_CM_128_HMAC_SHA1_80", as defined in RFC 5763 [40] and the SRTP protection profile "SRTP_AEAD_AES_128_GCM",as defined in RFC 7714 [46] are mandatory to support. Support of other protection profiles is optional.

SRTP Master Key Identifier (MKI):

Optional to use and support. Since a DTLS-SRTP handshake results in single SRTP master key, an endpoint has at most one active master key at any point in time. MKI signalling is therefore typically not required (the major exception would be if the peers perform frequent re-keying) and is not recommended.

Annex P (normative): Security aspects of next generation real time communication services

P.1 Security aspects of SBA in IMS media control interface

P.1.1 General

This clause describes the security features that are necessary to support SBA in IMS media control interface.

P.1.2 Protection at the network or transport layer

All service based network functions in IMS media control interface shall support protection at the network or transport layer as specified in clause 13 of TS 33.501 [47.

P.1.3 Authentication and authorization

All service based network functions in IMS media control interface and NRF shall support authentication and authorization as specified in clause 13 of TS 33.501 [47.

NOTE: It is assumed that slice related aspects are not applicable in IMS.

Annex Q (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
09-2009	SA#45	SP-090530	--	--	Presentation to SA for Information	---	1.0.0
12-2009	SA#46	SP-090826	--	--	Presentation to SA for Approval	1.0.0	2.0.0
12-2009	SA#46	--	--	--	Publication of SA-approved version	2.0.0	9.0.0
03-2010	SA#47	SP-100094	004	-	Various editorial corrections	9.0.0	9.1.0
03-2010	SA#47	SP-100094	005	-	Removal of Editor's note on specific error messages over Iq	9.0.0	9.1.0
03-2010	SA#47	SP-100094	006	-	Key lifetimes for end-to-access edge security	9.0.0	9.1.0
03-2010	SA#47	SP-100094	023	-	Removal of the ability to register e2e security capability	9.0.0	9.1.0
03-2010	SA#47	SP-100094	002	-	Correction of the use of reusable ticket	9.0.0	9.1.0
03-2010	SA#47	SP-100094	001	-	Clarification and correction in Clause 4	9.0.0	9.1.0
03-2010	SA#47	SP-100094	011	1	Security properties for e2ae protection using SDES	9.0.0	9.1.0
03-2010	SA#47	SP-100094	018	1	Corrections and clarifications in call set-up	9.0.0	9.1.0
03-2010	SA#47	SP-100094	013	1	KMS based e2e security	9.0.0	9.1.0
03-2010	SA#47	SP-100094	014	1	Integrity and confidentiality protection	9.0.0	9.1.0
03-2010	SA#47	SP-100094	015	1	GBA and its alternatives	9.0.0	9.1.0
03-2010	SA#47	SP-100094	020	1	Removal of editor's notes and editorial modifications	9.0.0	9.1.0
03-2010	SA#47	SP-100094	021	1	RFC 4771 mandatory for KMS based media plane security	9.0.0	9.1.0
03-2010	SA#47	SP-100094	022	1	Alignment of MIKEY-TICKET profiling with updated MIKEY-TICKET draft	9.0.0	9.1.0
03-2010	SA#47	SP-100094	016	1	Definitions and abbreviations corrections	9.0.0	9.1.0
03-2010	SA#47	SP-100094	019	1	Correction of notation	9.0.0	9.1.0
06-2010	SA#48	SP-100246	033	-	Registration Procedures	9.1.0	9.2.0
06-2010	SA#48	SP-100246	025	-	Editor's Note resolution in Sub. 5.4.2	9.1.0	9.2.0
06-2010	SA#48	SP-100246	026	1	e2ae indications	9.1.0	9.2.0
06-2010	SA#48	SP-100246	027	1	network impact for e2e security	9.1.0	9.2.0
06-2010	SA#48	SP-100246	028	1	abbreviations and editorial changes	9.1.0	9.2.0
06-2010	SA#48	SP-100246	029	-	Profiling of SDES	9.1.0	9.2.0
06-2010	SA#48	SP-100246	030	-	Correction of text on SDES parameters for e2ae security	9.1.0	9.2.0
06-2010	SA#48	SP-100246	031	-	Correction of text on SDES parameters for e2e security	9.1.0	9.2.0
06-2010	SA#48	SP-100246	032	-	Alignment with the updated MIKEY-TICKET draft	9.1.0	9.2.0
12-2010	SA#50	SP-100730	034	-	Correction to SDES profile	9.2.0	9.3.0
12-2010	SA#50	SP-100730	035	1	MIKEY-TICKET RFC 6043 reference	9.2.0	9.3.0
2011-03	-	-	-	-	Update to Rel-10 version (MCC)	9.3.0	10.0.0
2012-09	SA#57	-	-	-	Update to Rel-11 version (MCC)	10.0.0	11.0.0
2012-09	SA#57	SP-120602	036	-	Removing erroneous e2ae indication	11.0.0	12.0.0
2012-09	SA#57	SP-120602	037	-	Correction of confidentiality on the Iq interface	11.0.0	12.0.0
2012-09	SA#57	SP-120609	038	2	Extending the scope and structure of TS 33.328 to accommodate IMS media security extensions	11.0.0	12.0.0
2012-09	SA#57	SP-120609	039	2	Mechanisms for e2ae media protection for MSRP	11.0.0	12.0.0
2012-12	SA#58	SP-120856	040	1	Corrections on e2ae security for RTP	12.0.0	12.1.0
2012-12	SA#58	SP-120861	041	1	Corrections on MSRP security based on SIP signalling security	12.0.0	12.1.0
2012-12	SA#58	SP-120861	042	1	Security for immediate messaging based on SIP signalling security	12.0.0	12.1.0
2012-12	SA#58	SP-120861	043	--	Security for conferencing based on SIP signalling security	12.0.0	12.1.0
2012-12	SA#58	SP-120861	044	1	Security for forking and re-targeting based on SIP signalling security	12.0.0	12.1.0
2012-12	SA#58	SP-120861	045	1	33328 CR R12 Recommended use of Wildcarded identity	12.0.0	12.1.0
2012-12	SA#58	SP-120861	046	1	33328 CR Inclusion of session based messaging in KMS based solution	12.0.0	12.1.0
2013-03	SA#59	SP-130040	047	1	Adding a reference for the BFCP	12.1.0	12.2.0
			048	1	Removing Editor's Notes on missing e2e security		
			049	1	Insertion of reference to RFC 6714 (MSRP CEMA)		
			050	1	KMS based solution for secure conferencing		
			051	1	IANA considerations for MIKEY-TICKET		
2013-06	SA#60	SP-130256	052	2	IMS end-to-access-edge security for MSRP media and compatibility with RCS	12.2.0	12.3.0
			053	1	Editorial modification to security for conferencing based on SIP signalling security		
2013-09	SA#61	SP-130406	054	1	KMS based solution for immediate messaging	12.3.0	12.4.0
		SP-130406	055	1	Secure UDPTL based T.38 fax		
2013-12	SA#62	SP-130666	056	1	Updated reference for secure fax	12.4.0	12.5.0
			057	2	Addition of TLS profile for eMediaSec		
2014-03	SA#63	SP-140023	058	1	Correction of an erroneous implementation of agreed CR in section 7.2.1	12.5.0	12.6.0
2014-06	SA#64	SP-140312	060	1	IMS media plane security interworking for WebRTC access to IMS	12.6.0	12.7.0
2014-09	SA#65	SP-140587	061	1	TLS profile - resolution of Editor's Notes	12.7.0	12.8.0
			062	-	Editorial correction of reference to non-existing Annex Y		
2016-01	SA#70				Upgrade to Rel-13 (MCC)	12.8.0	13.0.0

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2017-03	SA#75					Promotion to Release 14 without technical change	14.0.0
2018-06	-	-	-	-	-	Update to Rel-15 version (MCC)	15.0.0
2020-07	-	-	-	-	-	Update to Rel-16 version (MCC)	16.0.0
2021-03	SA#91e	SP-210251	0067	-	A	IETF references updates	16.1.0
2021-12	SA#94e	SP-211379	0068	1	B	Security updates for algorithms and protocols for 33.328	17.0.0
2022-03	SA#95e	SP-220210	0069	-	D	Editorial corrections to Annex F of IMS	17.1.0
2023-09	SA#101	SP-230898	0071	-	B	Security aspects of NG RTC	18.0.0
2023-12	SA#102	SP-231335	0072	-	F	Update UE terminating procedures for e2DCe	18.1.0
2023-12	SA#102	SP-231335	0073	-	F	Change of the abbreviation DCMF to MF and related changes to the text and figures	18.1.0
2023-12	SA#102	SP-231335	0074	-	F	Add the abbreviation IMS AS	18.1.0
2023-12	SA#102	SP-231335	0075	-	F	Remove DC Application Server in Figure N.3.4-1 and add a NOTE	18.1.0
2023-12	SA#102	SP-231335	0076	-	D	Editorial changes to clause 7.2.5	18.1.0
2023-12	SA#102	SP-231335	0077	-	F	Change the P-CSCF(IMS AS) to IMS AS via the P-CSCF	18.1.0
2024-09	SA#105	SP-241093	0079	1	F	Replacing DCMF with MF	18.2.0

History

Document history		
V18.1.0	May 2024	Publication
V18.2.0	October 2024	Publication