3GPP TS 33.328 V11.0.0 (2012-09)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
IP Multimedia Subsystem (IMS) media plane security
(Release 11)

Keywords
security, IP, Multimedia, SIP

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

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 based media which is 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 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 in this release of the TS is based on the well established protocol SRTP. Key management solutions for SRTP are defined in 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] IETF RFC 4566: "SDP: Session Description Protocol".

[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 ".

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].

e2ae	End-to-access edge
e2e	End-to-end
GW	Gateway
IMS-ALG	IMS Application Level Gateway
IMS UE	IMS User Equipment
KMS	Key Management Service
MIKEY	Multimedia Internet KEYing
NAF	Network Application Function
TEK	Traffic Encryption Key
TGK	TEK Generation Key

4 IMS media plane security overview

4.1 Introduction

4.1.1 General

IMS media plane security is composed of two more or less independent key management solutions. The first solution, SDES, is for e2ae and for e2e media protection. The solution relies on the security of the SIP infrastructure and in particular on SIP signalling security.

The second 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.

4.1.2 Solution overview

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 4566 [17] 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.

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.

4.2 IMS media plane security architecture

4.2.1 General

This clause describes the impact of IMS media plane security on the IMS architecture. Three cases need to be distinguished. The IMS UEs are impacted in all three 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).

There are two prerequisites on the network infrastructure for e2e media plane security between two terminals by means of SRTP to become possible:

a) Transcoding shall not take place in the media path;

b) Nodes in the media path shall be configured to forward SRTP packets transparently.

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 SDES, 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. 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 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.

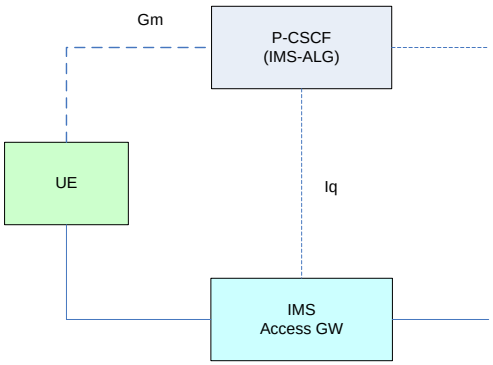

Figure 1: IMS signalling and media plane entities relevant to e2ae security

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.

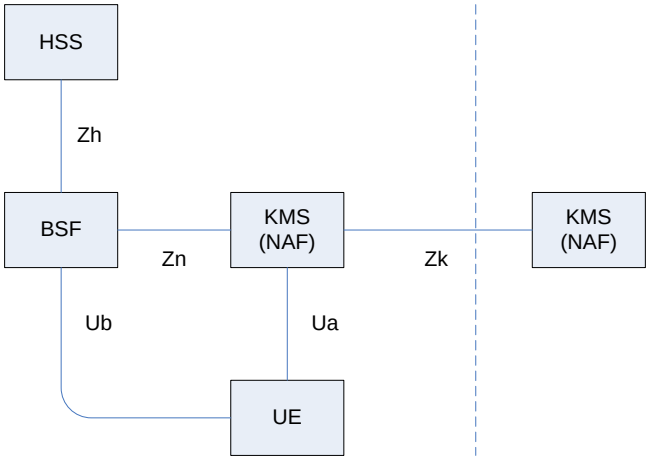

Figure 2: Reference model for key management for the KMS based solution

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.

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. An IMS UE may support SDES based media plane security mechanisms and/or KMS based media plane security mechanism. 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.

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 SDES based e2ae IMS media plane security.

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

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 SDES based e2ae IMS media plane security.

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

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 entirely relies 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.

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.

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.

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.

5.5 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 must 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.

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 provides 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).

6.2 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.

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 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 SDP Security Descriptions (SDES) as defined in [13].

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 (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.

6.2.1.3 Functional extension of the Iq interface for e2ae protection

For each session set-up, the P-CSCF (IMS-ALG) shall send the parameters contained in two specific 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 SDES crypto attribute selected by the P-CSCF (IMS-ALG) from the ones received from the IMS UE in the SDP Offer and the 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 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 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 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 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 Iq interface shall be protected by NDS/IP [5].

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." Note further that TS 33.210 [5] recommends encryption but does not mandate it, even over Za interface, but the confidentiality of the keys sent over the Iq interface is required. Encryption may need to be used to ensure this.

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 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.

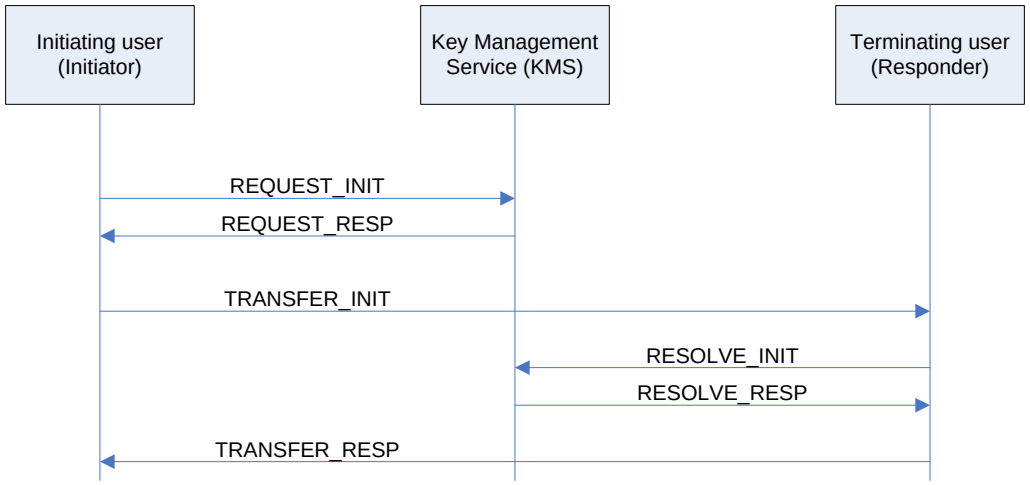

Figure 3: MIKEY-TICKET message exchanges

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 must 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.

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.

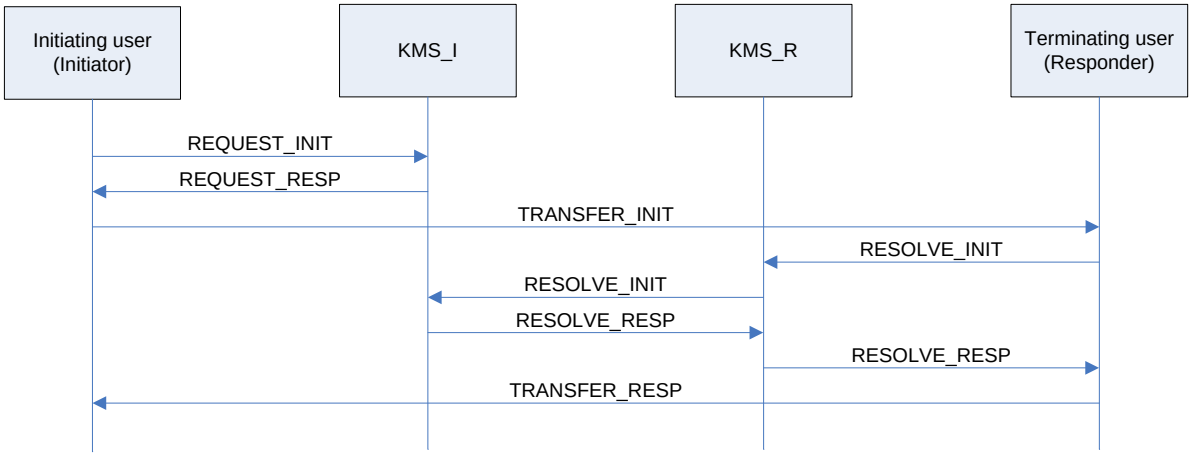

Figure 4: MIKEY-TICKET message exchanges between KMSs

7 Security association set-up procedures for media protection

7.1 IMS UE registration procedures

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.

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 call and both the IMS UE and the P-CSCF (IMS-ALG) have indicated support of e2ae security, 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, 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 call may contain a mixture of protected (e2ae and/or e2e) and unprotected media streams/sessions.

7.2 IMS UE originating procedures

7.2.1 IMS UE originating procedures for e2ae

Figure 5 shows the originating call set-up procedures for one RTP media stream 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.

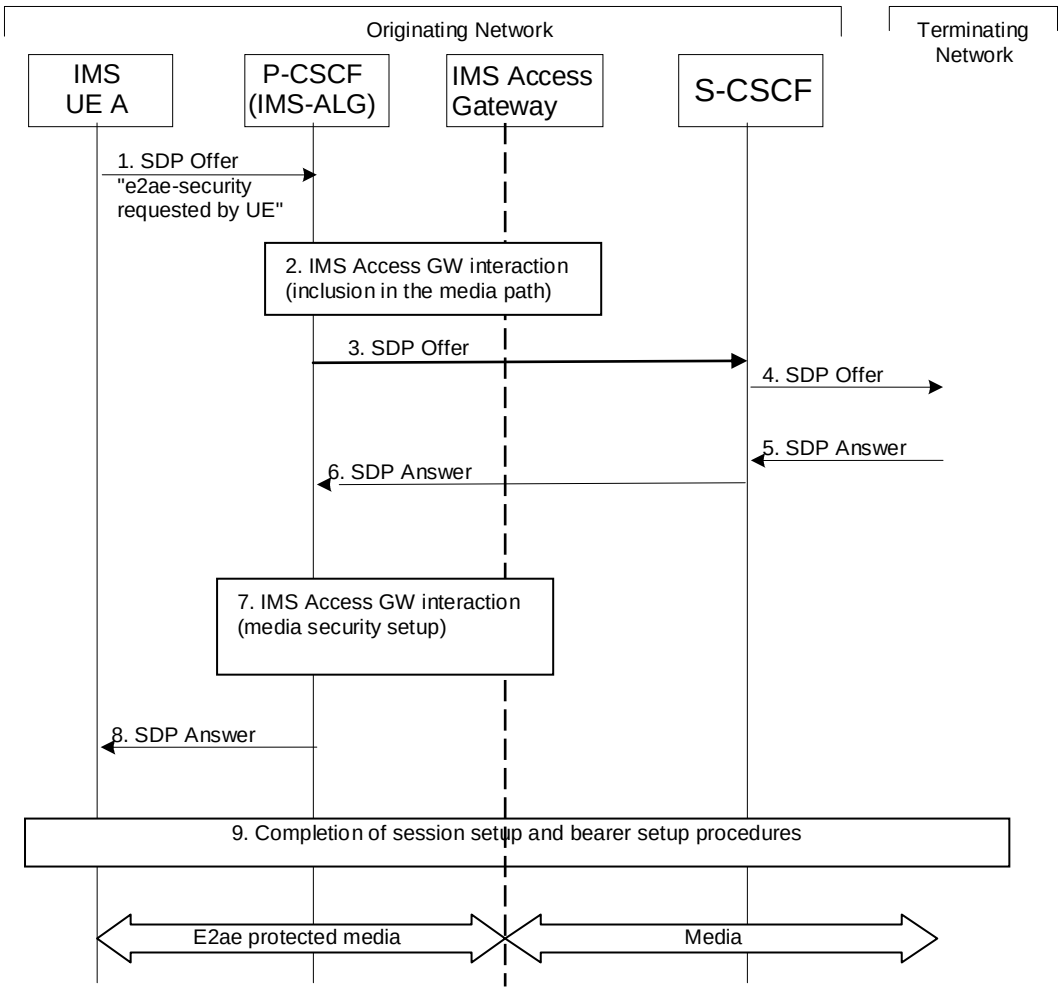

Figure 5: Originating call flow for e2ae case

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 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 prefers e2e-security for a RTP media stream. The originating procedures for establishing a RTP media streams with e2e-security are described in clauses 7.2.2 and 7.2.3 of this specification. The IMS UE may learn of a preference for e2e-security for a particular RTP 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 RTP media stream 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, together with an indication "e2ae-security requested by UE", to the P-CSCF (IMS-ALG). Each of these SDES crypto attributes contains 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.

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.

2. 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 during registration, the P-CSCF (IMS-ALG) allocates the required resources and includes the IMS Access GW in the media path. If the indication is not present the P-CSCF (IMS-ALG) proceeds as described in TS 23.228 [3].

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.

3. 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". 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) 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].

8. The P-CSCF (IMS-ALG) changes the transport from RTP to SRTP in the SDP Answer, includes the SDES crypto attribute created in step 7, and sends the SDP Answer to IMS UE A. The optional key lifetime field shall be omitted. 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. 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.

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

7.2.2 IMS UE originating procedures for e2e using SDES

Figure 6 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.

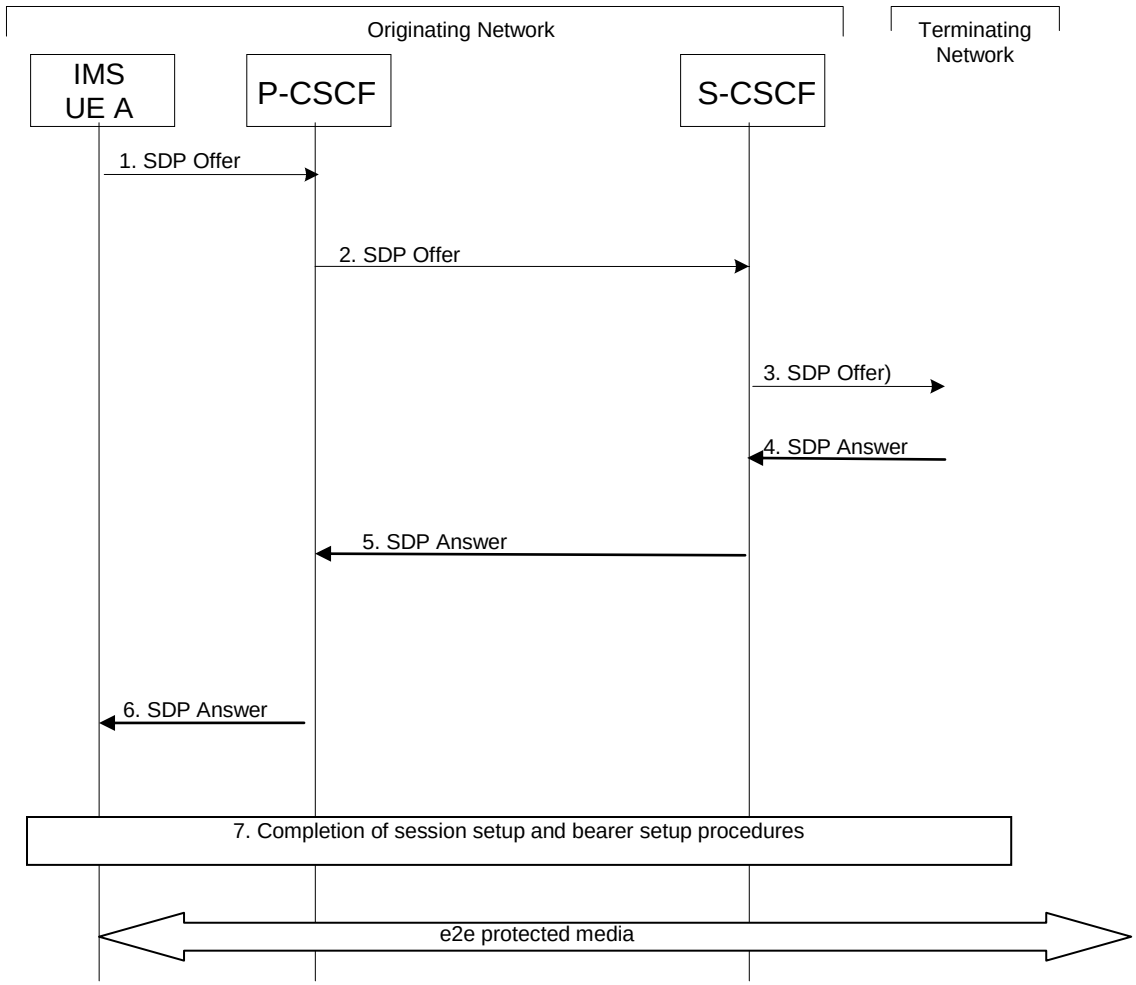

Figure 6: Originating call flow for e2e case using SDES

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 / encrypts 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 shows the originating call set-up procedures for one RTP media session/stream 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 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.

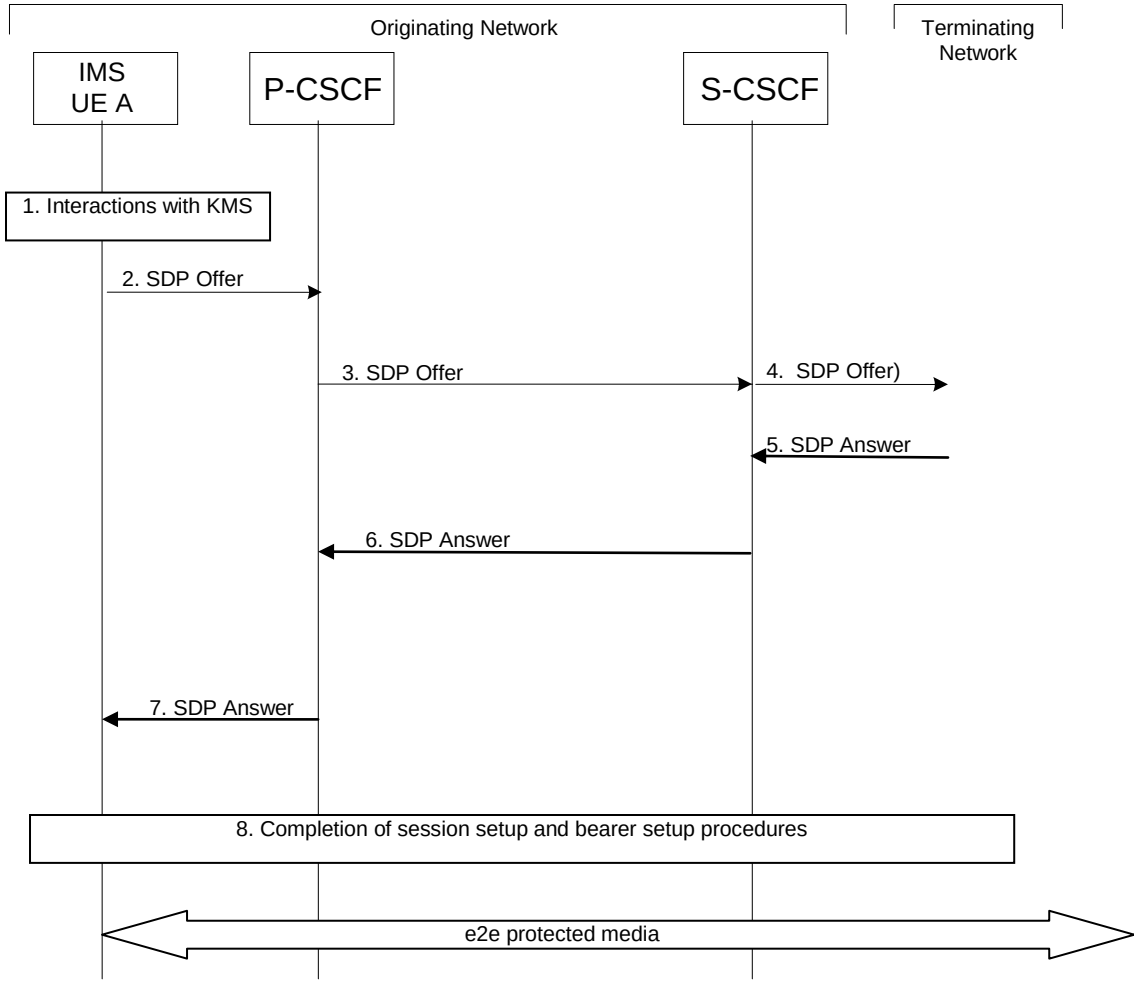

Figure 7: Originating call flow for e2e case using KMS

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 SRTP session/stream 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 completes the media security setup.

8. When the full session setup has been completed, and media can be sent, the protected media session/stream is sent between IMS UE A and IMS UE B. IMS UE A protects the media session/stream to and from IMS UE B using keys established using MIKEY-TICKET.

7.3 UE terminating procedures

7.3.1 UE terminating procedures for e2ae

Figure 8 shows the terminating call set-up procedures for one RTP 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.

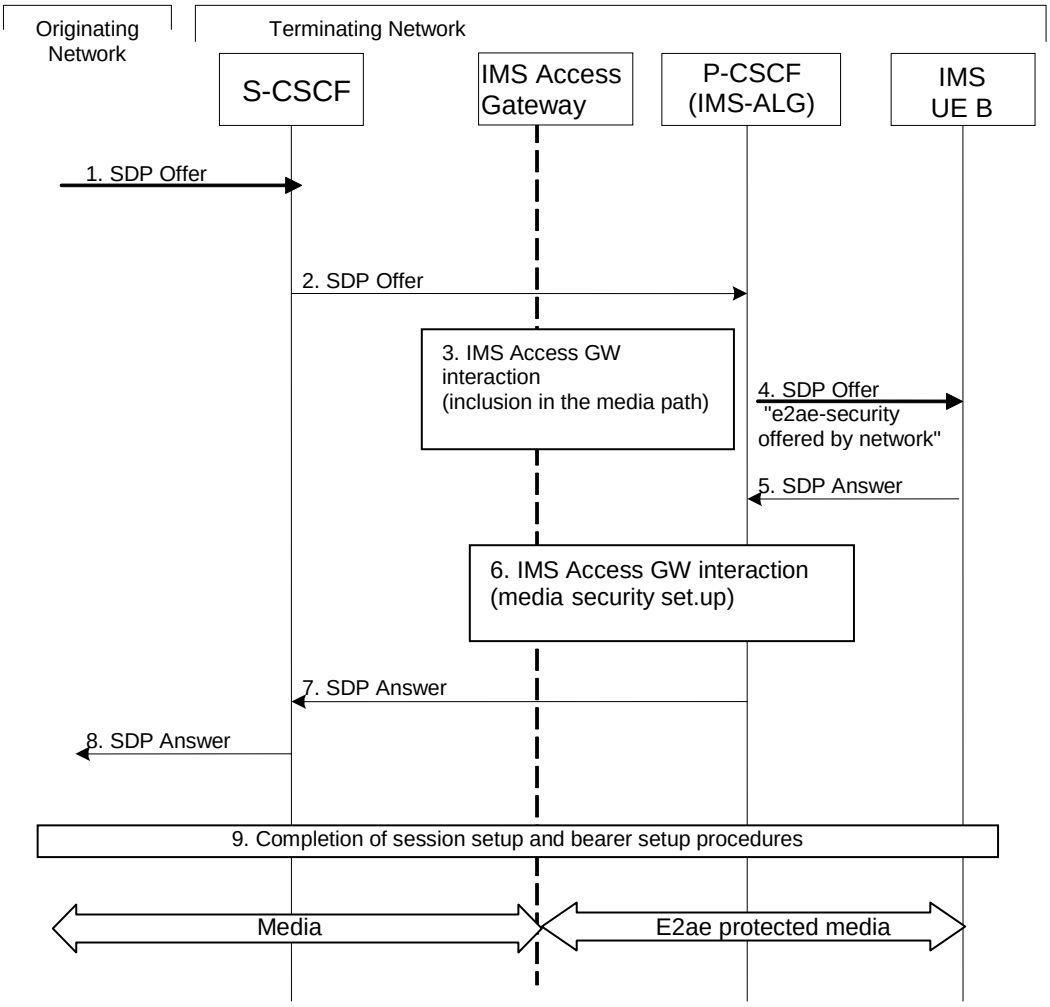

Figure 8: Terminating call flow for e2ae case

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 during registration and the P-CSCF (IMS-ALG) receives an SDP Offer for an RTP media stream from the S-CSCF, then the P-CSCF (IMS-ALG) shall establish e2ae-security as described in this clause.

NOTE 2: The P-CSCF (IMS-ALG) will not establish e2ae security if the SDP offer received from the S-CSCF indicates that e2e security is being offered (i.e. the offer is for an SRTP stream), 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 from the originating network.

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

3. The P-CSCF (IMS-ALG) checks whether both the IMS UE and the P-CSCF (IMS-ALG) indicated support of e2ae-security during registration. If this is the case the P-CSCF (IMS-ALG) proceeds as described in this clause and allocates the required resources and includes the IMS Access GW in the media path. If this is not the case the P-CSCF (IMS-ALG) continues as described for a call without IMS media plane security.

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) 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, and sends it to IMS UE B. 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.

5. 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 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.

6. The P-CSCF (IMS-ALG) communicates 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 IMS Access GW. 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].

7. The P-CSCF (IMS-ALG) changes the transport from SRTP to RTP in the SDP Answer, removes the SDES crypto attribute, and then sends the SDP Answer to the S-CSCF.

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

9. 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.

7.3.2 IMS UE terminating procedures for e2e using SDES

Figure 9 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.

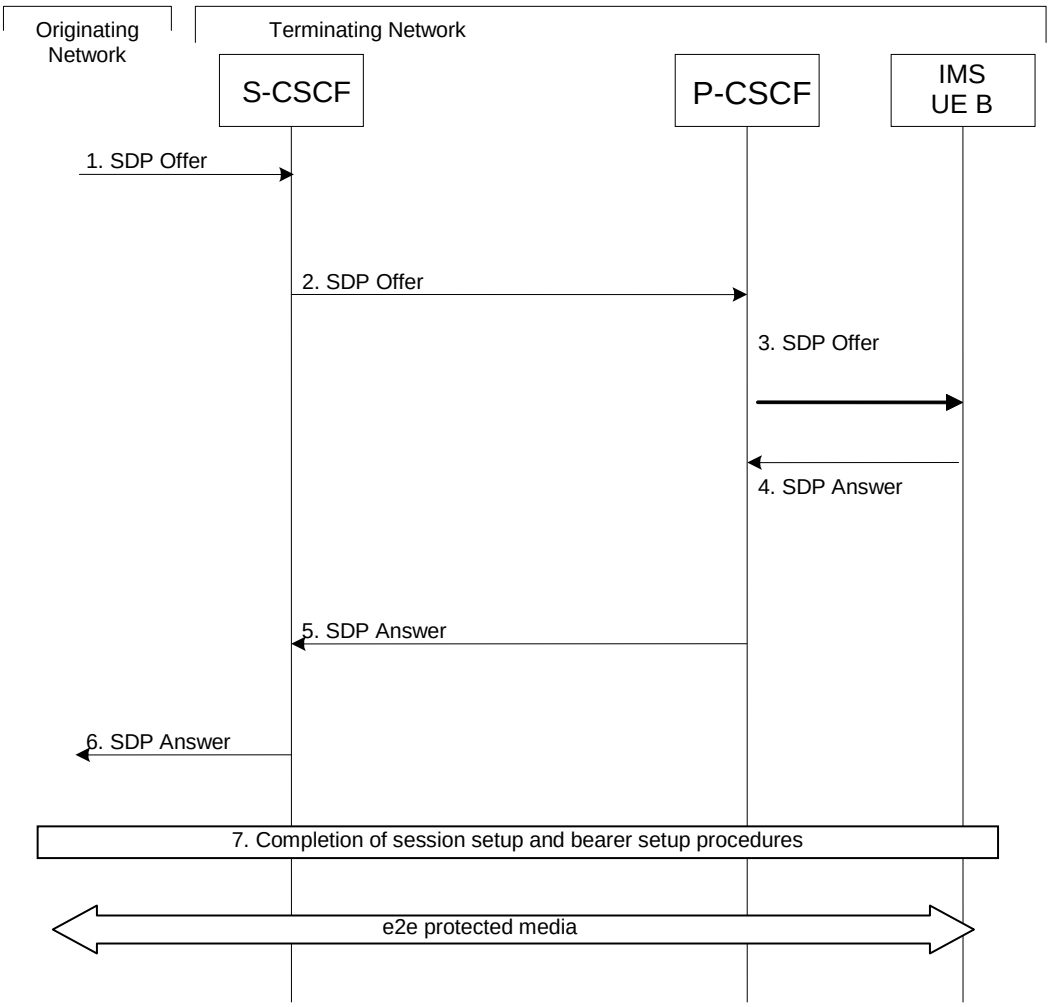

Figure 9: Terminating call flow for e2e case using SDES

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 10 shows the terminating call set-up procedures for one RTP media session/stream 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 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.

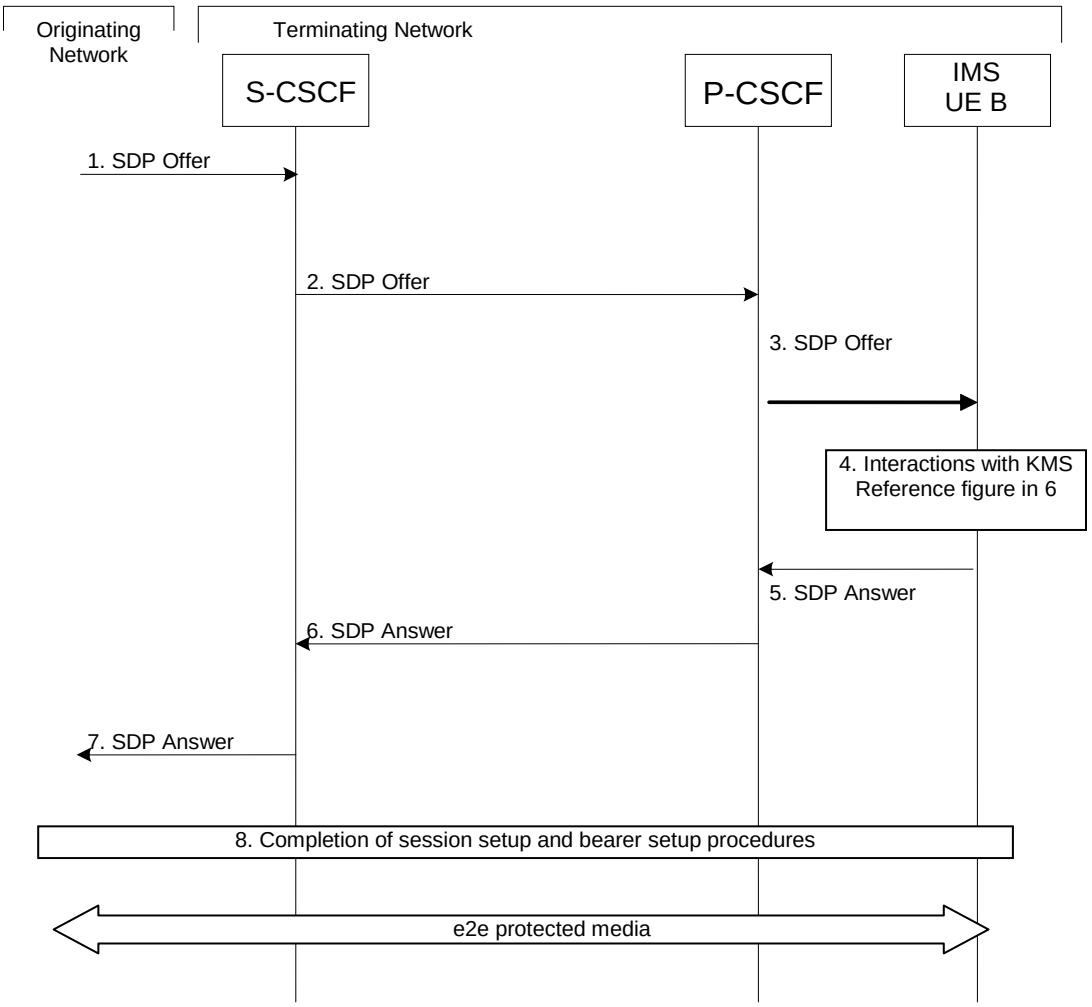

Figure 10: Terminating call flow for e2e case using KMS

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 SRTP media session/stream containing a MIKEY-TICKET offer.

2. The S-CSCF performs the required procedures according to TS 23.228 [3] and forwards the SDP offer for the SRTP media session/stream to the P-CSCF.
3. The P-CSCF forwards the SDP offer for the SRTP media session/stream to IMS UE B.
4. 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 SRTP media session/stream, 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.
8. When the full session setup has been completed, and media can be sent, the protected media session/streams are sent between IMS UE A and IMS UE B. IMS UE B protects the media session/streams to and from IMS A using keys established using MIKEY-TICKET.

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.

    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.

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.

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)" [RFC 4771] 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 PRFs MIKEY-1 and PRF-HMAC-SHA-256 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-1-160 and HMAC-SHA-256-256 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: must specify (IDRr), i.e. the intended recipients of the requested ticket. IDRapp shall be set to SRTP.
- 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-1-160 and HMAC-SHA-256-256 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 (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