3GPP TR 33.829 V2.0.0 (2013-03)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Extended IP Multimedia Subsystem (IMS) media plane security features (Release 12)

Keywords
IMS, SIP, Security

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 Report 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

Rel-9 MEDIASEC work resulted in the specification of solutions for media protection over the access network (e2m) and peer-to-peer (e2e) TS 33.328 [3]. For the peer-to-peer (e2e) media plane security, two solutions were standardized

- A media security solution to satisfy major user categories.
- A media security solution providing high quality end-to-end media security for important user groups like enterprises, National Security and Public Safety (NSPS) organizations and different government authorities.

However, the solutions do not cope with a number of requirements and relevant use cases of which many are discussed in TR 33.828 [2]. Solutions for use cases like conference (group) calls, protection of non-RTP media, deferred delivery, video/media on demand, AS-terminated media security and transcoder functionality described in TR 33.828 [2] and some widely used use cases like recording of protected media, communication diversion, and single radio voice call continuity (SRVCC) have not been addressed. It is therefore desirable to continue to study and develop solutions for these use cases and to evaluate which normative standardization work that is needed.

1 Scope

The present document details relevant use cases/services for different user groups and corresponding solutions for IMS media plane security which are not covered by TS 33.328 [3]. The corresponding requirements in the Rel-9 study documented in TR 33.828 [2] will be used as a basis. The covered use cases/services are: conference calls, protection of non-RTP media, early media, communication diversion, deferred delivery, protected media recording, video on demand, AS-terminated media security, transcoder functionality and SRVCC. Example user groups are enterprises, National Security and Public Safety (NSPS) organizations, different government authorities, and general public.

Editor's Note: The list of covered use cases/services shall be updated when the study is finalized.

Editor's Note: It is for further study whether protection of early media is possible in IMS.

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 TR 33.828: "IP Multimedia Subsystem (IMS) media plane security".

[3] 3GPP TS 33.328: "IP Multimedia Subsystem (IMS) media plane security".

[4] 3GPP TS 24.147: "Conferencing using the IP Multimedia (IM), Core Network (CN) subsystem".

[5] IETF RFC 4583: "Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams".

[6] 3GPP TS 24.605: "Conference (CONF) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification".

[7] 3GPP TS 23.216: "Single Radio Voice Call Continuity (SRVCC); Stage 2".

[8] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[9] 3GPP TS 24.247: "Messaging service using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".

[10] 3GPP TS 29.311: "Service level interworking for Messaging Services".

[11] 3GPP TS 24.604: "Communication Diversion (CDIV) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification ".

[12] IETF RFC 3428: "Session Initiation Protocol (SIP) Extension for Instant Messaging".

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

[14] IETF Internet-Draft draft-ietf-simple-msrp-sessmatch-08: "Session Matching Update for the Message Session Relay Protocol (MSRP)". (work in progress)

[15] IETF RFC 6135: "An Alternative Connection Model for the Message Session Relay Protocol (MSRP)".

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

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

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

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

[20] IETF RFC 5751: "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification".

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

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

[23] IETF RFC 4566: "SDP: Session Description Protocol".

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

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

[26] 3GPP TS 24.608: "Terminating Identification Presentation(TIP) and Terminating Identification Restriction (TIR) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification".

[27] IETF RFC 3264: "An Offer/Answer Model with the Session Description Protocol (SDP)".

[28] IETF RFC 6267: "MIKEY-IBAKE: Identity-Based Authenticated Key Exchange (IBAKE) Mode of Key Distribution in Multimedia Internet KEYing (MIKEY) ".

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

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

[31] IETF RFC 3711: "The Secure Real-Time Transport Protocol".

[32] GSM Association: “Rich Communication Suite 5.0 Advanced Communications, Services and Client Specification”, Version 1.0, 19 April 2012

[33] ITU-T recommendation T.38: "Procedures for real-time Group 3 facsimile communication over IP networks".

[34] 3GPP TS 26.114: "IP Multimedia Subsystem (IMS); Multimedia telephony; Media handling and interaction".

[35] IETF RFC 4572: "Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP) ".

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

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

3 Definitions, symbols and abbreviations

Delete from the above heading those words which are not applicable.

Clause numbering depends on applicability and should be renumbered accordingly.

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].

Key Escrow: A key recovery technique for storing knowledge of a cryptographic key or parts thereof in the custody of a third party, so that the key can be recovered and used in specified circumstances. Key escrow can further be characterized as active or passive according to the way the knowledge of the key is obtained. In that sense, active key escrow actively participates and affects the generation of the cryptographic key, while passive key escrow learns of the cryptographic key and does not affect the generation of cryptographic key.

Perfect Forward Secrecy: For a key agreement protocol, the property that compromising long-term keying material does not compromise session keys that were previously established using the long-term material.

3.2 Symbols

For the purposes of the present document, the following symbols apply:

Symbol format (EW)

<symbol> <Explanation>

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].

Abbreviation format (EW)

<ACRONYM> <Explanation>

4 Overview

5 IMS conferencing

5.1 Introduction

5.1.1 General

An overview of the IMS conferencing service is given in TS 24.147 [4]. The conferencing service provides the means for a user to create, manage, terminate, join and leave conferences. The conference system also can provide information (notifications) about conference events to the conference users. Conference users SUBSCRIBE to the information.

Conferencing applies to any kind of media stream by which users may want to communicate, including audio and video media streams as well as instant message based conferences and gaming. It is optional to support floor control. Floor control is implemented using BFCP (The Binary Floor Control Protocol) [5]. BFCP transport is TCP.

The conferencing service is implemented in an AS together with an MRFC and a MRFP. The functional split and the interfaces between these entities are depicted in Figure 5.1.1-1 (copy of Figure 4.1 in TS 24.147 [4])

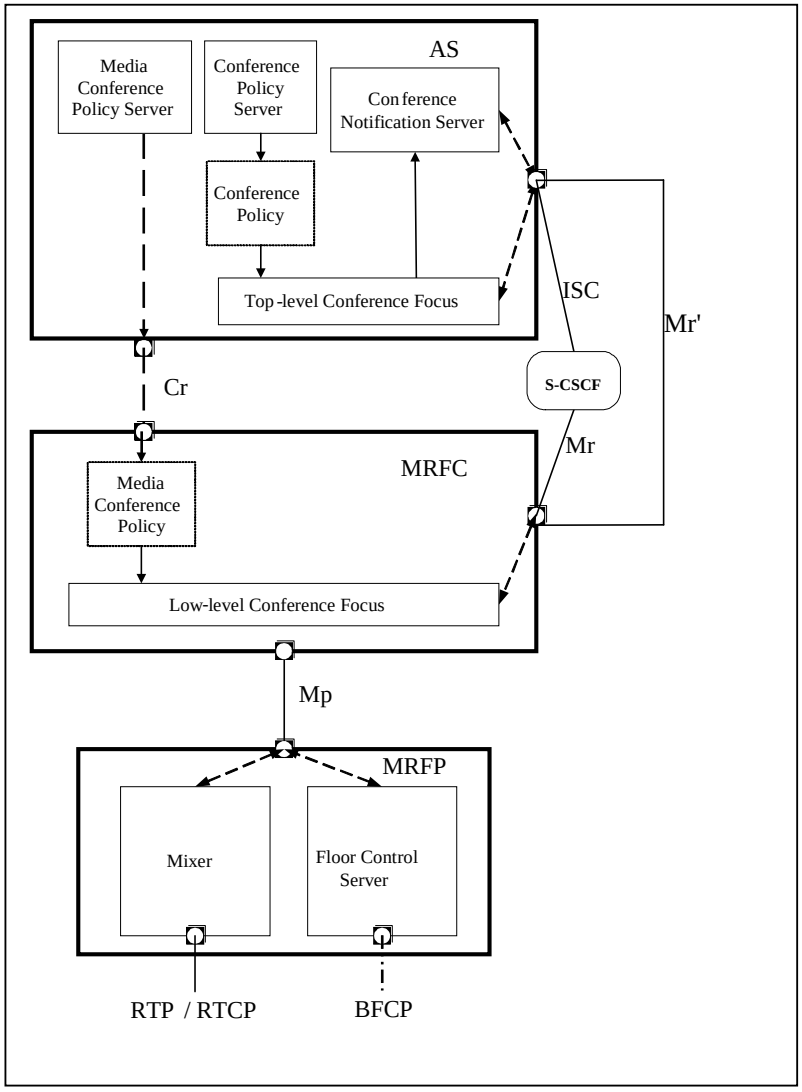


Figure 5.1.1-1: Functional split between the AS, MRFC and MRFP

The Focus (see Figure 5.1.1-1) in a conference solution is a SIP user agent that is addressed by a conference URI and identifies a conference. The focus maintains a SIP signalling relationship with each participant in the conference. The focus is responsible for ensuring, in some way, that each participant receives the media that make up the conference. The focus also implements conference policies. The focus is a logical role.

Figure 5.1.1-1 indicates that the network operator or the user may apply membership and media policies to a conference. Policy control mechanisms are currently not standardized.

In IMS, only ad hoc conferencing is specified. Ad hoc conferences are, as their name implies, instantiated on the fly by a user. Planned, pre-established conferences, often use non-IMS means to create the conference.

The protocol used for the Mr and Mr' reference points is SIP. The Cr reference point allows interaction between an Application Server and an MRFC for media control and session control. The Mp reference point allows an MRFC to control media stream resources provided by an MRFP.

5.1.2 Immediate security observations/requirements

To secure an IMS conference the following should be considered:

- **Key management.** The natural place to perform key management is in the MRFC. This means that media plane keys have to be transported from the MRFC to the MRFP over Mp, and that Mp should be protected. Other sensitive information (e.g. conference policies) may be transferred from AS to MRFC over Cr. The need for

protection of SIP signalling over Mr' (or ICS – Mr) has to be evaluated. The required protection of the interfaces may be different for different key management solutions.

- **Rekeying.** If a group key is used to protect media in a conference then it may be required to perform rekeying when a participant joins or leaves the conference; this to guarantee forward and backward security. The cost to do such rekeying may be high and it should be evaluated if and how such a service can be included in the secure conference service. The evaluation needs to be made per type of conference keying as the cost, complexity and relevance may differ between different solutions. One issue might be how to handle the beginning/end of a conference, where users join/leave frequently.

- **Mixer**. Requirements may differ depending on type of mixer. In use cases when the mixer performs switching of the media rather then mixing, it may not be necessary to decrypt and re-encrypt the media in the mixer, but normally incoming media to the mixer has to be deciphered and the mixed output signal enciphered before it is sent out.

  In conference scenarios where the conference system sends a common media stream to all or many conference participants, it would from an efficiency point of view be favourable to encrypt the common media streams based on group keys available to all recipients. A typical example of a conferencing situation when this would be applicable is in a voice conference where all listeners receive the same mixed media stream from the conference centre. On the other hand, in other conference scenarios it might be so that e.g. an outgoing video stream is uniquely composed per end-point and adapted to the receiving ends capabilities. However, to support both cases described, key management solutions for secure conferencing should be specified for establishment and use of both end-point unique and group keys.

-- **Event packages.** Conference event packages may carry security sensitive information and should thus be protected. This is explained in the security considerations chapter of RFC 4575 [17]. This means that NOTIFY messages carrying these event packages have to be protected when the trust model for the chosen key management solution requires it.

- **Floor control.** Floor control messages may disclose information which is sensitive about who is speaking and may thus have to be protected. As BFCP is transported over TCP, securing TCP is similar to securing MSRP.

- **Conference server "internal" interfaces.** The existing conference solution "internal" interfaces are ICS – Mr, Mr', Cr and Mp, see Figure 5.1.1-1 above. These interfaces provide the required functionality to implement a secure conference solution.

  If and when protection of these interfaces is required, NDS/IP can be used. If e2e protection between AS and MRFC is required, the Mr' interface should be used.

- **Authentication of participating users and conference service.** In some applications it may be essential that conference participants can authenticate the conference service and vice versa. In this way conference participants get assurance that they have been connected to a legitimate service. It may also be essential that the conference participants are securely informed about the other participants' identities.

5.1.3 Requirements

Editor's note: Requirements may be missing.

The following are general requirements on a secure conference solution are:

- A user shall be able to initiate creation of an ad hoc secure conference.
  .
  In other words, there shall be some means for an ad hoc conference creator to signal that the conference should be secure.

- Each conference participant shall be able to mutually authenticate with the conference centre.

  - All participants in a secure conference shall use media protection.

Editor's note: Conferences where some media/participant isn't secured could be possibly studied later.

- Different media streams shall use different key streams.

NOTE: This is to make sure that no two-time pads occur.

- It should be possible as an implementation option to use group keys to protect media streams intended for all participants.

  An example use case when this could be beneficial is when a mixed output stream is intended for all participants.

- Rekeying of a conference should be possible.

  Rekeying of a conference in the context of this document means that all shared key streams in the conference shall be based on new, fresh key material. Rekeying may occur when a participant joins or leaves a conference.

- A secure conference supporting conference event packages shall provide security for these event packages.

  Event packages may carry security critical information.

- A secure conference supporting floor control shall provide security for the floor control signalling.

  Floor control signalling could carry security critical information.

5.2 Use cases

5.2.1 Ad hoc conferencing

5.2.1.1 Main events

This clause gives a high level description of the main events in a creating and running an ad hoc conference. For a detailed and complete description see TS 24.605 [6] and TS 24.147 [4].

An ad-hoc conference is an unscheduled conference that is created on-the-fly by a user.

A user creates a conference by sending an INVITE with the request URI being a "conference factory URI". In a response the user gets a conference URI addressing the created conference. The INVITE creating the conference may contain a list of users which the conference focus shall invite as participants in the conference.

If a conference URI has been made available to users in some unspecified way, a conference may also be created on the fly when the first user calls the conference URI.

A user may join a conference by sending an INVITE with the request URI being the conference URI.

A user may subscribe to the conference event package (notifications on users joining /leaving the conference etc)

A conference participant can invite other users to the conference by:

a) Inviting a user to a conference by sending a REFER request to the user directly; or

b) Inviting a user to a conference by sending a REFER request to the conference focus.

A conference participant may leave the conference by sending a BYE to the conference focus. The conference focus may drop a participant by sending a BYE. A conference participant may request that another conference participant is removed from the conference by sending a REFER to the conference focus with a Refer-To header having the "method" parameter set to "BYE". Normally, when the user that created the conference (the conference owner) leaves the conference, the conference is closed and the conference focus sends BYE to all participants.

When the last conference participant leaves the conference the media plane resources are released.

5.2.1.2 Three party conferencing

A three party conference is an ad hoc conference with some extra features. One user initiates sessions with two other users and then joins them in a conference. The initiating user first puts both his sessions on hold, creates the conference, and then invites the users to join the conference by sending REFER requests to the users to join the conference. In some implementations the originator of the conference can toggle between the conferencing and peer-to-peer sessions.

5.2.2 Planned conferences

Planned conferences are not explicitly standardized. Therefore, they are out of scope of this document. Nevertheless, the key management solutions specified may support planned conferences.

5.3 Solution(s)

5.3.1 General

5.3.1.1 Policies for secure conferences

Whether a conference to be created is secure, or more exactly, the security properties required for a conference, can be considered to be part of the conference policies. In the following, examples of security related policies are given:

a) Only a specified set of users is allowed to the conference. This may be implemented in different ways. For example, it could be a "dial-out-only" conference, where the conference focus invites the specified users. In this case, if the focus gets no information about the identity of the terminating side, the focus must cancel the INVITE, as CDIV (see clause 9) may have happened, and the call may have been diverted to a user not belonging to the set of allowed users. In CDIV cases where the focus is informed about the identity of the terminating side, the focus must cancel the INVITE if the terminating id is not in the set of allowed users. If dial-in is allowed, the focus must reject all INVITEs that do not reveal the identity of the originating side (focus should send 433 "Anonymity disallowed") or reject all INVITEs by users not specified as allowed users.

b) Only secured media streams are used in the conference. When dialing out, the conference server offers secured media streams only, and when a user dials in, the conference server rejects any media streams that are not secured.

c) Group keys are used for certain media streams, and are renewed in case of certain events, e.g. each time a user joins or leaves the conference. For renewal of group keys, the conference focus may re-invite the participants, or may ask them via a REFER request to send a re-invite to the focus.

d) Group keys are not used; instead, the focus protects each media stream for each participant individually, thus ensuring that a participant cannot decrypt streams sent to other participants.

The examples (3) and (4) show two different approaches for ensuring that a participant who joins a conference after its beginning is not able to decrypt the media sent before he joined, and that a participant who left a conference is not able to decrypt the media sent after he left. Note that there may also be conferences where this is not required.

Note that policy control for conferences is currently not specified, so proprietary methods may be used by which users or network operators specify such security policies for conferences.

5.3.1.2 Group keys versus bilateral keys

Media sessions in ad hoc conferences are established using the SDP offer/answer model [27]. This means that the participants receive the media streams of the focus on individual IP addresses and ports. Multicast is thus only possible above the UDP/IP level, i.e. a common RTP session may be used. Using a common RTP session means the focus can send the same SRTP PDUs to all participants. This requires the usage of a group key for the media the focus distributes in this way. If the focus sends different PDUs to different participants, these different PDUs are encrypted individually, but still group keys can be used.

Alternatively, the focus may use separate RTP sessions for the different participants, even for common media. This allows full flexibility when choosing SSRC ids or the initial RTP sequence numbers. Each stream must be protected individually in this case, using a bilateral key, i.e. a key known only to the both sides.

The usage of group keys has certain security issues cf clause 5.3.1. This may require rekeying each time a participant joins or leaves the conference. The advantage of avoiding the complexity for rekeying when using bilateral keying has to be weighed against the performance gain when using group keys. The use of group keys reduces the number of keys to be stored. The result of the trade-off will depend on the envisaged use cases, which is why not both solutions are required to be always supported.

5.3.2 SDES-based solution

5.3.2.1 Discussion

When participating in a conference, a user may use e2ae security. This is not visible to the conference server and for the other participants in a conference. The remainder of this clause relates to media security applied between a conference participant and a conference server.

The SDES-based solution for e2e media plane security described in TS 33.328 [3] is applicable to the communication between a conference participant and the conference server, i.e. with the participant and the conference server as the two endpoints.

According to the use cases described above, the establishment of the conference includes INVITE dialogues between participants and the conference server. By these dialogues, SDP is exchanged in the bodies of SIP messages that describe the media flows between the participants and the conference server. In the SDES-based solution, crypto attributes as part of the SDP are used as described in [3] to exchange keys and other cryptographic parameters between the participants and the conference server.

With SDES, the sender of a media stream specifies the key used to protect this stream. This facilitates the usage of bilateral keys as well as of group keys.

The use of bilateral keys with SDES is straightforward and practically feasible. Their use is recommended as a rule. The use of group keys has advantages in certain situations, but also faces some issues as discussed further below. The remainder of this subclause deals with the use of group keys.

The consideration of group keys is motivated by the fact that, if the conference server distributes an identical media stream to multiple participants, the conference server may use a group key, meaning that encryption has to be performed only once and the same encrypted stream can be sent to these multiple participants. In this case, the conference server will specify the same crypto attribute in all dialogues used to set up this stream from the conference server to the participants.

For unicast media streams from participants to the conference server, usage of group keys does not allow for significant efficiency gain. In the SDES-based solution, each participant specifies an arbitrary key for such a media stream, and the conference server uses these individual keys for the individual streams it receives from individual conference participants.

If group keys are used, and at the same time the conference policies require that a participant can only decrypt the media stream of the focus during the time the participant is within the conference, the group keys must be changed each time a user joins or leaves. In case a participant leaves, the focus only needs to issue a re-INVITE to all remaining participants, specifying a new SDP offer with a modified SDES crypto attribute specifying one or more new keys. The participants may specify new keys for the streams they send in their SDP answers; they may also choose to specify the old keys again, which may result in a more seamless processing of the arriving media at the focus. In case a participant joins, in this solution the SRTP crypto contexts need to be re-initialized, in order to reset the SRTP roll over counter (ROC) to zero. This can be achieved by the focus specifying the common media stream(s) it sends to the participants as new streams, using the means described in RFC 3264. I.e., the focus will delete the existing streams in the new SDP (by setting the port number to zero) and offer new streams in the new SDP. In their answers, the participants should specify new (receive) ports for the common streams in order to allow them to distinguish conveniently between media encrypted with an old key and media encrypted with a new key.

NOTE 1: The practice of sending an SDP changing the audio session to port 0 and adding another media stream in the dialogue may have deployment issues. Moreover, there may be other possibilities to trigger a reset of SRTP crypto contexts. An alternative to resetting the crypto contexts may also be to use the ciphersuites specified in RFC 4771 [29] (see NOTE 3 below) and do only rekeying. A final decision on the method to be used is left to the normative stage.

As the ROC is not transmitted in SDES, the SDES solution would require re-initialization of crypto contexts of all participants each time a participant joins, if group keys are used (even if the conference policies would allow to continue using the current group key).

NOTE 2: A mere rekeying (i.e. switching to another SRTP master key) does not reset the ROC to zero, as stated explicitly by RFC 3711, section 3.3.1.

NOTE 3: RFC4771 [29] specifies ciphersuites that allow transmitting the ROC in RTP packets. However, RFC 4568 (SDES) defines a fixed set of ciphersuites that can be specified in the SDES crypto attribute, and this set does not comprise any of the ROC-carrying ciphersuites of RFC4771. So formally, these ciphersuites cannot be used with SDES.

Frequent re-initialization of crypto contexts can be avoided, if the focus takes care that the RTP sequence number never "rolls over", meaning the ROC is always equal to zero. This can be achieved if the focus is able to re-initialize crypto contexts before the ROC would roll over, cf. NOTE1. If the sequence number for RTP packets sent by the focus starts at a random number, the remaining time until roll over and re-initialization of the crypto context will be uniformly distributed over an interval of more than 20 minutes, i.e. it will be more than 10 minutes on average, for a voice stream with one packet per 20 ms.

NOTE 4: Randomness of the sequence number is specified as a "SHOULD-requirement" in RFC 3550 (RTP) [30] in order to support an encryption scheme specified in the same RFC, section 9.1. The RFC suggests that this mechanism may be weak, and other mechanisms may be used rather. De facto, this scheme is now obsoleted by the specification of SRTP, as used for IMS media plane security for RTP traffic. SRTP requires randomness for keys and salts, but not for the RTP sequence number. Nevertheless, choosing the initial sequence number randomly seems widely implemented, so this behaviour has to be taken into account. On the other hand, only the implementation of the focus would be affected.

If the sequence number for RTP packets sent by the focus started with zero, it would take more than 20 minutes for the sequence counter to roll over with the described voice stream. So, a focus could start with a sequence number of zero and trigger a re-initialization e.g. every 15 minutes. Participants may then join without re-initialization of the crypto context.

Because key management for the IMS media plane is done out of band, i.e. in the signalling plane, rekeying as well as re-initialization of crypto contexts may not operate seamlessly, i.e. it may result in short disturbance of the audio or video information rendered to a user depending on the implementation. Moreover, rekeying or crypto context re-initialization with a high frequency, e.g. when many users join or leave a conference in a short time interval, may cause a very high signalling load, and may exacerbate audio/video disturbance. (This observation is not specific to the SDES method.)

To avoid such issues, it is recommended to use bilateral keys with the SDES-based solution as a rule. Group keys may be used in scenarios where

the performance gain has high importance (e.g. the conference focus is not capable of handling the conference at all with bilateral keying)

AND [the conference policies do not mandate rekeying each time participants join or leave the conference

OR the focus is capable to handle rekeying/re-initialization of crypto contexts at the expected rate of joins/leaves].

When group keys are used, the conference focus may trigger a crypto context re-initialization before the RTP sequence number rolls over, thus ensuring that the ROC is always equal to zero, as described above. This allows that only rekeying but not crypto context re-initialization is done when users join. It also allows that users join without rekeying, if the conference policies allow that.

In this solution, conference server and participants rely on SIP signalling with respect to information about the identity of a communication peer, i.e. they rely on the P-Asserted-Identity. If the security policies comprise mutual authentication, participants and conference server must not suppress the delivery of the P-Asserted-Identity to the remote communication endpoint.

The SDES-based solution for conferencing inherits the security prerequisites and properties of the SDES-based solution for e2e media security. It requires trust in the conference server not to abuse the media. (For conferences where the conference server needs access to cleartext media, e.g. for mixing, this is an inherent requirement for all possible solutions.)

For this solution, integrity and confidentiality of SIP signalling are a prerequisite. This means at the same time that traffic that is part of any event packages associated to a conference, like NOTIFY messages, is protected.

SDES applies only for SRTP/SRTCP. A conference solution may also comprise floor control using BFCP which is transported over TCP. In this solution, BFCP is secured using TLS confidentiality and integrity protection.

Ciphersuites and session keys to protect BFCP are negotiated via the TLS handshake. The TLS record protocol secures the actual BFCP messages. Mutual authentication during the TLS handshake may be achieved via different means:

a) Usage of self-signed certificates, with the certificate fingerprints being transmitted using the SDP fingerprint attribute in the SDP offer-answer exchange.

   This approach is specified in RFC 4582. "TCP/TLS/BFCP" is used as the protocol identifier in the "m=" line of the SDP, and the "a=fingerprint" attribute is used to provide the fingerprint of the self-signed certificate.

b) Usage of PSK TLS.

   In this case, a PSK must be established between the two parties. Assuming that SIP signalling is integrity and confidentiality protected, and that any SIP proxies between the endpoints of the TLS connection to be established are trusted, a PSK may be selected by one peer and be transmitted within the SDP to the other peer. RFC 4566 specifies a "k=" line that may be used to transmit an encryption key, but does not recommend its usage, as – different from the scenario considered here – it does not assume sufficient SIP signalling security. Alternatively, the "key-mgmt" attribute specified in RFC 4567 may be enhanced for this purpose, or an additional attribute may be specified (like it was done in RFC 4568 [25] (SDES) for transmitting a key to secure RTP based communication).

   In this approach, the PSK will be protected during transport, but will be accessible by core network elements. It is assumed that this, like the SDES-based solution in TS 33.328, satisfies the security needs of major user categories.

NOTE: When using self-signed certificates or the "k=" line option for the PSK case then no further work in the IETF is expected to be required. For the other two options above for establishing the PSK, additional work in the IETF would be required. This needs to be taken into account when going to the normative stage. The decision whether more than one of the above options for TLS key management is to be mandated by 3GPP is left to the normative stage.

This solution for securing BFCP is very similar to a proposed solution for securing session based messaging. See clause 8.3.2.2 and 8.3.2.3 for a more detailed description and discussion of the solution.

5.3.2.2 Recommended Solution

When participating in conferences, IMS UEs may use e2ae security for RTP based traffic as specified in TS 33.328, and security for MSRP leveraging IMS control plane security, as specified in section 8.3.2.4.

For BFCP that may be used in conferences, security shall be supported analogously to security for session based messaging using MSRP and leveraging IMS control plane security. A dedicated indication for the support of TLS for BFCP during registration is used to allow indicating support for TLS for MSRP and support for TLS for BFCP independently.

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

The conference server may support e2e security for RTP based media between IMS UE and conference server as specified in TS 33.328 for the e2e security solution using SDES. To use this type of security, IMS UE and conference server specify usage of SRTP transport and the SDES crypto attribute for the respective media streams within the SDP offers and answers (as specified in TS 33.328). Usage of this type of security, i.e. accepting it when offered in incoming SDP offers (dial-in case) and offering it in outgoing SDP offers (dial-out case) is subject to the policies of the conference server.

To ensure that a user who joins or leaves an ongoing conference cannot decrypt the conference RTP media sent out by the conference server during the user's absence from the conference, group keys are not used. Instead, the conference server specifies individual keys per participant for all media streams it sends out.

The conference server may support TLS for MSRP and for BFCP, and accept and perform TLS when it is specified in incoming SDP offers (dial-in case). (TLS may be offered e.g. when the network chooses to apply TLS on every hop.)

The conference server may or may not request TLS for MSRP and for BFCP in SDP offers it sends in outgoing SDP offers (dial-out case). This depends on the policies of the operator. If the conference server is configured not to use TLS, MSRP and/or BFCP may still be protected by TLS over the access network to a participant, if the participant and the network have negotiated using this protection over the access network.

If the conference server applies TLS for MSRP or BFCP towards more than one participant, it uses TLS in a way that ensures that different keys will be used for different connections.

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

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

5.3.3 KMS-based solution

5.3.3.1 Introduction

Establishing a secure, ad-hoc conference in a potentially hostile environment presents a number of challenges. Ideally, the conference creator would only need to trust the conference factory and the users that he intends to invite, while an invited user would only need to trust the inviter. The KMS-based conferencing solution achieves by introducing a trusted-third-party, the KMS.

The KMS-based solution for conferencing is based on the functionality for KMS-based media security as described in TS 33.328 [3] and MIKEY-TICKET RFC 6043 [18]. The key management described and discussed is based on MIKEY-TICKET used in mode 1, i.e. there is a REQUEST, a TRANSFER and a RESOLVE exchange. Use of key forking is an essential component in the solution which provides user authentication. Key forking is available in MIKEY-TICKET mode 1 and 3. The solution is based on the assumption that that the conference system is an authorized user of KMS services.

5.3.3.2 Overview of the solution

Securing an ad-hoc conference requires several sub-problems to be solved. An overview of the problems and their proposed solution is presented below.

The first problem is admission control, i.e. determining the users that are allowed to join the conference. In the KMS-based solution the conference creator transfers a participant list to the conference focus and only the users present on this list are allowed to join. In order to prevent certain attacks however, the following requirements must be met: (1) the conference creator and conference focus must be certain of each other's identities and (2) the participant list must be authenticated and bound to the particular conference focus. To meet these requirements the conference creator and conference factory performs a TRANSFER exchange with the participant list included in a special extension payload.

The second problem concerns conference invitations. A user that receives a conference URI must be able to determine if the conference focus is legitimate or not. It is relatively easy to setup a fake conference focus that lies about the identity of the conference creator and the identities of the other conference participants. One way of preventing this is to use a special naming scheme for conference URIs that can only be used by legitimate conference systems (e.g. focusX.conferencing@operator.com). A user would check that the conference URI is of the required form and reject an invitation if the check fails. Another solution which can be used in parallel is to let the inviter vouch for the conference URI. Exactly how this is performed varies depending on the invitation technique but the basic idea is that the inviter uses (the pre-shared key variant of) S/MIME to authenticate the conference URI and the identity of the invited participant.

The third problem is protection of media. For the sake of simplicity and convenience, the KMS-based solution only uses bilateral keys. Another simplification is the requirement that the mixer actually performs mixing, i.e it has its own SSRCs (see note below). Together this means that the establishment of the media protection keys can be done in the

same way as in a point-to-point call between two UEs. Basically, the only difference is that one UE is replaced by the conference focus.

The fourth and final problem is protection of conference event notifications. Users subscribe to the conference event package and receive notifications in the same way in as in a normal ad-hoc conference. The difference here is that the user must be an authorized conference participant and that the state information is protected using (the pre-shared key variant of) S/MIME.

NOTE 1: In MIKEY-TICKET the SRTP master key is unique per SSRC. This is a difference compared to SDES which uses endpoint unique SRTP master keys (and a mechanism known as late binding). While the approach chosen by MIKEY-TICKET has many upsides, there is also a downside in that the SSRCs need to be explicitly signalled as part of the key exchange. In a conferencing scenario where the mixer acts as a translator this causes a problem: each time someone joins the conference the focus must send out the new participant's SSRCs to the old participants (this applies even when group key are not used). To cope with this problem it is required that the mixer always performs mixing, i.e. the SSRC field of SRTP packets sent out from the mixer contains the mixer's own SSRC. In case group keys would have been used, a positive side-effect is that there is no longer any need to enforce unique SSRC values within the RTP session (at least not from a security perspective).

NOTE 2: S/MIME refers to the pre-shared-key variant of S/MIME defined in Annex B of this TR, and not the RFC 5751 definition of S/MIME. The pre-shared key used to protect the message is transported in a TRANSFER_INIT message carried inside the S/MIME structure.

5.3.3.3 Secure conference creation with a conference factory URI

To create a secure conference the user first requests MIKEY-TICKET from the KMS with the conference factory URI as allowed recipient. The MIKEY-TICKET is used to generate a TRANSFER_INIT message which is sent inside an INVITE to the conference factory. This will allow the conference factory to securely authenticate the user and verify that the he is authorized to set up the conference. Provided the verification is successful, the conference factory creates a conference focus and includes a TRANSFER_RESP message in the SIP response. Since the conference URI is used as responder identity in this message, the user can authenticate the conference focus and verify that it was allocated by the conference factory.

The set of allowed participants may be specified at the conference creation by including an extension payload in the TRANSFER_INIT message. The extension payload (see Annex C) lists the SIP URIs of the other participants and is automatically integrity protected. To update the set of possible conference participants the conference owner can send an UPDATE or a re-INVITE to the focus with a new TRANSFER_INIT. In case of such an update, the TRANSFER_RESP message sent back serves no other purpose than confirming the update.

Note that the conference creator joins the conference as part of the conference creation. In fact, the call flow for creating a conference is identical to the call flow for joining a conference, except for the Request URI and the additional MIME body part holding the TRANSFER message. In particular, the establishment of the media protection keys through SDP offer/answer is unchanged.

An example INVITE is shown below (some headers have been excluded). The format of the SIP response is similar.

```
INVITE sip:conference-factory@home2.net SIP/2.0

From: <sip:user1_public1@home1.net>; tag=171828

To: <sip:conference-factory@home2.net>

Call-ID: cb03a0s09a2sdfglkj490333

Cseq: 127 INVITE

Contact: <sip:user1_public1@home1.net

Content-Type: multipart/mixed;boundary="boundary1"

Content-Length: <length>


--boundary1

Content-Type: application/sdp


<SDP offer goes here>


--boundary1

Content-Type: application/mikey

Content-Transfer-Encoding: base64


Mgj4hyruihyu8568dfg543...

--boundary1--
```

NOTE 1: The conference factory and the conference focus are, from a key management point of view, associated with a single KMS user. The URI for the conference factory and a conference focus are, from the KMS point of view, two different public user identities belonging to the same KMS user identity. The conference URIs a factory is allowed to create can be specified either via a rule or an explicit list. For example, this could be achieved by a naming convention; if the conference factory is named factory.conferencing@operator.com then conference URIs could be named focusX.conferencing@operator.com where X would be an identifier for a specific conference.

NOTE 2: In order for the conference creator to be able to securely identify the conference focus, the MIKEY-TICKET carried in the TRANSFER_INIT shall be profiled to use forking, i.e. the I flag shall be set to 1 (use forking). Furthermore, since there is no traffic to protect (e.g. RTP) the TRANSFER_INIT/RESP message shall not contain any crypto sessions (#CS =0). This also means that it is unnecessary to include any TEK, TGK, or GTGK in the MIKEY-TICKET.

5.3.3.4 Inviting other users to a secure conference

5.3.3.4.1 Conference creator includes an URI list at conference creation

The conference creator can request the conference focus to invite an initial set of participants by including a URI list in the INVITE sent to the conference factory. The conference focus will verify that each user in the list is an authorized participant and, provided the verification is successful, ask them to join the conference by sending out INVITEs.

Note that participants invited through URI lists are able to identify the conference focus (at media setup) but they cannot determine its trustworthiness. It is possible to set up a fake conference focus and fool an invited user about the identity of the conference creator and the identities of the other participants. To prevent this one could require that conference focus URIs follow a specific naming scheme (e.g. focusX.conf@operator.com) that only legitimate conference systems are allowed to use. An invited user would check the name of the conference focus and only accept the invitation if it is of the required form. Another solution to the problem is obviously to forbid URI lists and use one of the other invitation techniques instead.

An example INVITE is shown below (some headers have been excluded).

```
INVITE sip:conference-factory@home2.net SIP/2.0

From: <sip:user1_public1@home1.net>; tag=171828

To: <sip:conference-factory@home2.net>

Call-ID: cb03a0s09a2sdfglkj490333

Cseq: 127 INVITE

Contact: <sip:user1_public1@home1.net

Content-Type: multipart/mixed;boundary="boundary1"

Content-Length: <length>


--boundary1

Content-Type: application/sdp


<SDP offer goes here>


--boundary1

Content-Type: application/resource-lists+xml

Content-Disposition: recipient-list


<URI list goes here>

--boundary1

Content-Type: application/mikey

Content-Transfer-Encoding: base64


Mgj4hyruihyu8568dfg543...

--boundary1—
```

5.3.3.4.2 Conference creator sends REFER to conference focus

The conference creator can invite another user to join the conference by sending a REFER request to the conference focus with the SIP URI of the user in the refer-to header. Upon receipt of the request, the conference focus either sends an INVITE or a REFER request to the invited user (depending on the method parameter in the refer-to header). Regardless of the method used, the result is that the invited user joins the conference.

In order to mitigate spoofed conference URIs, the conference creator should include a Referred-By header in the REFER. The Referred-By header contains the identity of the conference creator and a reference to an S/MIME protected message/sipfrag body part, which in turn contains copies of the Referred-By, Refer-To, and Date headers. When the INVITE (or REFER) is sent by the conference focus it will contain a copy of the referred-by header and the referenced S/MIME entity. This will allow the invited user to authenticate the referrer and validate the correctness of the INVITE (or REFER). Provided users only accept conference invitations where the referrer is known and trusted, the conference focus and the information it sends out can also be trusted.

The REFER request could potentially be sent by some other user than the conference creator. However, since it is only the conference creator that can add the invited user to the set of authorized participants, it is probably easiest if the conference creator also sends the REFER.

An example REFER and an example INVITE are shown below.

```
REFER sip:conference1@mrfc1.home1.net SIP/2.0
From: <sip:user1_public1@home1.net>; tag=171828
To: <sip:conference1@mrfc1.home1.net>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 REFER
Contact: <sip:user1_public1@home1.net;
Refer-To: <sip:user2_public1@home2.net;method=INVITE>
Referred-By: <sip:user1_public1@home1.net>;
      cid=20398823.2UWQFN309shb3@home1.net
Content-Type: multipart/mixed;boundary="boundary1"
Content-Length: <length>

--boundary1
Content-Type: application/pkcs7-mime; smime-type=auth-enveloped-data; name=smime.p7m
Content-Length: <length>
Content-ID: <20398823.2UWQFN309shb3@home1.net>
*******************************************************
* Content-Type: message/sipfrag                       *
* Content-Disposition: aib; handling=optional         *
*                                                     *
* Refer-To: <sip:user2_public1@home2.net;method=INVITE>   *
* Referred-By: <sip:user1_public1@home1.net>;         *
*     cid=20398823.2UWQFN309shb3@home1.net            *
* Date: Thu, 21 Feb 2002 13:02:03 GMT                 *
*******************************************************
--boundary1
```

```
INVITE sip:user2_public1@home2.net SIP/2.0
From: sip:conference1@mrfc1.home1.net; tag=167854
To: <sip:user2_public1@home2.net>
Call-ID: cr03a0s39a2sdcglkj49432
Cseq: 127 INVITE
Contact: <sip:conference1@mrfc1.home1.net>
Referred-By: <sip:user1_public1@home1.net>;
      cid=20398823.2UWQFN309shb3@home1.net
Content-Type: multipart/mixed;boundary="boundary1"
Content-Length: <length>

--boundary1
```

```
Content-Type: application/sdp


<SDP offer goes here>

--boundary1
Content-Type: application/pkcs7-mime; smime-type=auth-enveloped-data; name=smime.p7m
Content-Length: <length>
Content-ID: <20398823.2UWQFN309shb3@home1.net>
*******************************************************
* Content-Type: message/sipfrag                       *
* Content-Disposition: aib; handling=optional         *
*                                                     *
* Refer-To: <sip:user2_public1@home2.net;method=INVITE>   *
* Referred-By: <sip:user1_public1@home1.net>;         *
*     cid=20398823.2UWQFN309shb3@home1.net            *
* Date: Thu, 21 Feb 2002 13:02:03 GMT                 *
*******************************************************
--boundary1--
```

5.3.3.4.3 Conference creator sends REFER to other user

The conference creator can invite another user to join the conference by sending a REFER request to the user and including the conference URI in the refer-to header. Upon receipt of the request, the invited user sends an INVITE to the conference focus and joins the conference.

In order to mitigate spoofed conference URIs, the conference creator should authenticate the REFER request. This is done by adding an S/MIME protected message/sipfrag body part which contains copies of the From, To, Call-ID, CSeq, Contact, and Date headers (this follows the AIB format specified in RFC 3893). The invited user should verify the identity of the referrer and only join the conference if the referrer is known and trusted.

The REFER request could potentially be sent by some other user than the conference creator. However, since it is only the conference creator that can add the invited user to the set of authorized participants, it is probably easiest if the conference creator also sends the REFER.

An example REFER is shown below (some headers are excluded).

```
REFER sip:sip:user2_public1@home2.net SIP/2.0

From: <sip:user1_public1@home1.net>; tag=171828

To: <sip:sip:user2_public1@home2.net>

Call-ID: cb03a0s09a2sdfglkj490333

Cseq: 127 REFER

Contact: <sip:user1_public1@home1.net;

Refer-To: <conference1@mrfc1.home1.net;method=INVITE>

Content-Type: application/pkcs7-mime; smime-type=auth-enveloped-data; name=smime.p7m

Content-Length: <length>


*********************************************************

* Content-Type: message/sipfrag                          *

* Content-Disposition: aib; handling=optional            *

*                                                        *

* From: <sip:user1_public1@home1.net>; tag=171828        *

* To: <sip:sip:user2_public1@home2.net>                  *

* Call-ID: cb03a0s09a2sdfglkj490333                      *

* Cseq: 127 REFER                                        *

* Contact: <sip:user1_public1@home1.net;                 *

* Refer-To: conference1@mrfc1.home1.net;method=INVITE    *

* Date: Thu, 21 Feb 2002 13:02:03 GMT                    *

*********************************************************
```

5.3.3.5 User joining a secure conference

A user joins the conference by sending (receiving) an INVITE to (from) the conference focus. The INVITE includes an SDP offer and an SDP answer is sent in the SIP response. The establishment of the media protection keys follows the procedure for "e2e security using KMS" described in TS 33.328 [3] with the difference that the terminating UE (originating UE) is replaced by the conference focus.

A high level and simplified description is as follows: The initiator requests a MIKEY-TICKET from the KMS and generates one or several TRANSFER_INIT messages which are included in the SDP offer. The responder extracts the TRANSFER_INIT messages, resolves the MIKEY-TICKET, and responds with one or several TRANSFER_RESP messages included in the SDP answer. When the answer arrives the initiator extracts the TRANSFER_RESP message(s) and derives the same set of media protection keys as the responder.

NOTE 1: The INVITE body may contain other MIME entities besides the SDP offer. For example, if the INVITE is sent by the conference focus due to a REFER from the conference creator, the body contains an S/MIME part asserting the referrer's identity. Furthermore, in the conference creator's case the body always contains a TRANSFER_INIT message since conference creation and conference joining occurs simultaneously.

NOTE 2: The SDP offer/answer may include additional media lines describing Binary Floor Control (BFCP) streams. The protection of BFCP streams follow the solution described for protection of TCP/MSRP in this TR.

5.3.3.6 Subscription to conference event package

The conference creator or a conference participant may subscribe to the conference event package as described in RFC 4575 using the stored conference URI. Upon receipt of the SUBSCRIBE request, the conference notification service verifies that the sender is an authorized conference participant and, provided the verification is successful, establishes the subscription to the conference state information.

Whenever there is a change to the conference state the subscription service will notify the subscribers by sending a NOTIFY message. The state information is carried in the NOTIFY body shall be confidentiality and integrity protected using S/MIME.

6 SRVCC

Editor's Note: The service requirement for this feature should be confirmed by SA1.

6.1 Introduction

Single Radio Voice Call Continuity (SRVCC) refers to the voice call continuity between IMS over PS access and CS access for calls that are anchored in IMS when the UE is capable of transmitting/receiving on only one of those access networks at a given time. For facilitating session transfer (SRVCC) of the voice component to the CS domain, the IMS multimedia telephony sessions needs to be anchored in the IMS.

Figure 6.1-1 shows a brief architecture of SRVCC based on the figures in TS 23.216 [7]. This architecture also applies for the roaming scenario. The MSC Server in the figure is enhanced for SRVCC.

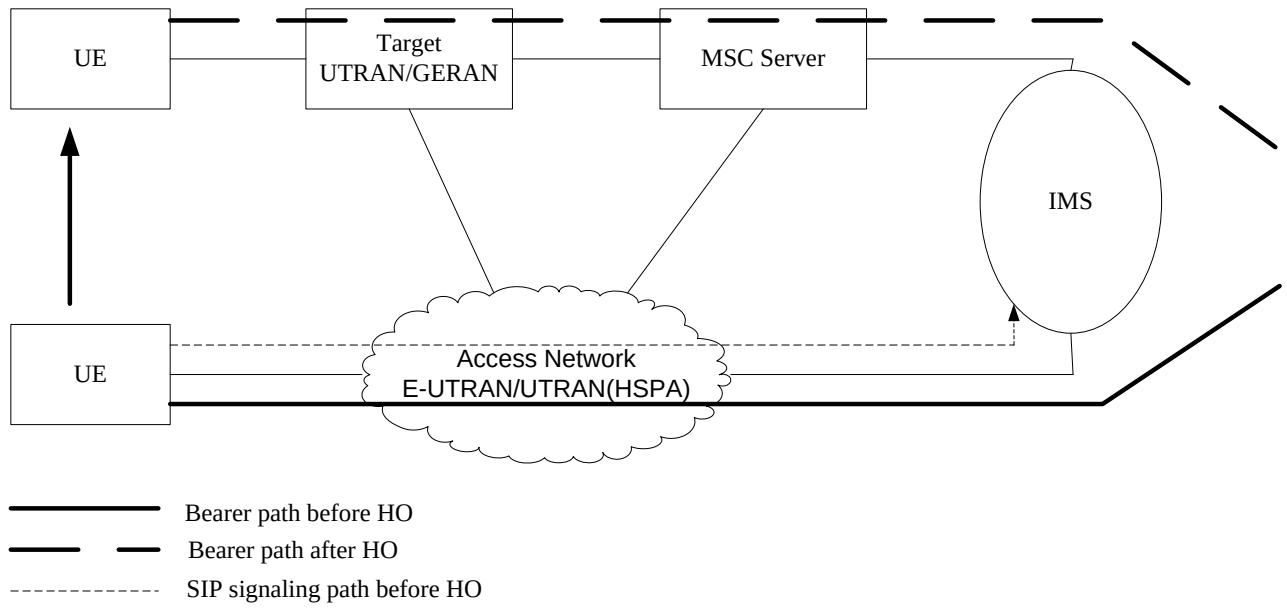


Figure 6.1-1: SRVCC Architecture

An overall high level concept for SRVCC from access network (E-UTRAN or UTRAN (HSPA)) to UTRAN/GERAN is depicted in Figure 6.1-2. This figure is based on information flows taken from TS 23.216 [7].

MME/SGSN in E-UTRAN/UTRAN (HSPA) first receives the handover request from E-UTRAN/UTRAN(HSPA) with the indication that this is for SRVCC handling, and then triggers the SRVCC procedure with the MSC Server enhanced with SRVCC via the Sv reference point if MME/SGSN has SRVCC STN-SR information for this UE. MSC Server enhanced for SRVCC then initiates the session transfer procedure to IMS and coordinates it with the CS handover procedure to the target cell. MSC Server enhanced for SRVCC then sends PS-CS handover Response to access network, which includes the necessary CS HO command information for the UE to access the UTRAN/GERAN.

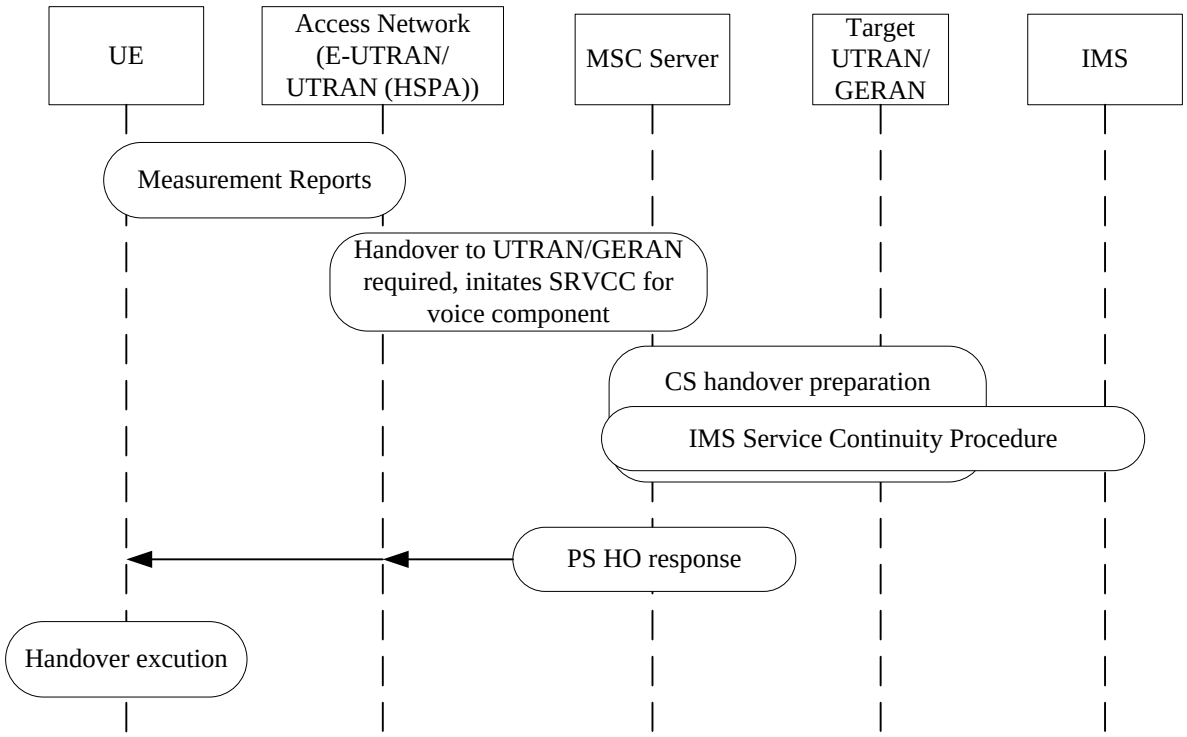


Figure 6.1-2: Overall high level concepts for SRVCC from access network to UTRAN/GERAN

6.2 Use case description

If a UE requires protected communication, after the SRVCC procedure, the media still needs to be protected, and the security should not be degraded after the handover. In this scenario, end-to-end security requirement needs to be always satisfied.

Editor's note: VCC handover scenarios should be studied and the media protection termination points defined for each scenario.

6.3 Solution(s)

To maintain end-to-end security when SRVCC occurs, and to minimise the impact on current network deployment and network elements, the following solution is proposed.

The general idea is that, when secure communication is required, the encrypted media stream, i.e. the SRTP stream is considered as the user data in CS domain, which will be transparently transmitted over the CS network. The enhanced MSC, eMSC, determines the communication is a secure session, either by an indication during the signalling exchange or by analysing the received media stream.

NOTE: How the eMSC is informed by the indication of a secure communication is FFS.

One option would be to make the UE aware of whether the CS domain supports the media plane security capability of SRVCC or not. It can be achieved by an indication of this capability included in the handover command message sent by the EPS network. If the security capability is not supported by the CS domain, the UE determines whether to continue the communication without protection or to hang up. If the e2e security capability of SRVCC is supported by the CS domain, a UE which requires e2e security is able to encrypt the voice data using SRTP and send the SRTP stream as the user data through CS domain.

eMSC is responsible for the protocol conversion. It decapsulates CS data to get the SRTP stream, then does encapsulation again over UDP/IP and sends the packet over IP bearer to UE B. And when eMSC receives the SRTP packet from UE B, it encapsulates the SRTP packet to voice data packet and sends the data through CS domain to UE A, which has successfully handed over to the CS domain after the SRVCC procedure. For UE B, in aspect of handling the secure communication, it doesn't see any difference before and after the SRVCC. The session key materials

generated/negotiated based on the IMS media plane security mechanisms before the SRVCC procedure will still be used after the SRVCC procedure. Thus, the e2e security can be guaranteed for this scenario.

Editor's Note: The feasibility and mechanisms for transparent transmission of an SRTP stream over the CS network are ffs.

Editor's Note: The LI issue should be further studied.

7 Services for user groups with high security requirements

7.1 General

Some user groups with enhanced security requirements resembling enterprises (e.g., corporate and government enterprises) may have limited trust in the inherent IMS security. Moreover, these enterprises may find it more cost-effective to work with third-party managed service providers for all their communications needs, while still retaining the secrecy of enterprise data.

7.2 Use cases

Targeted use cases are Enterprises, National Security and Public Safety, Government communications, first responders, etc. which may have limited trust in the existing IMS security and/or may desire to provide their own key management service. An example use case is an operator that owns IMS infrastructure and provides managed services to Enterprises for their IP telephony and Multimedia Applications.

In TS 33.328 [3] two solutions were standardized, one for major user categories and one for the above mentioned use cases. Some of the above user groups desire or require the following additional requirements, not provided by the solutions standardized in TS 33.328 [3]:

- Elimination of passive key escrow.
- Perfect forward secrecy between sessions.

Active key escrow may still be possible.

Editor's note: It is for further study whether elimination of passive key escrow capability without elimination of active key escrow is a significant enough security uplift to justify standardization of a completely new IMS media plane security solution. Lawful interception requirements for this use case are also for further study.

7.3 Solution(s)

7.3.1 MIKEY-IBAKE

MIKEY-IBAKE, as specified in IETF RFC 6267 [28], is a key management protocol variant for the Multimedia Internet KEYing (MIKEY) which relies on trusted key management service. In particular, MIKEY-IBAKE utilizes Identity Based Authenticated Key Exchange framework which allows the participating clients to perform mutual authentication and derive a session key in an asymmetric identity based encryption framework. This framework, in addition to providing mutual authentication, provides ways to eliminate the key escrow problem and provides perfect forward secrecy.

NOTE: As stated in RFC 6267 [28], the actual session keys used for traffic protection are generated between the end users and thus are not known by the KMS or any other entity in the network. As such, MIKEY-IBAKE enables complete elimination of key escrow. In addition, session keys are generated according to an Elliptic Curve based Diffie-Hellman protocol, ensuring that MIKEY-IBAKE provides perfect forward secrecy. On the other hand, to satisfy LI requirements the session keys need to be made available to the LI entities. There are multiple approaches to satisfy this requirement.

Additionally, the following call scenarios are securely supported: secure forking, retargeting, deferred delivery and pre-encoded content.

In the case that MIKEY-IBAKE is used for deferred delivery there are some requirements on mailbox security that need to be addressed to protect against source spoofing and alteration of deposited messages – see TR 33.828 [2] for details.

Editor's note: LI solutions for MIKEY-IBAKE are currently being discussed by SA3-LI.

Editor's note: It should be clarified are properties in 7.2 still enjoyed with modified LI solution for MIKEY-IBAKE.

MIKEY-IBAKE is explained in TR 33.828 [2]. TR 33.828 [2] also provides MIKEY-IBAKE signaling call flows and their description, cf. clause 7.6.2.1 of TR 33.828 [2].

8 IMS messaging

8.1 Introduction

8.1.1 General

The stage 3 specification of messaging services in IMS is given in TS 24.247 [10] which is based on the stage 2 specification given in clause 5.16 in TS 23.228 [8]. Clause 4 in TS 24.247 [9] gives the following overview of IMS messaging features:

The messaging service within the IM CN subsystem provides the means for a user to send or receive single messages immediately to / from another user and to create and participate in a messaging conference with one or more other users. Participants to such message based communication may be internal or external to the home network.

When to use an immediate message and when to use a session-based messaging session will depend on the application.

NOTE: Some participants may always use session-based messaging, while others may use immediate messaging or a combination of session-based messaging and immediate messaging dependant of the characteristics of the messaging session. The criteria are implementation and application specific.

For immediate messaging the procedures for page-mode messaging, as defined in RFC 3428 [12] or for session-mode messaging, as defined in RFC 4975 [13], draft-ietf-simple-msrp-sessmatch [14] andRFC 6135 [15] are utilized. When to use a page-mode messaging and when to use session-mode messaging session for the purpose of immediate messaging will depend on the application.

For session-based messaging and session-based messaging conferences, the Message Session Relay Protocol (MSRP) is utilized to transport messages.

As described above, there are three types of messaging services in IMS: immediate messaging, (one-to-one) session-based messaging and session-based messaging conferences. These use cases and the corresponding SIP signalling is described in more detail in clause 8.2.

More advanced services like delivery reports, chat alias, private messages, conversation history, barring, and participant information has been standardized by IETF and OMA. The services are invoked/used by sending information in SIP headers or MIME content types, which is parsed by an AS or another terminal. It is ffs if these services have impact on the security solution.

Message interworking is described in TS 29.311 [10].

8.1.2 Immediate security observations

- For immediate message e2ae security and even hop-by-hop security covering the whole signalling path is already standardized (SIP security). To accomplish e2e security in the same way as for RTP-based media some type of application layer security e.g. an enhanced version of S/MIME is needed.
- For immediate message the key management signalling has to be half-roundtrip (i.e. no negotiation). The key management signalling could be transferred in a SIP header or in the SIP body.
- The solution should also support sending of messages to multiple recipients.
- For session-based messaging (MSRP), e2ae, hop-by-hop security could be achieved by using TLS. If no application servers are involved then TLS may provide end to end security.To accomplish e2e security in the same way as for RTP-based services e.g. an enhanced version of S/MIME is needed.
- For MSRP, the key management is not limited to half-round trip and can therefore include some negotiation. For TLS, the key management could be transferred in a SIP header. Some extra per-message information may also be needed in the MSRP body. For end-to-end security, the credentials for key management could be transferred in a MSRP header or in the MSRP body with an appropriate MIME type (e.g. application/mikey).
- For session-based messaging conferencing, an end-to-end security solution may use a group key. As the architecture for session-based messaging conferencing and ordinary voice conferences are similar, they could eventually use similar security solutions. However, in contrast to voice, messages may typically not require mixing, i.e. there may be less need for cleartext media access by the conference server.
- MSRP is also used for services like file transfer and image share. A solution for secure MSRP should therefore also take requirements for such services into consideration.

8.2 Use cases

8.2.1 Immediate messaging

8.2.1.1 General

In immediate messaging there is no protocol session involved as each message is independent of the previous messages. Messages are sent using the SIP MESSAGE method (RFC 3428 [12]). The messages can contain any type of payload (not only text), formatted with an appropriate MIME type.

```
MESSAGE sip:user2@domain.com SIP/2.0
Via: SIP/2.0/TCP user1pc.domain.com;branch=z9hG4bK776sgdkse
Max-Forwards: 70
=4958in.com
Cal.2.3.4
CSeq: 1 MESSAGE
Content-Type: text/plain
Content-Length: 31

All your base are belong to us.
```

The message is routed like an SIP INVITE and the sender gets a 200 OK as response. A MESSAGE request does not create a SIP dialog.

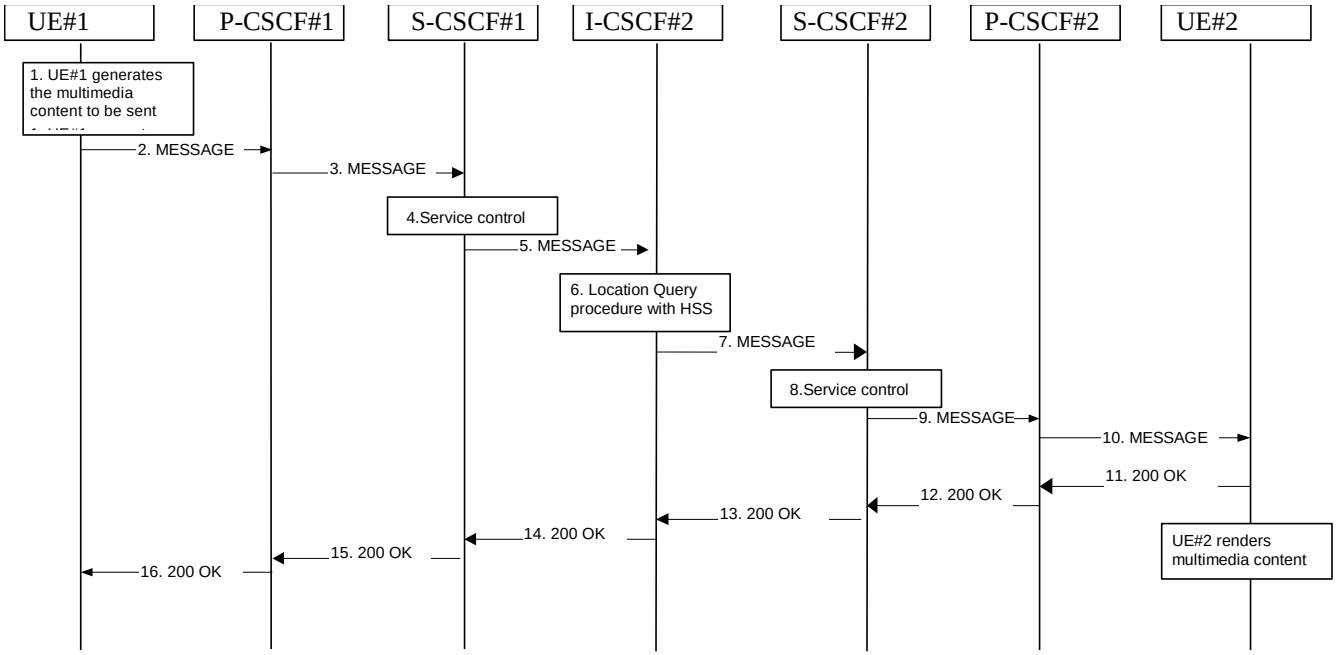


Figure 8.2.1.1-1: Immediate messaging procedure to registered Public User Identity

In step 4 and 8 the S-CSCF may reject (based on operator policy) the MESSAGE request with an appropriate response, e.g. if content length or content type of the MESSAGE are not acceptable. S-CSCF invokes whatever service control logic is appropriate for this MESSAGE request. This may include routing the MESSAGE request to an Application Server, which processes the request further on.

8.2.1.2 Deferred delivery

If UE#2 is unregistered, service control is invoked by its S-CSCF as shown in step 8 in the figure below. If UE#2 has a deferred delivery service activated, the MESSAGE request is routed to an AS, that holds the MESSAGE request and delivers it when UE#2 becomes reachable (not shown in the figure below).

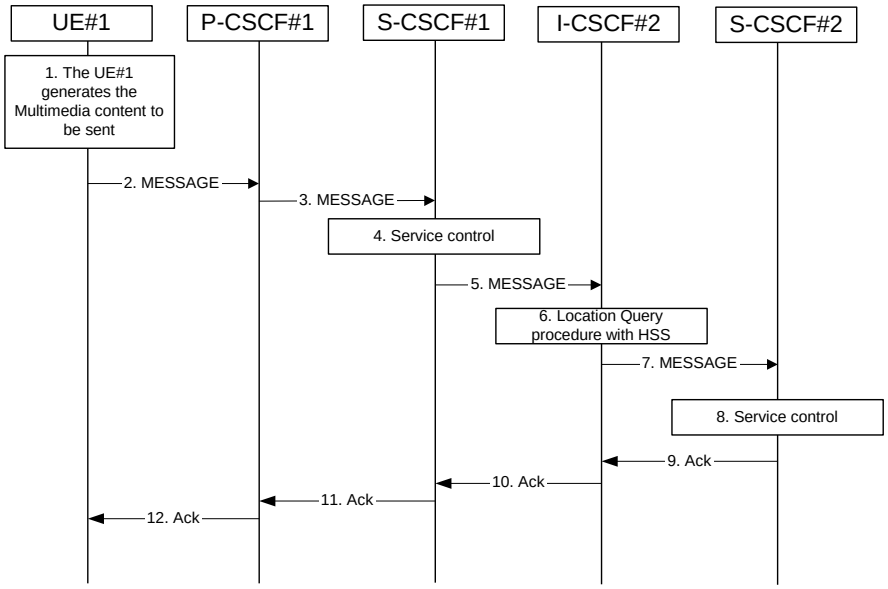


Figure 8.2.1.2-1: Immediate messaging procedure to unregistered Public User Identity

8.2.1.3 Multiple recipients

A single MESSAGE request can be sent to multiple recipients. This can be done in two ways:

- Address the MESSAGE request to a PSI (Public Service Identity) identifying a predefined group. The MESSAGE request will be routed to the AS hosting the PSI, which creates and sends MESSAGE requests addressed to each one of the group members.

- Address the MESSAGE request to the AS that implements the role of the List Server. Multiple IMPUs is included in a multipart body according to RFC 5365 [16]. The AS creates and sends MESSAGE requests addressed to each one of the group members.

The AS returns 202 Accepted.

8.2.2 Session-based messaging

8.2.2.1 (One-to-one) session-based messaging

Before any instant message can be sent a session must be established using SIP/SDP. The actual messages are sent using MSRP (RFC 4975 [13]) on top of TCP. The messages can contain any type of payload (not only text), formatted with an appropriate MIME type.

```
MSRP a786hjs2 SEND
To-Path: msrp://biloxi.example.com:12763/kjhd37s2s20w2a;tcp
From-Path: msrp://atlanta.example.com:7654/jshA7weztas;tcp
Message-ID: 87652491
Byte-Range: 1-31/31
Content-Type: text/plain

All your base are belong to us.
-------a786hjs2$
```

Message sessions may be either established end to end between two UEs (as shown in Figure 8.2.2.1-1 below) or may involve one or more intermediate nodes (e.g. an Application Server performing per message charging).

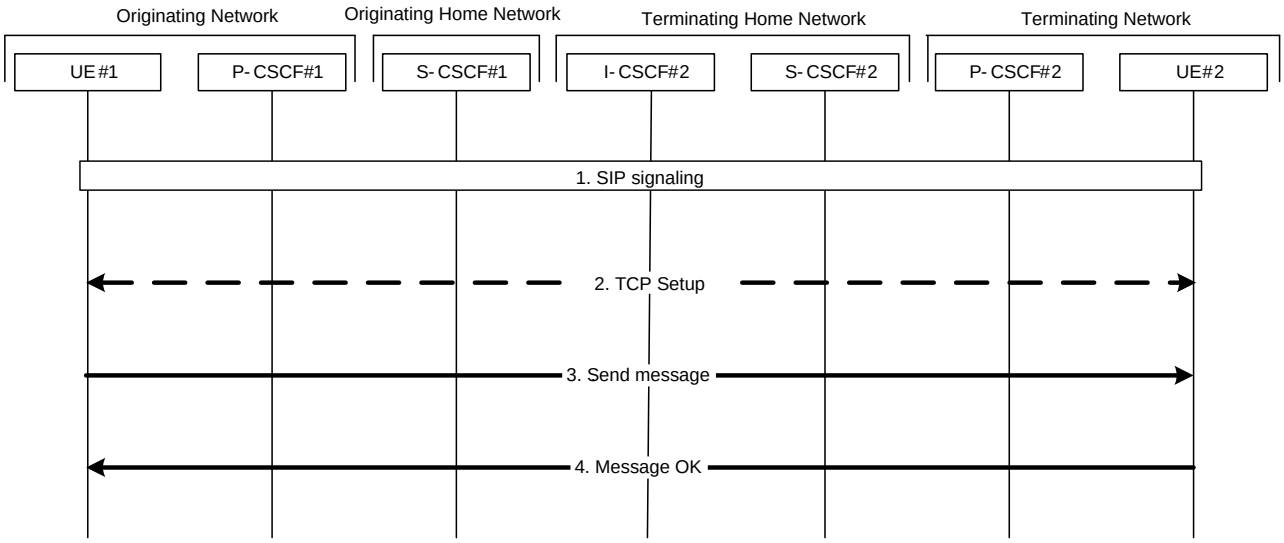


Figure 8.2.2.1-1: Establishment of a MSRP session

An MSRP session between two users can be established with involvement of an intermediate node (messaging AS) if for example charging mechanisms are required. In this case the AS is able to inspect the SIP signalling as well as the exchanged messages and their content. Example call flow for establishment of MSRP session with intermediate nodes can be found in clause A.4.3 of 24.247.

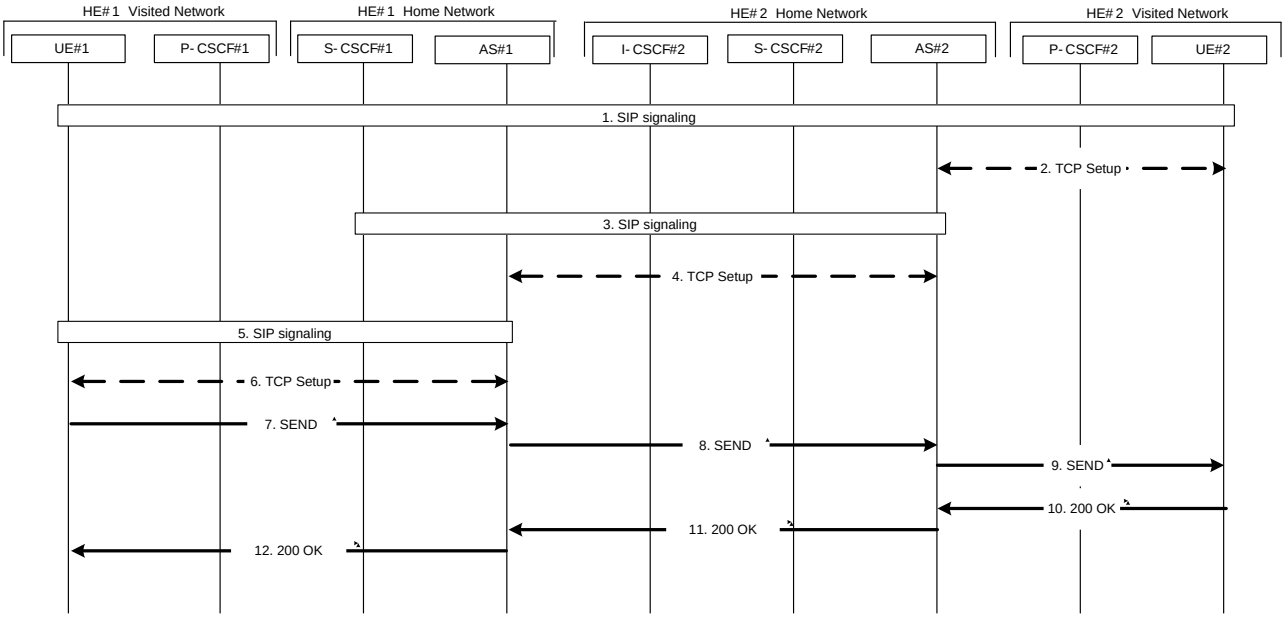


Figure 8.2.2.1-2: Establishment of a MSRP session with Intermediate Nodes

8.2.2.2 Session-based conference messaging

Session-based messaging between more than two UEs requires the establishment of a session based messaging conference. Within session based messaging conferences including multiple UEs (e.g. multiparty chat conferences) an MRFC/AS controls the media resources, and the MSRP/TCP connection is established hop-by-hop via an MRFP. The functional split between AS, MRFC and MRFP is the same as the one described in clause 4 of TS 24.147 [4] for SIP based conferences. Example call flow for establishment of session-based messaging conference can be found in clause A.5.1 of 24.247. The UE can connect to a conference by sending an SIP INVITE to the MRFC/AS as illustrated in Figure 8.2.2.2-1.

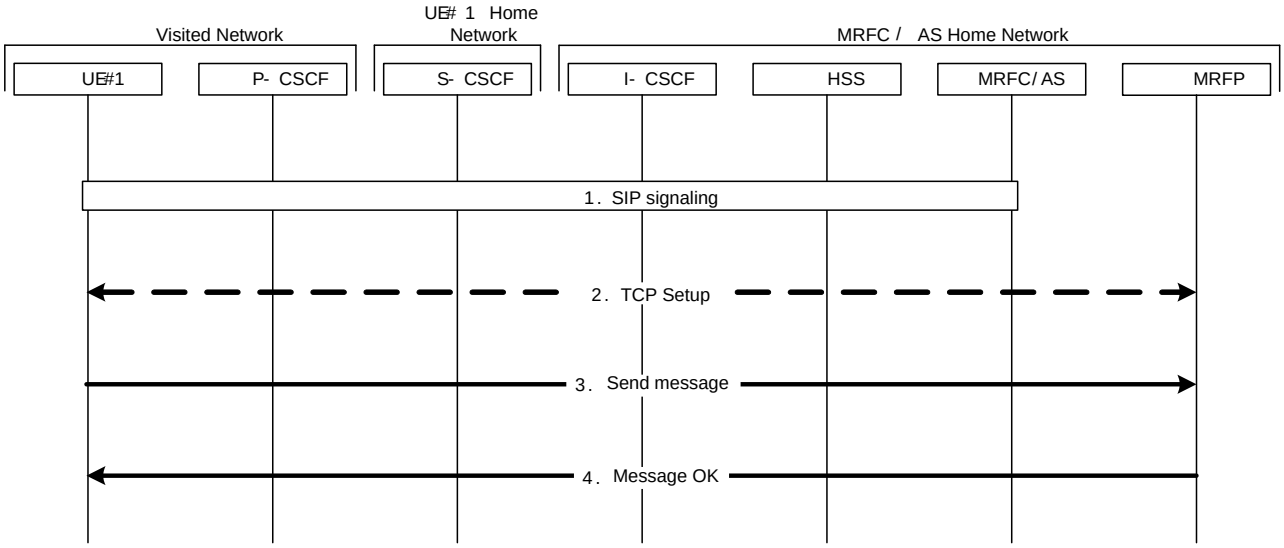


Figure 8.2.2.2-1: Establishment of a MSRP messaging conference

The MRFC/AS can also invite a UE to a messaging conference.

8.3 Solution(s)

8.3.1 KMS-based solution

8.3.1.1 Immediate messaging

8.3.1.1.1 UE sends a SIP MESSAGE

A UE prepares a protected SIP message as described in Clause 5.3.1.2 of TS 24.247 [9], with the difference that S/MIME is applied for content protection. Here S/MIME refers to the pre-shared-key variant of S/MIME defined in Annex B of this TR, and not the RFC 5751 definition of S/MIME. This variant of S/MIME encrypts and authenticates the MIME content using a symmetric key that is transported inside a TRANSFER_INIT message. An example of a protected MESSAGE is shown below.

```
MESSAGE sip:user2@domain.com SIP/2.0
Via: SIP/2.0/TCP user1pc.domain.com;branch=z9hG4bK776sgdkse
Max-Forwards: 70
From: sip:user1@domain.com;tag=49583
To: sip:user2@domain.com
Call-ID: asd88asd77a@1.2.3.4
CSeq: 1 MESSAGE
Content-Type: application/pkcs7-mime;
smime-type=auth-enveloped-data;
             name=smime.p7m
Content-Length: <length>

*******************************************************
* Content-Type: text/plain                            *
```

```
*                                                     *
* All your base are belong to us.                     *
*******************************************************
```

The UE must make sure that the MIKEY-TICKET inside the TRANSFER_INIT is resolvable by all the intended recipients. Typically, the intended recipient is the URI indicated in the To header field of the request. This is true when:

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

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

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

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

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

8.3.1.1.2 UE receives a SIP MESSAGE

Upon receipt of a protected SIP MESSAGE, the UE extracts the protected content and hands it over to S/MIME for integrity verification and decryption. The responder also checks if the sender identity reported back by S/MIME matches the identity contained in the From header field. In case the identities differ, the S/MIME identity takes precedence and must be displayed to the user. As described above, this may happen when a list server re-encrypts the content but leaves the From header field intact. The same thing happens when a list server adds its own protected content to a forwarded message (for example the identities of the other recipients). Otherwise the handling is as described in clause 5.3.1.3 of TS 24.247 [9].

Deferred delivery with MIKEY-TICKET can be accommodated by using a replay cache for TRANSFER_INIT messages which does not enforce any message age restriction (this is not required either by [19]), The replay cache would accept a new entry as long as the cache is not full or if the entry is more recent than the oldest entry (determined from the message timestamp). If the cache is full and the oldest entry is older, the oldest entry is deleted and the new entry is inserted. Furthermore, the size of the cache must be adjusted according to the expected message intensity and the offline time (i.e. the period during which the UE is unreachable). The AS can also reduce the likelihood that a valid message gets rejected by delivering all the deferred messages in order, starting with the oldest one. However, even with the increased cache size, in case of high volume of messages or extended offline time the entry may not be found in the cache and needs to be dropped at the UE due to the outdated Timestamp.

8.3.1.1.3 List server forwards a SIP MESSAGE to multiple recipients using a PSI

A protected SIP MESSAGE that includes a PSI in the request URI is forwarded by the list server to all the entries in the associated URI list as described in Clause 5.3.3.1 and Clause 5.3.3.2 of TS 24.247. The only difference is that the protected content in the incoming message must be re-encrypted before it is copied to the outgoing message. When the list server decrypts the content it must verify that the sender identity reported by S/MIME matches the identity in the To header field of the incoming message. Provided the verification is successful, the list server re-encrypts the content and

sets the MIKEY-TICKET in the TRANSFER_INIT to be resolvable by all the entries in the predefined URI list. The re-encrypted content is then copied to all of the outgoing messages.

8.3.1.1.4 List server forwards a SIP MESSAGE to multiple recipients using a URI-list

A protected SIP MESSAGE with a URI-list included in the multipart body is forwarded by the list server to all the entries in the list as described in Clause 5.3.3.3 and Clause 5.3.3.4 of TS 24.247. There is no need to re-encrypt the protected content since the MIKEY-TICKET inside the TRANSFER_INIT is resolvable by the final recipients.

If the list server includes a URI-list in the outgoing SIP message, as described in RFC 5365 [12], it should be protected using S/MIME. It is possible to encrypt the URI-list once and copy it to all the outgoing messages by using a MIKEY-TICKET that is resolvable by all the recipients.

8.3.1.2 One-to-one session based messaging

In this solution, MSRP sessions are protected using TLS-PSK and MIKEY-TICKET. The PSK used in the TLS handshake is established by performing a TRANSFER exchange as part of the SDP offer/answer.

MSRP sessions and RTP session are similar in that they are both negotiated through SDP and have associated m-lines. The way the TRANSFER exchange is carried out using the "key-mgmt" attribute therefore remains the same. In fact, if the "key-mgmt" attribute is used at SDP session level, the same TRANSFER exchange can be used to setup up keys for both SRTP and TLS-PSK.

To protect an MSRP session, the offerer sets the protocol identifier to "TCP/TLS/MSRP" and includes a Crypto Session (CS) of type TLS in the TRANSFER_INIT message. The TRANSFER_INIT message is generated in the same way as in the e2e security solution for RTP based traffic, and is added to the SDP as a "key-mgmt" attribute at session or media level. The TEK associated with the CS is the PSK that will be used in the TLS handshake (see Annex D).

MSRP allows several sessions to share the same TCP connection by using the same port value in multiple m-lines. However, since TLS connections cannot be multiplexed, the MSRP sessions must all share the same TLS connection. This causes a problem when MIKEY-TICKET is used since the PSK is specific for each session. To get around this problem, sharing of a TCP connection is not permitted in this solution.

Also note that a TLS connection may span more than one TCP connection if media anchoring is employed and a media gateway is inserted in the media path. This may be required, for example, in order to perform NAT traversal. The media gateway will not have access to the plaintext data and will simply relay the TLS records between the incoming and outgoing TCP connection. In order for this to work, however, both the peers and the media gateway need to support the Connection Establishment for Media Anchoring (CEMA) extension to MSRP defined in [reference].

Since the purpose of this solution is to provide end-to-end security, intermediate nodes cannot be allowed to terminate the TLS connection and access the plaintext media. Therefore, if either peer notices that the other endpoint is not as expected, the MSRP session setup should be aborted. The identity of the other peer is determined from the TRANSFER_INIT/TRANSFER_RESP message and is always verified by the KMS.

8.3.1.3 Session based messaging conferences

In this case, an MRF/AS acts as a conference server and distributes all messages sent by one participant to all the other participants in the session. Participants can join the conference by sending an INVITE to the conference URI (Public Service Identifier) representing the messaging session.

The conference server shall be configured to only accept TCP connections secured by TLS. In the "dial-in" case, it can enforce usage of TLS by rejecting INVITEs that do not specify TCP/TLS/MSRP as the media protocol. In the "dial-out" case, it can enforce the usage of TLS by specifying TCP/TLS/MSRP as the media protocol. The establishment of the MSRP session is identical to the one-to-one case, except that one UE is replaced by the conference focus.

8.3.2 Solutions that leverage IMS control plane security

8.3.2.1 Immediate messaging

In this solution, security for immediate messaging (using SIP MESSAGE) solely relies on IMS control plane protection. SIP MESSAGE messages are transported in the IMS control plane and are thus protected.

The IMS control plane can be secured using IPsec or TLS between the IMS-UE and the P-CSCF and between core network elements. Similar to the "SDES-based solution" for key management for the protection of real time traffic (see TS 33.328 [3], clause 6.2.2), integrity protection as well as confidentiality protection shall be applied.

In this solution, core network elements in the control plane have access to the message content, in particular P-, S- and I-CSCF. The solution implies that subscribers trust the network in not abusing the message content.

Like in the SDES-based key management described in TS 33.328 [3], a user A sending a message to user B has no indication about the degree of protection of the message between the core network and user B.

Application servers may be used for storing instant messages for a user that is currently not registered or for distributing instant messages to multiple recipients. In this solution, such application servers have access to the message content and must be trusted. If an AS receives a SIP MESSAGE for distribution, it may need to check the authorization of the sender. This requires identification of the sender, which is provided securely via the P-Asserted-Identity header (assuming integrity protection for the control plane, as stated above).

8.3.2.2 One-to-one session based messaging

8.3.2.2.1 General

In this solution, MSRP sessions are secured using TLS confidentiality and integrity protection. TLS endpoints may be IMS UEs, but also intermediate nodes within the network. Like the IMS UE, such intermediate nodes need not only media plane connectivity, but also control plane connectivity. They may be split in a control plane and a media plane node, like the MRF is split into MRFC and MRFP. In this case, security properties required for the control plane in this solution, like e.g. integrity protection or confidentiality protection, are also required for the interface between control plane part and media plane part of the intermediate node. To avoid complexity, intermediate nodes are described as one entity in the following, even if they are split into a control plane and a media plane node.

NOTE: Such intermediate nodes are for example involved in the message flow shown in Figure 8.2.2.1-2 (nodes AS#1 and AS#2).

Ciphersuites and session keys to protect the media transport are negotiated via the TLS handshake. The TLS record protocol secures the actual media. Mutual authentication during the TLS handshake may be achieved via different means:

a) Usage of self-signed certificates, with the certificate fingerprints being transmitted using the SDP fingerprint attribute in the SDP offer-answer exchange.

   This approach is specified in RFC 4975 [13]. "TCP/TLS/MSRP" is used as the protocol identifier in the m-line of the SDP, and the "a=fingerprint" attribute is used to provide the fingerprint of the self-signed certificate.

   It is assumed in this approach that SIP signalling is integrity protected, and that any SIP proxies between the endpoints of the TLS connection to be established are trusted. This means that the certificate fingerprints can be transported securely. If the fingerprints of the certificates used for the TLS handshake match the fingerprints transmitted via SIP signalling, then each TLS endpoint can be sure that TLS is really established between the nodes that exchanged the SIP signalling.

b) Usage of PSK TLS.

   In this case, a PSK must be established between the two parties. Assuming that SIP signalling is integrity and confidentiality protected, and that any SIP proxies between the endpoints of the TLS connection to be established are trusted, a PSK may be selected by one peer and be transmitted within the SDP to the other peer. RFC 4566 [23] specifies a "k=" line that may be used to transmit an encryption key, but does not recommend its usage, as – different from the scenario considered here – it does not assume sufficient SIP signalling security. Alternatively, the "key-mgmt" attribute specified in RFC 4567 [24] may be enhanced for this purpose, or an additional attribute may be specified (like it was done e.g. in RFC 4568 [25] (SDES) for transmitting a key to secure RTP based communication).

   In this approach, the PSK will be protected during transport, but will be accessible by core network elements. It is assumed that this, like the "SDES-based solution" in TS 33.328, satisfies the security needs of major user categories.

NOTE: When using self-signed certificates or the 'k-line' option for the PSK case then no further work in the IETF is expected to be required. For the other two options above for establishing the PSK, additional work in the IETF would be required. This needs to be taken into account when going to the normative stage. The decision whether more than one of the above options for TLS key management is to be mandated by 3GPP is left to the normative stage.

As for media security for RTP based traffic (specified in TS 33.328), protection may be offered for the access only, i.e. via a TLS connection between the IMS UE and an intermediate node within the core network. This is called e2m security in the following.

If security covers the whole transport connection between two IMS UEs, but is provided in a hop-by-hop manner, i.e. via a chain of TLS connections, this is called hop-by-hop security.

8.3.2.2.2 E2m security for one-to-one session based messaging

8.3.2.2.2.1 Terminating security at an AS

TS 23.228 [8] already describes the usage of intermediate nodes in session based messaging. For this, in the originating as well as in the terminating case, the S-CSCF, when processing an INVITE message establishing an MSRP session, routes the message to an intermediate node that acts as a SIP B2BUA and also as media relay for the session. Assuming that intermediate nodes are used on the originating and terminating side, and that these intermediate nodes are different ones, the connection will be established in at least three hops.

An example for this is shown in Figure 8.2.2.1-2: The intermediate nodes are AS#1 and AS#2, and TCP connections are established between UE#1 and AS#1, AS#1 and AS#2, and AS#2 and UE#2. In this example, when e2m security is applied for UE#1, the TCP connection between the UE#1 and AS#1 is secured using TLS. Independent from this, when e2m security is applied for UE#2, the TCP connection between the UE#2 and AS#2 is secured using TLS.

In this approach, how to use TLS (including how to negotiating whether TLS is used) can be considered to be part of the application and as such is outside the scope of 3GPP.

The communication will be available in the clear at the AS and can be intercepted there for LI purposes.

8.3.2.2.2.2 Terminating security at the IMS access gateway

Rather than at an AS, TLS may also be terminated at the IMS access gateway. In this way, many of the concepts for e2ae security for RTP based traffic specified in TS 33.328 [3] could be re-used, e.g. the

procedures for indicating the support for e2m security and for establishing MSRP sessions with e2m security could be done analogously to the procedures for e2ae security in TS 33.328 [3]:

A UE that is willing to make use of e2m security indicates this in the REGISTER request. If the network is willing to support e2m security for this UE, it indicates this in the reply on the REGISTER request. Although such indications are already specified for e2ae security for RTP based media, it is proposed in this case to introduce additional indications for e2m security for session based messaging, to allow using e2ae for RTP based media and e2m security for session based messaging selectively. If both UE and network have indicated support for e2m security in this way,

a) in the originating case, the originating UE may request e2m security for an MSRP session to be established by using "TCP/TLS/MSRP" (rather than "TCP/MSRP") in the m-line of the SDP offer, and by using an SDP attribute indicating the request for e2m security

b) in the terminating case, if no security is specified in an incoming request, the network will indicate the usage of e2m security for the MSRP session to be established by using "TCP/TLS/MSRP" (rather than "TCP/MSRP") in the m-line of the SDP offer sent to the terminating UE, and by using an SDP attribute indicating that the offered security is e2m security.

In both cases, the network inserts the IMS access gateway as an intermediate node. The TCP connection from the UE is terminated by the IMS access gateway and is secured using TLS. Another TCP connection is used from the IMS access gateway towards the other endpoint of the MSRP session (possibly via additional intermediate nodes).

Like for e2ae security for RTP based traffic, the interface between P-CSCF/IMS-ALG and IMS access gateway must allow passing the required information (e.g. the certificate fingerprints). This may be achieved by exchanging the relevant parts of the session description (using SDP), as it is the case for e2ae security for RTP-based traffic.

In this approach, the network operator has access to the cleartext communication content at the IMS access gateway, so LI can be supported conveniently.

Both methods for mutual authentication and key establishment described in 8.3.2.2.1 could be used. However, for e2m and for hop-by-hop security between UEs the same method should be chosen, to avoid that an IMS-UE must implement two different methods. Usage of self-signed certificates may not be compliant with LI requirements in some special cases of hop-by-hop security – see discussion in the following clause 8.3.2.2.3.

8.3.2.2.3 Hop-by-hop security for one-to-one session based messaging

In one-to-one session based messaging, a TCP connection may be established directly between two IMS UEs, without intermediate nodes. TLS for this TCP connection can provide e2e security for the message session (this is considered a special case of hop-by-hop security).

If key management is done using self-signed certificates, the network operator need not contribute to the media encryption (except for transporting the certificate fingerprint and the TLS handshake messages) and cannot access the cleartext media.

Note: Whether this approach complies to LI requirements has not been clarified during this study. Clarification was not necessary, as this approach has not been chosen to become part of a normative specification.

If key management is done by transmitting a PSK within the SDP as described above, the operator can facilitate lawful interception as he has access to the PSK and all exchanged information.

As Figure 8.2.2.1-2 shows, a one-to-one messaging session may involve intermediate nodes, and several TCP connections in a chain to provide media transport. In this case, each TCP connection can be secured using TLS. The media protection is interrupted at each intermediate node in this scenario. The intermediate nodes can perform their assigned functions with access to the cleartext media.

The intermediate nodes must decrypt and re-encrypt all traffic in the message session. Besides their assigned functions, they could also provide unencrypted communication content for LI purposes.

If an IMS-UE establishes a media session indicating the protocol TCP/TLS/MSRP in the SDP without indicating the request for e2m security, this is considered as a request for hop-by-hop security between UEs as described in this clause.

8.3.2.3 Session based messaging conferences

In this case, an MRF/AS acts as a conference server and distributes all messages sent by one participant to all the other participants in the session. Participants can join the session by sending an INVITE to the PSI (Public Service Identifier) representing the messaging session. The MRF/AS receives the P-Asserted-Identity of the inviting subscriber, so it can enforce that only authorized subscribers can participate in the session. In case the subscriber sending the INVITE does not reveal his identity, the MRF/AS may reject the INVITE by sending a 433 "Anonymity disallowed".

In any messaging conference, participants may use e2m security for messaging. This is transparent for the conference server.

NOTE: A UE may also implement a conferencing service, and may use e2m security, transparently for the participants. However, this is not in the focus of this specification.

A conference server may also be configured to accept only TCP connections secured by TLS for a specific messaging conference. In the "dial-in" case, it can enforce usage of TLS by rejecting INVITEs that do not specify TCP/TLS/MSRP as the media protocol. In the "dial-out" case, it can enforce the usage of TLS by specifying TCP/TLS/MSRP as the media protocol. However, this does not guarantee that the media is secured on all transport hops, as intermediate nodes may exist between the conference server and the participating UEs that terminate media protection and relay media onto unprotected TCP connections towards UEs.

On the other hand, a UE (or a messaging conference server) that establishes an MSRP session using TCP/TLS/MSRP as the media protocol and does not use e2m security as specified above, may expect the network not to change the transport to TCP/MSRP on some other transport hop. If the involved networks meet this expectation, and if the conference server rejects INVITEs not specifying TCP/TLS/MSRP, it is ensured that all media belonging to the messaging conference is secured on all transport hops.

Both variants for mutual authentication in TLS described in clause 8.3.2.2.1 can be used, i.e. either self-signed certificates or a PSK.

NOTE: If self-signed certificates are used, and a UE connects without an intermediate node directly to the conference server, and the conference server is not controlled by the operator, the operator may not be able to fulfil LI requirements, as stated in the Note in clause 8.3.2.2.3.

The conference server has access to the cleartext messages and must be trusted, as must be all intermediate nodes and all involved SIP proxies.

8.3.2.4 Preferred approach for IMS messaging security that leverages IMS control plane security

This section describes which of the various alternatives and options described in clauses 8.3.2.1 to 8.3.2.3 are recommended to be chosen, resulting in a solution that is supposed to satisfy major user categories.

8.3.2.4.1 Security for immediate messaging using SIP MESSAGE messages leveraging IMS control plane security

An IMS UE that requires security for immediate messaging leveraging IMS control plane security shall apply suitable protection of SIP signaling in general, in particular encryption in addition to integrity protection. It is understood that this protection is ensured on the first hop only, and that nodes in the IMS core may have access to the cleartext message content. In this approach, the usage of the "P-Asserted-Identity" header provides secure identification of the sender of a message by the receiver, unless the sender has chosen to hide its identity, in which case the receiver will not learn the sender's identity.

8.3.2.4.2 Security for session based messaging using MSRP leveraging IMS control plane security

Security for session based messaging leveraging IMS control plane security comprises only e2ae security. MSRP is secured over the access network between IMS UE and IMS access gateway by usage of TLS as specified in RFC 4975 [13], i.e. based on self-signed certificates and the exchange of certificate fingerprints via SIP/SDP.

An IMS UE that is willing to use e2ae security for every MSRP media stream for which it does not request e2e security indicates this during IMS registration. In its response, the network indicates whether it supports the mechanism. If the IMS UE has indicated its willingness and the network has indicated its support, the mechanism will be applied to every MSRP media stream originated or terminated by the IMS UE unless the UE indicates that it wants to use e2e security. The mechanism may even be applied to every MSRP media stream originated by the IMS UE if the IMS UE has not indicated its willingness during registration, but offers MSRP over TLS, for backward compatibility with RCS 5.0 [xx].

For this, as the originating endpoint, the IMS UE specifies "TCP/TLS/MSRP" and an "a=fingerprint" attribute in the SDP offer. Moreover, the IMS UE adds an SDP attribute indicating the request for e2ae security to the description of the MSRP media stream. (If the IMS UE does not use this indication, and does not use protocol elements indicating a request for e2e security either, the network will behave as if the IMS UE had used the e2ae indication. Cf. also NOTE below.) The network inserts the IMS access gateway into the media path. The IMS access gateway terminates TLS properly, using its own certificate (the fingerprint of this certificate is returned to the originating IMS UE in the SDP answer). From the IMS access gateway in the direction towards the terminating IMS UE, plain TCP may be used on the next hops, assuming that the interfaces are protected e.g. using NDS/IP or physical protection. Optionally, TLS may be used. The IMS access gateway relays between the TLS connection towards the originating IMS UE and the connection in the direction towards the terminating IMS UE.

In the terminating case, if the IMS UE at the terminating side and its P-CSCF have both indicated to support the mechanism during REGISTER, the network shall also insert the IMS access gateway into the media path, setup TLS towards the terminating IMS UE and relay the traffic, as it is done on the originating side. (In the SDP sent to the terminating IMS UE, the P-CSCF adds an SDP attribute to the description of the MSRP media stream indicating that the offered security is e2ae security.)

NOTE: Indication of the usage of e2ae security in INVITE messages is redundant in this approach, as a request for e2e security is expected to require specific protocol elements (like key-management attributes inside the SDP) and can thus be recognized by the network and by the terminating IMS UE. However, to keep the procedures close to the procedures for e2ae security for RTP based media, and to stay flexible for possible future enhancements, it seems reasonable to use the indications.To support IMS UEs behind NATs and IMS UEs that do not implement TCP/TLS

server functions, the SDP attribute “a=setup:passive” as specified in RFC 4145 is used in the SDP sent to IMS UEs to specify that the IMS access gateway acts as TCP server. The IMS access gateway also acts as TLS server, i.e. the IMS UE is expected to start TLS with the TLS client-hello message after the TCP connection has been established.

In this approach, the usage of the “P-Asserted-Identity” header provides secure identification of one endpoint of a message session by the other endpoint, unless an endpoint has chosen to hide its identity, in which case the other endpoint will not learn the other endpoint’s identity. In this case, an endpoint may reject or abort the session.Security for session based messaging conferences leveraging IMS control plane security is provided as described in the subclause “recommended solution” in section 5.3.2.

9 Communications diversion

9.1 Introduction

Communications Diversion (CDIV) service is a widely used service which enables a served user, to divert the communications addressed to the served user’s address to another destination according to the specified CDIV services.

CDIV is specified in TS 24.604 [11] including the following CDIV services:

- Communication Forwarding Unconditional (CFU).
- The CFU service enables a served user to have the network redirect to another user communications which are addressed to the served user's address.
- Communication Forwarding Busy (CFB).
- The CFB service enables a served user to have the network redirect to another user communications which are addressed to the served user's address and meet busy.
- Communication Forwarding No Reply (CFNR).
- The CFNR service enables a served user to have the network redirect to another user communications which are addressed to the served user's address, and for which the connection is not established within a defined period of time.
- Communication Forwarding on Not Logged in (CFNL).
- The Communication Forwarding on Not Logged-in (CFNL) service enables a served user to redirect incoming communications which are addressed to the served user's address, to another user (forwarded-to address) in case the served user is not registered (logged-in).
- Communication Deflection (CD).
- The CD service enables the served user to respond to an incoming communication by requesting redirection of that communication to another user.
- Communication Forwarding on Subscriber Not Reachable (CFNRc).
- The CFNRc service enables a user to have the network redirect all incoming communications, when the user is not reachable (e.g. there is no IP connectivity to the user's terminal), to another user.

In SIP terminology, if an INVITE is diverted, the terms “forking” (when the INVITE is sent to several SIP user agents in parallel) and “re-targeting” (when an INVITE is sent to a SIP user agent different from the originally targeted SIP user agent) are used. TS 33.328 currently describes issues with forking and re-targeting without explicitly mentioning the CDIV service.

9.2 Use cases and requirements

In CDIV scenarios, the diverted communication should still be protected with the required security level. In such cases, a call usually terminates in a phone registered by a user other than the intended receiver; the caller cannot know whether a call will be diverted when the caller makes the call. What the caller knows is just the identity of the intended user.

For secure communication, assurance about the identity of the communication peer is important. IMS provides mechanisms for user identity assurance but also for user anonymity. In the following a short overview is given.

When communications diversion is possible, a calling user cannot always be sure whether a session will be established to the intended callee or to another user (to which the call has been diverted to). Depending on the subscription options selected by the *called* user, the calling user may or may not be notified about diversion of a call (by receiving a response 181 - call is being forwarded).

A user calling another user with the goal to establish a media session with e2e media security may want to make sure that the session is established with the called user rather than with some other user, to which the call may have been diverted.

If no indication of the call being forwarded is received, a way to find out whether the call has been diverted is to check the response on the INVITE for a P-Asserted-Identity header field containing the public identity of the answering IMS user. However, such a header field may or may not be present. (If the Privacy SIP header is set to "id" in the response, the P-Asserted-Identity header is removed in the terminating network. This may happen if a supplementary service such as Terminating Identity Restriction is used by the called subscriber - see TS 24.608 [26] for details.)

If a P-Asserted-Identity is given and matches the called identity, the calling user knows that the call is established as intended. Otherwise, the calling user either knows which other user he will be connected to (namely when the call has been diverted and the P-Asserted-Identity of the diverted-to user is presented to the caller), or the caller knows that the call has been diverted without knowing to whom, or the caller only gets the information that the identity of the terminating user is unknown.

9.3 Solution(s)

9.3.1 SDES-based solution

9.3.1.1 General

For e2ae security, CDIV does not make any difference. E2ae security on the originating side is independent of the called user. If a "diverted-to" user and his terminating network have agreed on the usage of e2ae security (during registration), e2ae security will be applied for terminating calls, not depending on whether these calls have been diverted or not. Moreover, usage of e2ae security on the terminating side is transparent for the calling user.

The remainder of this clause relates to SDES-based e2e security.

If SDES is used, when communication diversion service is trigged, the AS will re-invite the corresponding user still using SDES-based solution for a secure communication. For example, user A initiates a call to user B which has subscribed the CDIV service. When the diversion condition is met, the call is re-invited by the CDIV AS to user C which is pre-assigned by user B. If SDES is used, A includes a key K1 in the SIP message, AS obtains K1 and includes it in the SIP message to C, C responds with a SIP message including a second key K2, thus the communication between A and C is protected.

As described in clause 9.2, user A may not be notified about the call being diverted. It may receive the identity of the terminating user C in a response message, or it may not receive the identity of the terminating user. In the SDES-based solution, no other means is available besides the control plane information (i.e. the SIP messages) to get assurance about the identity of the terminating user.

However, users could (try to) identify the callee during the call, via media communication, e.g. by recognizing the other user's voice. This is in general necessary, even if the identity of the terminating party is transmitted, because the terminating SIP user agent may be used by any human user that has physical access to the respective SIP phone or computer, not only by the registered subscriber. (Physical protection of such end devices cannot be assumed for major user categories.)

If SDES is used for establishing the media security association, the key for encrypting the media stream sent by the calling user is provided within the SDP part of the INVITE message. In cases of call diversion, this INVITE may reach the originally intended recipient (depending on the type of call diversion). If the call is subsequently established to the diverted-to user, the originally intended recipient may therefore be able to decrypt the media sent by the calling user, if he is somehow able to eavesdrop the encrypted media stream (e.g. by some kind of successful attack on the media routing mechanisms). (A call may even be diverted more than once, so more than one user not terminating the call may see the key allowing to decrypt the media stream of the calling user.)

9.3.1.2 SDES solution 1

When the calling user realizes that the call is established to another user than the intended callee, and he has learnt the identity of this other user then, in order to ensure that the key is known by no other user, the calling user may cancel the call and issue a new INVITE to the diverted-to user, with a new SDES crypto attribute and a different key. When however realizing that the id of the terminating user cannot be verified, the calling user has only the options to cancel the call or to proceed with the call, aware of the fact that the terminating identity is unknown.

NOTE: Possibly, alternative methods, e.g. sending an UPDATE instead of an INVITE, are feasible and useful. It has not been clarified during this study whether the original callee could potentially see the UPDATE message in this case. Note that, when using the UPDATE method, the identity of the diverted-to user need not be known.

The risk of abuse of this situation seems to be rather low (only the original callee and possibly intermediate diverted-to users see the key, only one direction of the media session is affected, mostly an additional manipulation of the media routing is required). One can argue that this risk is acceptable for the major user categories for which the SDES e2e solution is intended.

9.3.1.3 SDES solution 2

In this sub clause, to guarantee e2e security and avoid the risk of key exposure in call diversion case, an alternative SDES solution is given. If SDES is used, when communication diversion service is trigged, the recipient will generate a new key K2 and a MOD, the parameter MOD is used together with the key generated by the calling UE to generate a new key to protect the media sent from the calling user. The key K2 may also be used as the MOD, then the recipient may only generate one key which is consistent with the normal SDES solution. For example, UE A initiates a call to UE B which has subscribed the CDIV service. When the diversion condition is met, the call is re-invited by the CDIV AS to UE C which is pre-assigned by user B. If SDES is used, UE A includes a key K1 in the SIP message, the AS sends re-invite SIP message which includes K1 to the UE C, thus UE C knows now SDES method is used and it will learn this is a CVID call by the "CAUSE" value, the usage and the specification of the CAUSE parameter refers to RFC 4458 and TS 24.604. Then UE C generates a second key K2 and a MOD, it generates new K1' based on K1 and MOD, and responds with a SIP message including K2 and MOD, when UE A receives the SIP message including K2 and OMD, UE A will generate new K1' based on K1 and MOD the same way as UE C. Thus the communication between UE A and UE C is protected by these two keys, i.e. UE A uses K1' to protect the media sent from UE A to UE C, UE C uses K2 to protect the media sent from UE C to UE A.

If a call is diverted more than once, when the session is successfully established, the latest MOD and the second key from the UE which at last answers the call will be included in the 200 OK message sent to the calling UE, other users will not see the key and MOD used to protect the communication.

Editor's Note: Further work in IETF will be required before this comes to the normative text.

9.3.1.4 Recommended solution

As described in 9.3.1.1, in certain cases of diverted media sessions it cannot be ensured that no endpoint except the one finally terminating the session sees the keys used by the initiator of the media session. It is assumed that this is an acceptable risk for major user categories. Therefore, no additional security mechanisms are specified for CDIV in the SDES based media plane security solution.

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

Therefore no further standardisation is needed for the purpose of CDIV in the SDES-based case.

9.3.2 KMS-based solution

9.3.2.1 General

If KMS is used, the diverted user must be authorized. In normal use of the KMS-based solution when the caller requests a ticket based on the identity of the intended user, a diverted call will very likely fails as the ticket is not valid for the terminating side.

One way to support secure communication of CDIV use case, is to require that the KMS should be able to authenticate the diverted-to user. Another option is to allow the diverted to user to decline the call with an appropriate failure code. This would allow the caller to send a new invite with or without security.

9.3.2.2 KMS-based solution number 1

In this sub clause, a possible solution based on KMS is given. The solution basically works as follows: Firstly, 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 desired recipient. When the recipient subscribes the CDIV service and the diverting condition is met, the call will be forwarded to the pre-assigned user by the CDIV AS. The recipient presents the ticket to the KMS and the KMS returns the keys on which the media security shall be based. When the terminating side requests the KMS to resolve a ticket and return the keys to be used, the KMS interworks with CDIV AS, i.e., KMS sends a inquire request to AS with the identity of initiator, the desired user and the diverted-to user, AS checks whether the diverted-to user is correct, and response to the KMS with the inquire result. 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. Thus the KMS knows whether the diverted-to user is authorized to resolve the ticket or not.

Figure 9.3.2-1 illustrates the procedure of secure CDIV using KMS-based solution, here the CFU service is used as an example to describe the security procedure, the procedure of other CDIV services is in principle the same. The procedure shown in figure 9.3.2-1 is based on signalling flow for a successful communication forwarding unconditional described in TS 24.604 [11]. Note that for simplicity some of the nodes, e.g. CSCFs in IMS network, and messages have been omitted. The detailed signalling flow for a successful communication forwarding unconditional based on an AS providing the forwarding is described in TS 24.604 [11] A1.1.

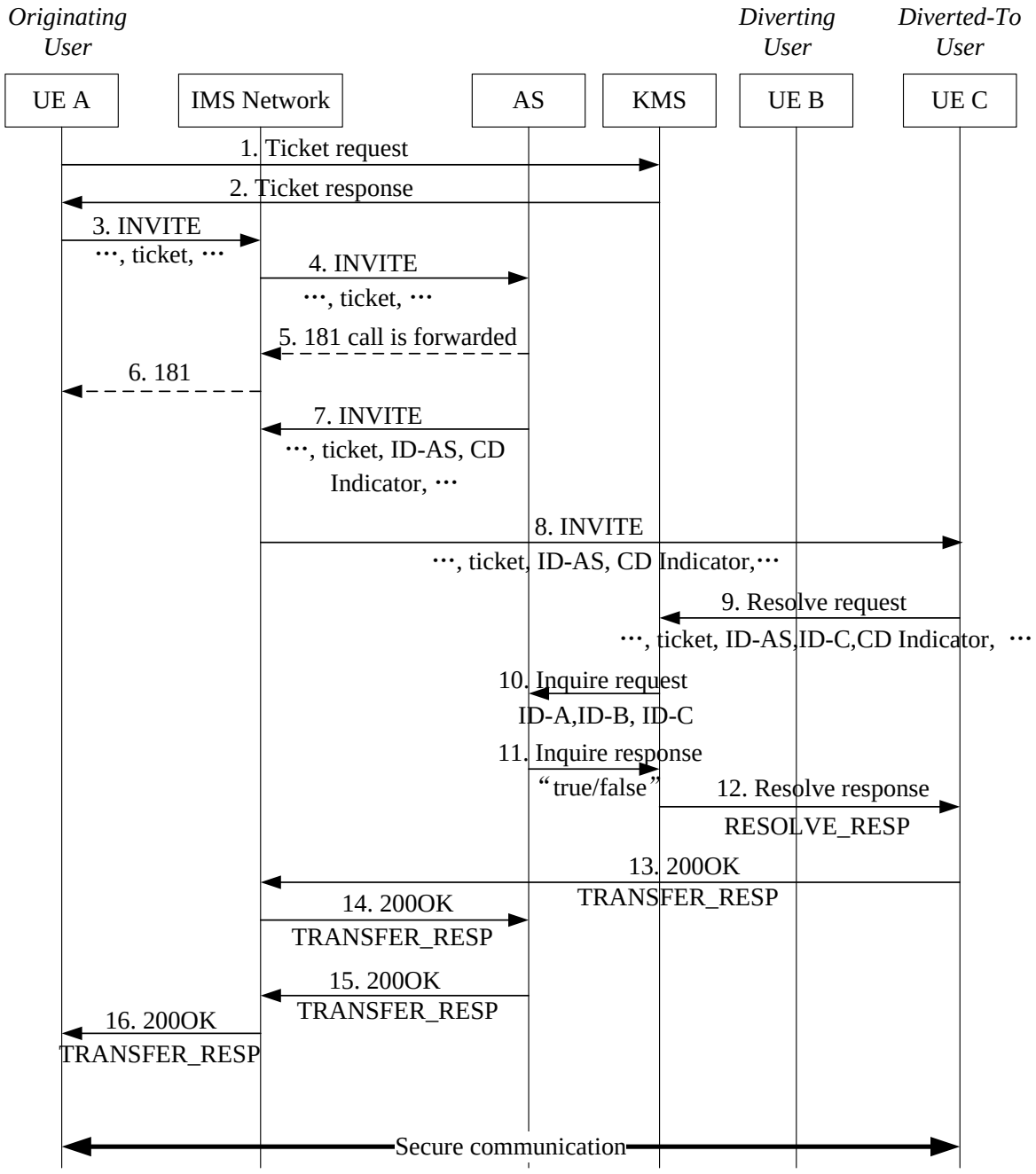


Figure 9.3.2-1: Procedure of secure CDIV using KMS-based solution

Description:

User B has activated the CFU service.

a) UE A requests a ticket from the KMS to communicate with UE B.

b) The KMS generates a corresponding ticket and sends it back to UE A in the ticket response message.

c) UE A sends initial INVITE request including the ticket towards UE B through the IMS network.

d) UE B is subscribed to the CFU service, with the use of the IFC, the INVITE message is forwarded to the AS.

e-f) Procedures for CFU are executed. Depending on the value of subscription option "*Originating* user receives notification that his communication has been diverted (forwarded or deflected)", a 181 (Call Is Being Forwarded) response is sent towards the UE A indicating that the communication is diverted.

g) An INVITE request including URI-C as destination is sent back from the AS to the S-CSCF in the IMS network. Additional the History-Info header, identity of the AS and possibly a CDIV indication is included.

h) The INVITE message is sent to the UE C through the IMS network.

i) UE C sends ticket resolve message to the KMS including ticket, ID-AS, ID-C and possible CDIV indication.

j) The KMS sends a inquire request including ID-A, ID-B based on information about allowed recipients carried in the ticket and the authenticated identity ID-C carried in the resolve request message.

k) The AS checks whether UE C is the correct diverted-to user set by UE B and then sends inquire response message to the KMS to inform the inquire result.

l) If UE C is authenticated as the correct user, the KMS resolves the ticket and returns the keys to UE C in resolve response message. Otherwise, the KMS refuses to solve the ticket.

m-p) UE C sends 200 OK including TRANSFER_RESP message to UE A as specified in TS 33.328 [3].

Thus the communication between UE C and UE A can be protected.

9.3.2.3 KMS-based solution number 2

This clause does not really propose a new solution but describes how current procedures could be used and handled in call diversion scenarios. The handling is described in the following step by step description:

a) Tickets prescribing key forking are used.

b) The caller requests a ticket for the intended receiver. The ticket may include other receivers as well.

c) The caller INVITEs the intended receiver using the requested ticket.

d) The INVITE is diverted with the original ticket.

f) The receiver checks if he is an authorized user of the ticket. If he is, he accepts the INVITE. If not

g) The receiver declines the call and responds with an error message indicating that it is not authorized for a secure call using the ticket in the INVITE. The response includes the identity of the receiver.

NOTE: A user declining the invitation because he is not authorized to use the received ticket will of course not receive any session keys from the KMS. If an authorized receiver declined the invitation but still resolved the ticket he would get session keys unique for him and thus not the same as another user would get, due to the fact that key forking is prescribed.

h) The caller checks the error message and notices that the responder was not authorized for use of the ticket.

i) The caller now checks the identity of the responder and notices that it is different from the identity of the intended receiver.

j) The caller now checks if the responder is authorized and depending on the outcome the caller either continues the secure call or hangs up.

This described handling of call diversion has the benefit that there is no need for new network functionality. Furthermore it leaves the decision on how to handle a diverted secure call to the initiator of the call.

10 Mid-call lawful Interception

10.1 Introduction

10.2 Use cases

10.3 Solutions

10.3.1 Carrying key recovery material in MKI field

Editor's Note: The following provides a potential solution for mid-call interception. Alternative solutions that could be considered may include storing information relating to the call (including keying information) in the P-CSCF, periodic re-keying, or the ekt solution (draft-mcgrew-srtp-ekt) being considered by IETF.

An overall high level concept of mid-call lawful interception for MIKEY-TICKET is shown in Figure 10.3.1-1. Each UE is assigned a secret key S_A that is also known to the KMS. The secret key along with the nonce value N generates a ciphering sequence N', that with MIKEY-TICKET TEK session key produces TEK'. In order to regenerate the TEK, the KMS uses the secret key S_A with the nonce N and TEK'. These values are carried in the SRTP MKI field of the SRTP Header [31].

Although encryption of the SRTP Header is not required, as an added measure of security the nonce N and TEK' portion are encrypted with the encryption key available for securing initiator-KMS TICKET requests. It is noteworthy even if the SRTP MKI field were somehow to be decrypted by an attacker; session secrecy is maintained as the secret key S_A remains unknown.

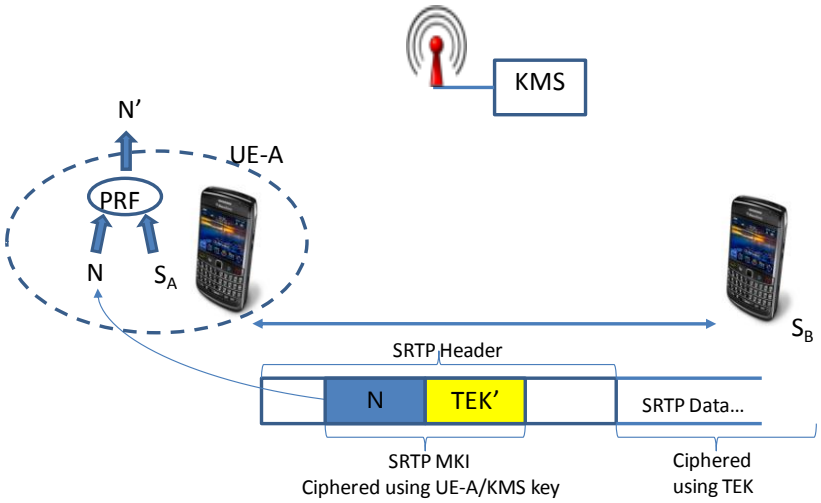


Figure 10.3.1–1: Lawful Intercept enhancement to MIKEY-TICKET

10.3.2 Use locally stored information

A general observation that can be done related to mid-call start of intercept is that to be able to even distinguish the media stream for the user, the network needs to understand what media and codecs are being used, what port numbers are applicable, IP addresses etc are used in a particular stream. There is also a need to correlate the media information with the user (i.e., what signaling information the UE included during call setup).

To be able to activate mid-call start of intercept, the function that is performing this, needs to have the information from the offer / answer exchange setting up the call available. Otherwise, the mid-call start of intercept function will not be

able to associate the user and the related media session (and its media information). This is true regardless if media security is enabled or not.

When media security is applied, media security (both e2e and e2ae) is negotiated through SDP signaling, same as codec negotiation. If the node that is required to perform mid-call start of intercept (e.g., P-CSCF), stores the SDP information from the offer / answer exchange, that node will also have the media security information (such as keys) available in the same location as well (SDES parameters for SDES, or a Ticket for MIKEY). When a mid-call start of intercept is triggered, the entire SDPs are available, and related media security information from the SDES or MIKEY-TICKET can be provided to the LI system (in the same fashion as for an active call setup LI trigger). As the full media security information that was negotiated during the call setup is available, there will be no difference from an LI point of view between LI at session start and LI at mid call.

11 IMS T.38 fax

11.1 Introduction

The transmission of fax over IP networks is specified in the ITU-T recommendation T.38 [33] and uses either TCP or UDP for transport. T.38 allows transmission of fax over IP networks in real time and allows interworking with the legacy PSTN T.30 fax protocol. For the TCP transport, IFP (Internet Fax Protocol) is encapsulated in TPKT. For the UDP transport, IFP data is encapsulated in either UDPTL (UDP Transport Layer) or RTP. The purpose of UDPTL and RTP is to provide sequence numbering and packet redundancy (to cope with packet loss).

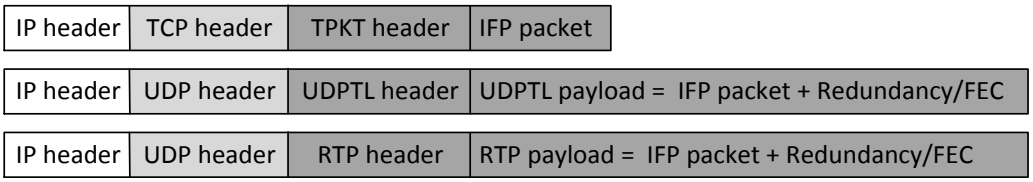


Figure 11.1–1: Packet structures for T.38 fax transmission

UDPTL (UDP Transport Layer) is the predominant means for transporting T.38. For IMS, a profile of T.38 fax is specified in Annex L of TS 26.114 [34]. This profile only supports UDPTL/UDP transport.

A T.38 fax call is established in SIP/SDP similar to how an audio or messaging session is established. The media line is constructed somewhat differently depending on the protocol that is used for transmission.

```
m=audio 49170 RTP/AVP 100 101
a=rtpmap:100 t38/8000
a=rtpmap:101 parityfec/8000
a=...
m=image 49170 udptl t38
a=...
m=image 49172 tcp t38
a=...
```

Figure 11.1–2: Example SDP offering all T.38 fax transmission alternatives (some parts of the SDP offer have been excluded)

11.2 Use cases

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

11.3 Analysis

Three potential solutions for securing IMS T.38 fax calls can be immediately identified:

- Change the IMS transport protocol to IFP/TPTK/TCP and use TLS for protection together with the fingerprint mechanism described in RFC 4572 [35] or MIKEY-TICKET.
- Change the IMS transport protocol to RTP/UDP and use SRTP for protection together with SDES or MIKEY-TICKET.
- Continue to use UDPTL/UDP for transport and use DTLS [36] for protection together with the fingerprint mechanism described in RFC 5763 [37] or MIKEY-TICKET.

Out of these, the last solution is seen as the best one. It uses the same UDPTL/UDP transport as is currently used in IMS and the impact on existing implementations should therefore be small. Implementing e2ae with any of the other solutions would require the IMS UEs to support T.38 fax over IFP/TPTK/TCP or RTP/UDP which is not widely implemented or used. The PSTN GW (or IMS-AGW) would also need to support and perform protocol conversion to and from T.38 fax over IFP/TPTK/TCP or RTP/UDP. A solution based on DTLS similar to the TLS based solution for e2ae protection of MSRP and BFCP is described in detail below.

11.4 E2ae security for T.38 fax using DTLS

This solution is very similar to the e2ae solution for MSRP described in clause 8.3.2.4.2. In this solution, T.38 fax using UDPTL/UDP transport is secured e2ae between IMS UE and IMS-AGW by usage of DTLS (RFC 6347 [36]). The solution leverages IMS control plane security by using self-signed certificates and exchanging the certificate fingerprints via SIP/SDP. Usage of the “P-Asserted-Identity” header provides secure identification of the other endpoint. The parts in RFC 5763 [37] related to NAT and certificate fingerprint checking could potentially be reused.

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

The originating IMS UE specifies “UDP/TLS/UDPTL” and an “a=fingerprint” attribute in the SDP offer. Moreover, the IMS UE adds an SDP attribute "e2ae-security requested by UE" indicating the request for e2ae security to the description of the T.38 fax call. The network inserts the IMS access gateway into the media path. The IMS access gateway terminates DTLS properly, using its own certificate (the fingerprint of this certificate is returned to the originating IMS UE in the SDP answer). From the IMS access gateway in the direction towards the terminating IMS UE, plain UDP may be used on the next hops, assuming that the interfaces are protected.

Editor’s Note: How to indicate the use of secure T.38 is non-security stage 3 issues left for CT1 to decide, but a new proto identifier "UDP/TLS/UDPTL" would require a standards track RFC.

12 Conclusions

12.1 IMS messaging security

This clause includes the conclusions and recommendations for normative work on the media security enhancement for IMS messaging security.

For session based messaging, the following methods are concluded to be specified:

- For end-to access edge security, the TLS based mechanism using fingerprints is to be adopted. In this solution, which leverages IMS control plane security, TLS is terminated in the IMS access gateway controlled by the P-CSCF. IMS UE and network exchange e2ae security indications during IMS registration and session set-up. If both IMS UE and network sent the indications during IMS registration, the mechanism will be applied to every MSRP media stream originated or terminated by the IMS UE unless the UE indicates that it wants to use e2e security. For details see clause 8.3.2.4.2.

- For end-to-end security, the PSK-TLS with MIKEY-TICKET based mechanisms as specified in clause 8.3.1.2 are to be adopted.

There are no end-to-end security solutions for session based messaging that leverage IMS control plane security.

For immediate messaging, the following methods are concluded to be specified:

- a solution leveraging IMS control plane security, current IMS signalling mechanisms are to be reused as defined in TS 33.203.
- For end-to-end message security, the S/MIME extension using MIKEY-TICKET according to clause 8.3.1.1 are to be adopted.

12.2 IMS conferencing security

Editor's Note: Conclusions relating to the end-to-end case not leveraging IMS control plane security are ffs

This clause includes the conclusions and recommendations for normative work on the media security enhancement for IMS conferencing security.

For conferencing security leveraging IMS control plane security, the following methods are concluded to be specified:

- For RTP-based media, the SDES-based methods for e2ae and e2e specified in the main body of Ts 33.328 are applied also to conferencing security. This is possible as group keys are not to be used. Instead, the conference server specifies individual keys per participant for all media streams it sends out. Because e2ae may suffice in many cases when the conferencing server resides in the operator network SRTP support in the conferencing server is optional.
- For BFCP, the same e2ae methods as for session-based messaging leveraging IMS control plane security are to be specified. The Conference Server optionally supports TLS for BFCP and for MSRP (for messaging conferences).

12.3 IMS call diversion security

This clause includes the conclusions and recommendations for normative work on the media security enhancement for IMS call diversion security.

No additional security mechanisms are specified for CDIV in the SDES based media plane security solution.

CDIV in the KMS based media security solution is to be handled using existing procedures as described in clause 9.3.2.3. In order to avoid the additional signalling roundtrip and ticket request, it is recommended to make tickets resolvable by everyone. This is done by setting the intended recipient to the wild carded identity ?@? when the ticket is created.

12.4 Mid-call start of intercept

It is concluded that mid-call start of intercept can be achieved for media security based on the local stored information as described in Clause 10.3.2.

12.5 IMS T.38 fax security

This clause includes the conclusions and recommendations for normative work on the media security enhancement for IMS T.38 fax security. The following method is concluded to be specified:

- For end-to access edge (e2ae) security, the DTLS based mechanism using fingerprints is to be adopted. In this solution, which leverages IMS control plane security, DTLS is terminated in the IMS access gateway controlled by the P-CSCF. IMS UE and network exchange e2ae security indications during IMS registration and session set-up in the same way as for RTP and MSRP based media. It is done independently from the indication of support for e2ae security for RTP or MSRP based media, and uses its own indications. For details see clause X.4.

Annex A: IANA considerations

A.1 IANA assignments

This clause defines several new values for the namespace Prot Type defined in IETF RFC 3830 [19]. IANA is requested to record the assignments in Table A.1 to the namespace Prot Type in the MIKEY payload registry. The Prot Types can be used by any MIKEY mode.

Table A.1: Prot Type (Additions)

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

Editor's Note: 3GPP can only make these registrations if draft-arkko-mikey-iana becomes an RFC. Currently an RFC is needed to register new values. The draft is AD-sponsored and in last call (since 30 March 2011).

TLS: This Prot Type provides a pre-shared key (TEK) to be used in pre-shared key ciphersuites for (D)TLS. As the TLS handshake includes key-management and derives a TLS session keys, the TEK can be used to set up several TLS sessions. As the TLS handshake includes negation of parameters, security policies (SP payloads) shall not be associated with the Crypto Session (CS).

PSK/MIME: This Prot Type provides keys to be used to protect MIME content as specified in Annex B.

Editor's Note: It is ffs which keys to use (TEK, encr_key, auth_key, salt_key) and whether Security Policies (SP payloads) are needed.

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

Annex B: Pre-shared key MIME protection

Secure/Multipurpose Internet Mail Extensions (S/MIME), defined in IETF RFC 5751 [20], is a standard for encryption and signing of MIME encoded data. S/MIME uses Cryptographic Message Syntax (CMS), defined in IETF RFC 5652 [21], to cryptographically protect MIME entities. Unfortunately, S/MIME was designed for public key cryptography and does not specify how a MIME entity can be encrypted and authenticated using a pre-shared key. However, extending S/MIME to also support symmetric crypto is not a major issue since CMS already defines the necessary message constructs and algorithms.

B.1 New smime-type parameter

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

Table B.2: smime-type (addition)

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

AuthEnvelopedData is a CMS type defined in IETF RFC 5083 and is intended to be used with authenticated encryption modes, such as AES-CCM and AES-GCM. This allows us to both authenticate and encrypt arbitrary data using a single key. The key is generated at random and is transported alongside the protected data in a RecipientInfo sub-element (in encrypted form). Table B.3 shows the authenticated encryption algorithms supported in this specification.

Table B.3: Authenticated encryption algorithms

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

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

Editor's note: Whether we can continue using the MIME type application/pkcs7-mime when the new smime-type parameter is introduced is FFS. It might be necessary to register a new MIME type application/X with IANA (in the vendor tree where vendor is 3GPP).

B.2 Creating an Auth-Enveloped message

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

a) The MIME entity to be protected is prepared according to Section 3.1 in S/MIME [20].

b) The MIME entity and other required data is processed into a CMS object of type AuthEnvelopedData. The key for the desired content-authenticated-encryption algorithm is generated at random and encrypted for each recipient. The details of this encryption depend on the type of key management technique used. Section X explains how the key is transported using MIKEY-TICKET.

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

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

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

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

    smime-type=auth-enveloped-data;

    name=smime.p7m

Content-Transfer-Encoding: base64

Content-Disposition: attachment; filename=smime.p7m

rfvbnj756tbBghyHhHUujhJhjH77n8HHGT9HG4VQpfyF467GhIGfHfYT6

7n8HHGghyHhHUujhJh4VQpfyF467GhIGfHfYGTrfvbnjT6jH7756tbB9H

f8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4

0GhIGfHfQbnj756YT64V
```

B.3 Using MIKEY-TICKET to transfer the protection key

The key used to protect the MIME entity is transferred in the RecipientInfo field of AuthEnvelopedData. This field can have several different formats and one that is particularly suited to be used together with MIKEY-TICKET is OtherRecipientInfo. This type has the following ASN.1 definition:

```
OtherRecipientInfo ::= SEQUENCE {
    oriType OBJECT IDENTIFIER,
    oriValue ANY DEFINED BY oriType }
```

A new oriType with an oriValue of type OCTET STRING is defined for MIKEY-TICKET:

id-ori-mikey OBJECT IDENTIFIER ::= { x y z }

The value field contains a TRANSFER_INIT message with a single Crypto Session of type PSK/MIME. The TEK associated with the CS is the key used as input to the authenticated encryption algorithm. Contrary to what is usually done, the TEK is not derived from a TGK/GTGK carried in the TICKET. Instead the TEK is carried inside a KEMAC payload that the sender adds to the TRANSFER_INIT message. The advantage of transporting the TEK instead of deriving is that it can be generated beforehand, independent of the TRANSFER_INIT message.

Note that since the TRANSFER_INIT message is replayed protected, the protected MIME entity is replayed protected as well.

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

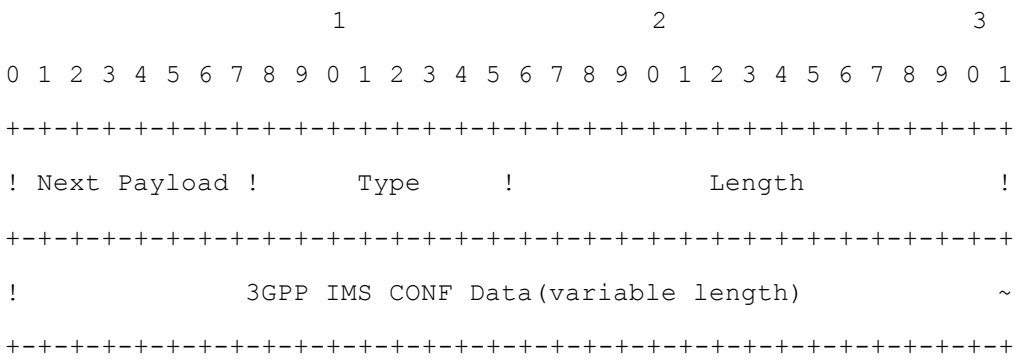
Editor's note: The new object identifier {x y z} must be registered under some suitable subtree

Annex C: MIKEY general extension payload for 3GPP ad-hoc conferencing

This Annex specifies a new MIKEY General Extension Payload to transport the participant list in an ad-hoc conference established according to Clause 5.3.3 (KMS-based solution) in this document.

C.1 Payload format

The 3GPP IMS CONF Type (Type TBD) formats the MIKEY General Extension payload as follows:



- Next Payload and Length are defined in Section 6.15 of RFC3830
- Type (8 bits) identifies the type of the General Extension Payload (see Section 6.15 of RFC3830). This Annex adds a new type. It specifies the use of Type TBD for 3GPP IMS conferencing.
- 3GPP IMS CONF Data (variable length): defines a variable length Data field. This field is constructed by zero or more ID payloads (see Section 6.7 of RFC3830).

  3GPP IMS CONF Data = {IDpartic}

  IDpartic contains the identity of a user that is authorized to join the conference.

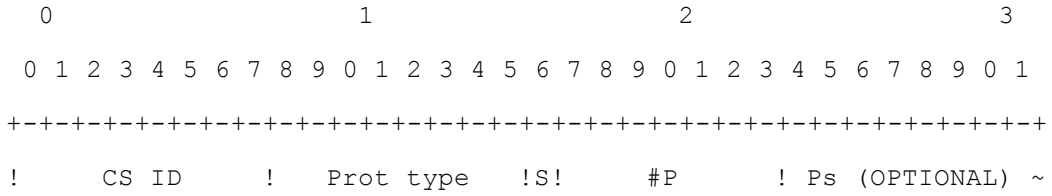
Editor's note: The 3GPP IMS CONF type must be registered with IANA

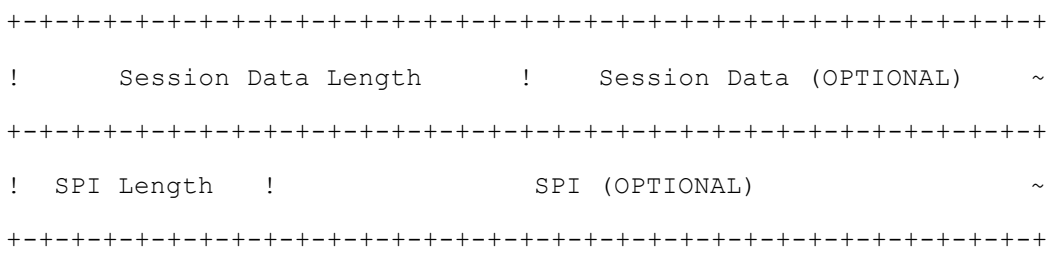
Annex D: Setup of TLS-PSK using MIKEY

Although MIKEY [19] only specifies how to establish key data and algorithm settings for the SRTP protocol, it can easily be extended to carry the security parameters needed for setting up almost any kind of security protocol. This Annex describes how MIKEY is used to establish a PSK to be used in a TLS-PSK handshake.

D.1 The TLS Prot Type

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





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

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

Editor's note: The Prot Type TLS must be registered with IANA

D.2 Establishing a TLS connection

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

- TLS client/server role: the role of each peer is negotiated by means outside of MIKEY (e.g. as part of the establishment of the transport association in SDP). Typically, the client (server) in the transport protocol assumes the role of client (server) in the TLS protocol.
- Set of allowed TLS Ciphersuites: any of the TLS_PSK_* and TLS_DHE_PSK_* Ciphersuites can be used (defined in RFC 4279 and RFC 4285). Other ciphersuites are allowed but they may require additional parameters that are not provided by the CS.
- PSK identity: this value is not used. The PSK identity is set to the empty string by the client and is ignored by the server.
- PSK identity hint: this value is not used. The identity hint is an optional value provided by the server in the server hello message.

- PSK: The PSK is the TEK associated with the CS. The SPI in the CS points to a TGK or GTGK from which the TEK is derived using the CS ID (and some other parameters). The SPI could also point to a TEK directly.

D.3 Usage with SDP

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

RFC 5246 describes how the key-mgmt attribute is used to perform a MIKEY exchange in SDP and how an m-line can be mapped to set of SRTP CSs (one for each SSRC). If the key-mgmt attribute is used at session level then the MIKEY exchange contains CSs for all the m-lines in the SDP and the mapping is based on the order of the m-lines. If the key-mgmt attribute is used at the media level then the CSB only contains the CSs for that m-line. Mixing of session and media level attributes is allowed by 5246 but the expected behaviour is not well defined. Another restriction is that the offerer must know how many SSRCs that the answerer will use for a particular m-line.

The mapping between an X/TLS/Y m-line and a TLS CS is done in the same way as the mapping between and SRTP m-line and a set of SRTP CSs. The only difference is that in X/TLS/Y case, the set is reduced to a single element.

Annex E: MIKEY-TICKET profile for pre-shared key MIME protection

The MIKEY-TICKET profile for pre-shared key MIME protection is the same as the profile for IMS Media Plane security (see Annex D of TS 33.328 [3]) except for a few minor differences. These differences are explained below.

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

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

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

- The (pre-generated) TEK value that was used to protect the MIME entity and that is associated with the CS shall be included inside a KEMAC payload. The TEK has associated salt or key validity period.

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

The Ticket Resolve exchange is unchanged

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

- The F flag shall be set to 0 indicating that TRANSFER_RESP should not be sent

- The G shall be set to 0 indicating that the Responder should not generate RANDRi

- The I shall be set to 0 (no-forking) unless proof-of-origin is required for the MIME entity

- The L shall be set to 1 indicating that the initiator may supply session keys

- The KEMAC payload in the TICKET shall not contain any keys besides MPKi since this is the only key that is used (the TEK is generated by the initiator and is transported outside of the TICKET in a separate KEMAC payload)

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

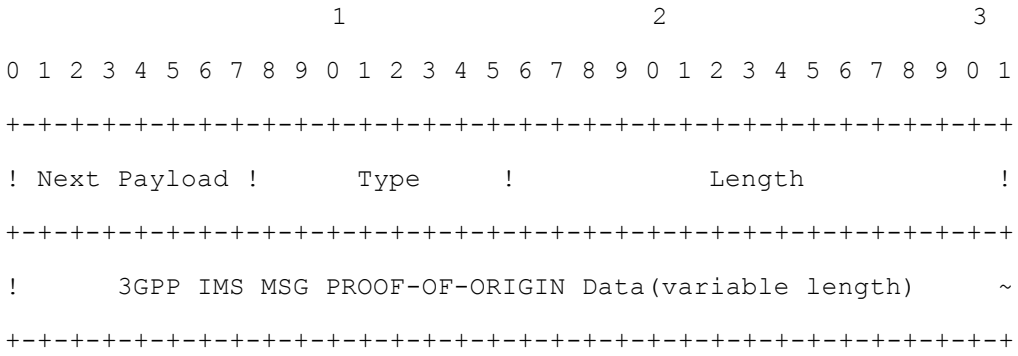
Editor's note: Proof-of-origin requires that Initiator Data is included in the TICKET payload which in turn requires that forking is enabled. However, forking was originally intended to be used in the cases where the responder is able to send a TRANSFER_RESPONSE, and the MIKEY-TICKET was written with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

Annex F: MIKEY general extension payload for message proof-of-origin

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

F.1 Payload format

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



- Next Payload and Length are defined in Section 6.15 of RFC3830
- Type (8 bits) identifies the type of the General Extension Payload (see Section 6.15 of RFC3830). This Annex adds a new type. It specifies the use of Type TBD for 3GPP IMS MSG PROOF-OF-ORIGIN.

  3GPP IMS MSG PROOF-OF-ORIGIN Data (variable length): contains the data whose origin needs to be asserted. The interpretation of the data is application/context specific (data could for example be the hash of a much longer message, where the hash algorithm is defined by the application/context)

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

Annex G: Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2010-06					Report skeleton created		0.0.0
2010-07					Output of SA3#60	0.0.0	0.0.1
2010-11					Output of SA3#61	0.0.1	0.0.2
2011-02					Output of SA3#62	0.0.2	0.0.3
2011-06					Output of SA3#63	0.0.3	0.0.4
2011-06					Output of SA3#63 with correction to title of section 8.3.2	0.0.4	0.0.5
2011-08					Draft output of SA3#64	0.0.5	0.0.6
2011-09					Final output of SA3#64	0.0.6	0.0.7
2011-11					Output of SA3#65	0.0.7	0.0.8
2011-12					Output of SA3#63 with addition of paragraph to section 6.3 which was accidentally deleted when creating version 0.0.6.	0.0.8	0.0.9
2012-02					Output of SA3#66	0.0.9	0.0.10
2012-06					Output of SA3#67	0.0.10	0.0.11
2012-07					Output of SA3#68	0.0.11	0.0.12
2012-09	SA#57				Presented for information	0.0.12	1.0.0
2012-11					Output of SA3#69	1.0.0	1.1.0
2013-01					Output of SA3#70 : the implemented pCRs are documents S3-130131 and S30196	1.1.0	1.2.0
2013-03	SA#59				Version for approval	1.2.0	2.0.0