3GPP TR 29.828 V0.2.0 (2013-08)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Study on Extended IMS media plane security features and TCP-related NAT traversal support; IMS H.248 profiles aspects (Release 12)

MCC selects keywords from stock list.

Keywords
<keyword[, keyword]>

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.

1 Scope

The present document investigates the IMS H.248 profiles requirements and procedures to support the stage 2 requirements specified in 3GPP TS 33.328 [2] for Extended IMS media plane security features.

This includes in particular the following aspects:

1. Provide end-to access edge protection of session based messaging (MSRP) traffic using TLS and certificates fingerprints exchanged over SDP;
2. Provide end-to-end protection of session based messaging (MSRP) traffic using TLS;
3. Provide end-to access edge protection of BFCP based traffic, using TLS and certificates fingerprints exchanged over SDP;
4. Provide optional support of TLS protection of BFCP and MSRP based traffic at the Conference Server.
5. Analyse requirements and procedures for TCP bearer control and related NAT traversal support.

   NOTE: this aspect is not specific to media security and may result in normative work via another work item.
6. Provide support of TCP-based IP transport connections for TLS security sessions, which includes possible NAT traversal support during the TCP connection establishment phase, possible correlations between the establishment (and release) events of TCP connections with TLS session establishment (and release).

This study will cover:

- Identification of the key issues and the main design considerations that should drive the definition of stage 2 requirements and procedures for the Iq, Ix and Mp profiles;
- Identification of the requirements and procedures for the Iq, Ix and Mp profiles for support of end-to-access edge and end-to-end media security for session-based messaging (MSRP [6]) and conferencing (BFCP [16]);
- Identification of the ITU-T H.248 extensions necessary to fulfill the 3GPP requirements and identification of potential missing gaps that should be taken into account by ITU-T Q3/16;
- Conclusions and Recommendations for the normative work.

The results of this study will be used to identify the changes required in the 3GPP specifications to support Extended IMS media plane security.

2 References

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

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

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

[2] 3GPP TS 33.328: "IMS Media Plane Security".

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

[4] 3GPP TS 24.247: "Messaging service using the IP Multimedia (IM) Core Network (CN) subsystem - Stage 3".

[5] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

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

[7] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

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

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

[10] IETF RFC 4976: "Relay Extensions for the Message Sessions Relay Protocol (MSRP)"

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

[12] IETF RFC 4145: "TCP-Based Media Transport in the Session Description Protocol (SDP)".

[13] Draft draft-ietf-simple-msrp-sessmatch-10: "Session Matching Update for the Message Session Relay Protocol (MSRP)"

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

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

[16] IETF RFC 4582: "The Binary Floor Control Protocol (BFCP)".

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

[18] GSM Association RCC 0.7: "Rich Communication Suite 5.1 Advanced Communications Services and Client Specification, Version 1.0, August 2012".

[19] OMA-TS-SIMPLE_IM-V2_0-20120731-C: "Instant Messaging using SIMPLE Candidate Version 2.0 – 31 Jul 2012".

[20] IETF RFC 793: "Transmission Control Protocol".

[21] 3GPP TS 24.147: "Conferencing using the IP Multimedia (IM), Core Network (CN) subsystem".

[22] ETSI TS 183 018 V3.5.2 (2010-01): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control: H.248 Profile Version 3 for controlling Border Gateway Functions (BGF) in the Resource and Admission Control Subsystem (RACS); Protocol specification".

[23] ITU-T Recommendation H.248.37 (06/2008): "Gateway control protocol: IP NAPT traversal package".

[24] ITU-T Recommendation H.248.84 (07/2012): "Gateway control protocol: NAT traversal for peer-to-peer services".

[25] 3GPP TR 33.830: "Feasibility study on IMS firewall traversal".

3 Definitions, symbols and abbreviations

3.1 Definitions

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

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

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

TLS-client: the entity that initiates a TLS session establishment to a server (see IETF RFC 5246 [7]).

TLS-server: the entity that responds to requests for TLS session establishment from clients (see IETF RFC 5246 [7]).

TLS endpoint: either a TLS-client or a TLS-server.

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].

BFCP	Binary Floor Control Protocol
e2ae security	End-to-access-edge security
e2e security	End-to-end security
IMS-AGW	IMS Access Media Gateway
IMS-ALG	IMS Application Level Gateway
IM CN	IMS Core Network
MSRP	Message Session Relay Protocol

4 Key issues and Design considerations for Extended IMS media plane security features

Editor's Note: this clause intends to identify the key issues to address and the main design considerations that should drive the definition of stage 2 requirements and procedures.

4.1 Media security for Session based messaging (MSRP)

4.1.1 General design considerations

IMS messaging concepts and procedures are specified in 3GPP TS 23.228 [3] (see subclause 5.16), 3GPP TS 24.247 [4] and 3GPP TS 24.229 [5].

3GPP TS 33.328 [2] specify IMS media plane security mechanisms for session based messaging (MSRP) for both e2ae protection and e2e protection. Integrity and confidentiality protection for MSRP based media is achieved by TLS protection.

NOTE: Immediate messaging (i.e. page-mode messaging) is out of the scope of eMEDIASEC.

The salient points of MSRP based media security are: (see 3GPP TS 33.328 [2] for a comprehensive description):

a) support of e2ae protection or e2e protection of MSRP-based media is optional for UEs and the network; support for IMS media integrity and confidentiality protection is mandatory in an IMS UE and IMS-AGW supporting e2ae protection of MSRP-based media. IMS media confidentially protection should be used when IMS media plane security is used, while the use of IMS media integrity protection is optional.

b) indications of UE and network support for e2ae security for MSRP are exchanged between the UE and the P-CSCF during the IMS registration in the same way as for RTP based media. MSRP media security uses its own indications "e2ae- security for MSRP supported by the UE" and "e2ae-security for MSRP supported by the network". If both the IMS UE and the network indicate support for e2ae security for MSRP during the IMS registration, then the IMS UE (for an IMS originating session set-up) or the P-CSCF (for an IMS terminating session set-up) shall request e2ae security for MSRP media streams to be established, unless e2e security is used. If compatibility with GSMA RCS 5.1 [18] is desired, the indication of support for e2ae security during the IMS registration is not a necessary prerequisite for the use of e2ae security.

c) for e2ae protection of MSRP based media:

- media security is provided between the IMS UE and the IMS-AGW;
- when the SIP-level MSRP session setup is completed, the TCP transport connection and TLS security seesion shall be established between the IMS UE and the IMS-AGW;
- key management is based on the ciphersuites and session keys negotiated via the TLS handshake protocol between the UE and the IMS-AGW. Mutual authentication during the TLS handshake protocol is achieved using certificates, with the certificate fingerprints being transmitted using the SDP fingerprint attribute in the SIP/SDP offer-answer exchange between the UE and the P-CSCF (IMS-ALG);
- the IMS-ALG needs to be enhanced to be able to terminate the key management protocol, as well as handle indications, which are specific to e2ae security and are inserted in SIP messages.
- the IMS-AGW needs to be enhanced to be able to originate or terminate TLS protecting MSRP. The Iq interface between the IMS-ALG and the IMS-AGW needs to be enhanced to be able to transport parameters related to the management of TLS cryptographic contexts.
- media security context update is not used with e2ae security.

d) For e2e protection of MSRP based media:

- media security is provided between an IMS UE and a remote IMS or non-IMS UE or MRFP (conference server);
- media security is achieved through the same KMS and ticket concept that is used for RTP traffic. The key management mechanisms are defined by MIKEY-TICKET [11]. The established key is used to setup a TLS-PSK tunnel between the two parties. TLS media packets are then forwarded transparently by any nodes present in the media path (e.g. IMS-AGW, TrGW);
- e2e protected MSRP sessions are set-up without IMS-ALG support, which means that such sessions can be set-up in networks not providing the IMS-ALG functionality in the P-CSCF.

4.1.2 Assumptions and limitations for MSRP support

IMS session-based messaging is supported as specified in 3GPP TS 24.247 [4] and 3GPP TS 24.229 [5], i.e. using:

- from Rel-6 onwards:
  - the Message Session Relay Protocol (MSRP) as defined in IETF RFC 4975 [6];
- additionally, from Rel-8 onwards:
  - MSRP as extended by IETF RFC 6135 [8] (mandatory support);
  - MSRP as extended by IETF RFC 6714 [9] (mandatory support).

The following MSRP recommendations are not required to be supported per existing 3GPP specifications:

- IETF RFC 4976 [10] (MSRP relay) defines a MSRP protocol extension
- draft-ietf-simple-msrp-sessmatch-10 [13] (Session Matching Update for MSRP) – obsolete

However, draft-ietf-simple-msrp-sessmatch-10 [13] is used by the GSMA [18] and OMA [19] specifications that extend IMS for MSRP messaging.

Table 4.1.2-1 summarizes in which 3GPP, GSMA and OMA specifications those MSRP extensions are used.

Table 4.1.2-1: MSRP usage in 3GPP, GSMA and OMA

	IETF RFC 4975 [6] (MSRP)	IETF RFC 4976 [10] (MSRP relay)	IETF RFC 6135 [8] (Alternative connection model for MSRP)	IETF draft-ietf-simple-msrp-sessmatch-10 [13] (Session Matching Update for MSRP)	IETF RFC 6714 [9] (CEMA for MSRP)
3GPP TS 24.247 [4] (Rel-8 onwards)	x	-	x	-	x
OMA-TS-SIMPLE_IM-V2 [19]	x	-	x	x	-
GSMA RCC 0.7 [18]	x	-	x	x	-

IETF RFC 6135 [8] ("COMEDIA for MSRP") enables support of MSRP clients located behind firewalls by enabling the SIP/SDP level negotiation of the TCP connection setup direction (by using the IETF RFC 4145 [12] "a=setup:" SDP attribute).

IETF RFC 6714 [9] ("CEMA for MSRP") defines a mechanism enabling intermediate nodes (e.g. MGW) to pass MRSP messages without having to modify them, and also enabling MGWs to pass TLS encrypted MSRP messages transparently. The applicability of the related MSRP procedural modifications is negotiated on SIP level via the new SDP attribute "a=msrp-cema". If the negotiation indicates that not both peers support the MSRP procedural modifications, a fallback to IETF RFC 4975 [6] applies and a MGW needs to behave as MSRP B2BUA to pass MSRP; for TLS-encrypted MSRP, the MGW also needs to decrypt and re-encrypt TLS (TLS B2BUA). IETF draft-ietf-simple-msrp-sessmatch-10 [13] provides an alternative mechanism to avoid that a MGW that passes MSRP messages needs to modify them, which was obsoleted in IETF RFC 6714 [9].

There are a number of IETF RFCs and documents, related to the (SIP based) application control of MSRP-(over-TLS-)over-TCP connections. Figure 4.1.2.1 aims to provide an overview over MSRP related IETF standards.

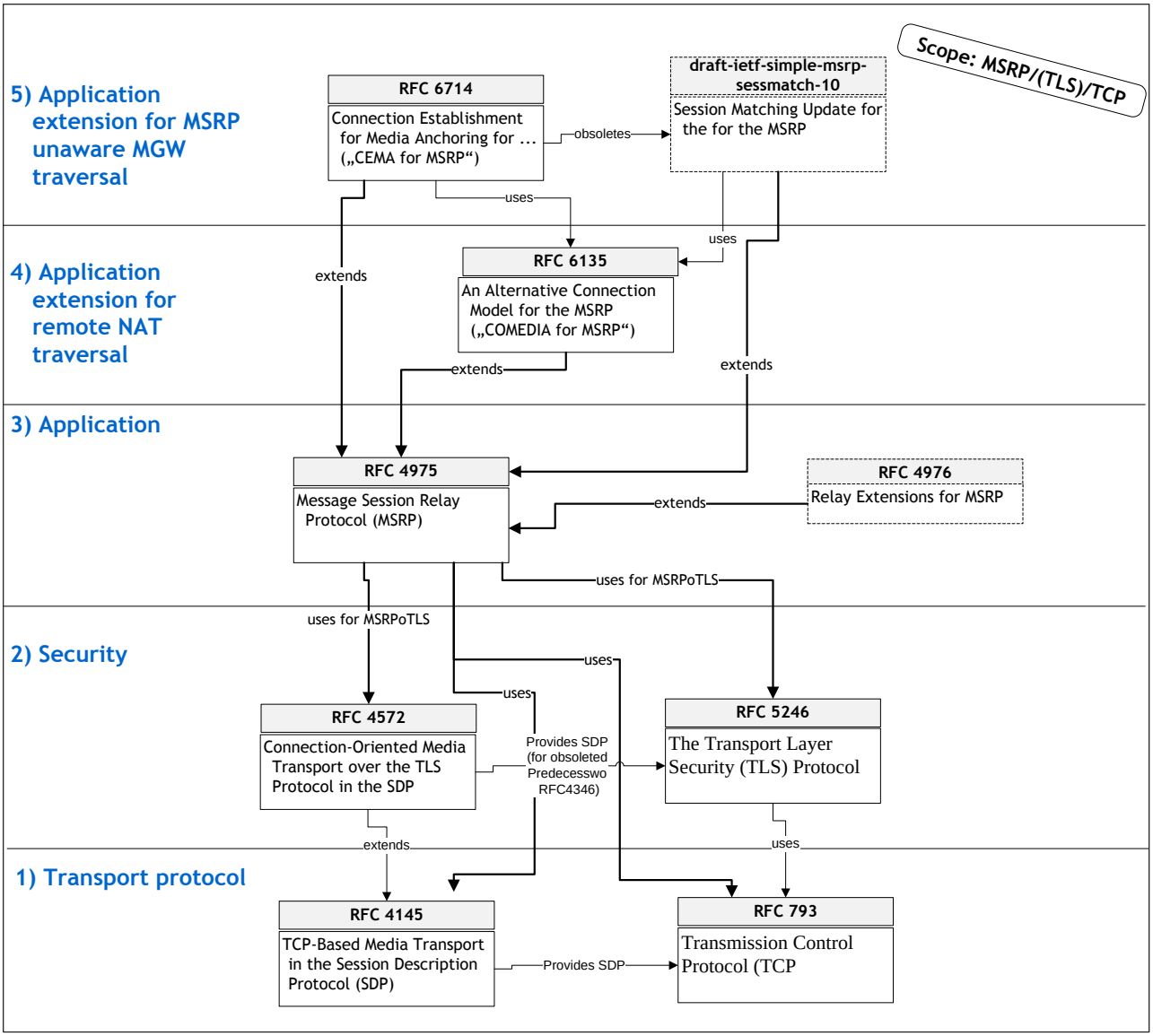

Figure 4.1.2.1: Overview of IETF document concerning NAT-T supported MSRP-(over-TLS-)over-TCP services, as typically used in SIP-based application control signalling

The present study will investigate e2ae and e2e security for MSRP implementations supporting IETF RFC 4975 [6] in combination with IETF RFC 6135 [8] ("COMEDIA for MSRP") and either IETF RFC 6714 [9] ("CEMA for MSRP") or draft-ietf-simple-msrp-sessmatch-10 [13].

Scenarios without support of IETF RFC 6135 [8] (e.g. for support of pre-Rel-8 3GPP UEs) should be considered only as an option within the 3GPP H.248 profiles.

4.1.3 Scenarios in scope

TLS shall be supported over TCP transport (see IETF RFC 793 [20]). Support of TLS over other reliable transport protocol e.g. SCTP is not required and thus not considered as part of eMEDIASEC.

The following scenarios shall be supported as part of eMEDIASEC:

a) TLS to non-TLS interworking for e2ae protection of MSRP-based media:

- e2ae only applies to the IMS-AGW; application of e2ae security is not visible to the TrGW or MRFP.

- this corresponds to an MSRP session between an IMS UE with e2ae security applied, towards another IMS UE without e2ae applied or a non-IMS UE or an MRFP;
- this can also correspond to a local MSRP session with e2ae applied for both UEs, where the figure only depicts a 'half call model".

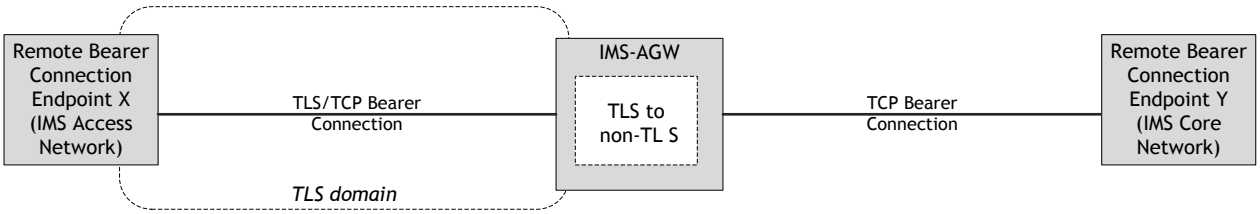

Figure 4.1.3.1: TLS (IMS Access Network) to non-TLS (IMS Core Network) interworking for e2ae protection of MSRP-based media

NOTE 1: Whether the IMS-AGW is MSRP-agnostic or MSRP-aware is discussed in a dedicated subclause and thus not depicted in the figure.

NOTE 2: TLS-based protection can also be used inside the core network. In this case, when e2ae security is used, TLS has to be established also from the IMS-AGW towards the IMS Core Network. Both TLS sessions are independent. This use case is documented in TS 33.328 [2] but not further described in this specification.

Editor's Note: it is FFS whether support of TLS-based protection inside the core network adds any specific requirement beyond those to be defined for TLS-based protection towards the IMS access network, and if so, whether this should be covered or not by the IMS H.248 profiles.

b) Transparent TLS packets forwarding for e2e protection of MSRP-based media:

- this corresponds to an MSRP session between an IMS UE and e.g. another IMS or non-IMS UE or an MRFP with e2e security applied;
- the MGW can be an IMS-AGW or a TrGW.

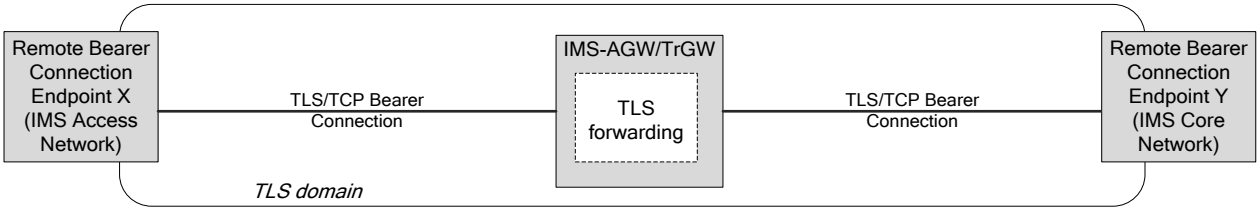

Figure 4.1.3.2: Transparent TLS packets forwarding for e2e protection of MSRP-based media

c) TLS to non-TLS interworking for e2e protection of MSRP-based media:

- the MRFP (conference server) can support TLS for MSRP, i.e. originate/terminate TLS traffic with e2e media security from/to a remote MSRP sender/receiver;

- the MRFP can also communicate with other remote bearer connection endpoints, with or without e2e media security; if TLS is also used towards other remote endpoints, each TLS session is independent from the other (i.e. different keys).

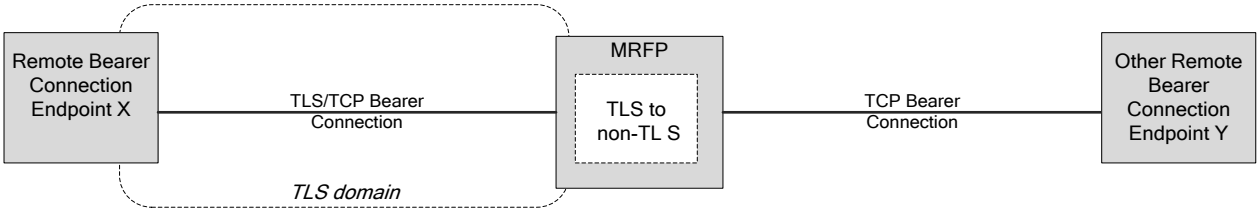

Figure 4.1.3.3: TLS to non-TLS interworking for e2e protection of MSRP-based media at the MRFP

In the above scenarios, the IMS UE (with e2ae or e2e security applied) may be located behind a remote firewall/NAT device. i.e. NAT-Traversal should be considered.

NOTE 3: Support of NAT traversal (at layers L4/L3) is basically agnostic to any higher layer (i.e., L4+) security sessions, hence not specific to eMEDIASEC.

4.1.4 MSRP-agnostic vs MSRP-aware mode

Table 4.1.4-1 discusses the eMEDIASEC relevant IETF documents from perspective of end-to-end connectivity aspects (such as NAT-T), independent of media security usage or not.

Table 4.1.4-1: MSRP awareness concerning end-to-end user plane connectivity

	Originator of TCP connection setup	MSRP client takes destination address for TCP connection setup from	Session matching at MSRP client between SDP path and path in MSRP messages includes address information	MGW needs to insert own address into path in MSRP messages	Controller needs to modify SDP path attribute	MSRP relays supported	Support of extension is negotiated
IETF RFC 4975 [6] (MSRP)	SDP offerer	SDP MSRP path attribute	Yes	Yes	Yes	Yes	-
IETF RFC 6135 [8] (Alternative connection model for MSRP)	Negotiated via IETF RFC 4145 [12] SDP setup attribute	Depends on whether other extensions below are used in combination					Yes (fallback to IETF RFC 4975 [6] if setup attribute is missing)
draft-ietf-simple-msrp-sessmatch-10 [13] (Session Matching Update for MSRP)	Depends on whether IETF RFC 4975 [6] is used in combination	SDP MSRP path attribute	No	No	Yes	Yes	No (no interoperability with IETF RFC 4975 [6] MSRP client)
IETF RFC 6714 (CEMA for MSRP) [9]	Negotiated via IETF RFC 4145 [12] SDP setup attribute (Parallel usage of IETF RFC 4975 [6] is mandated)	SDP c-line and m-line	Yes	No (Yes if fallback to to IETF RFC 4975 [6] occurs and is supported)	No	Yes, by fallback to IETF RFC 4975 [6]	Yes, via new SDP CEMA attribute

Based on the assumptions and limitations identified in subclause 4.1.2 and the Table 4.1.4-1, it is concluded that:

a) the IMS-AGW shall support application-agnostic interworking for TLS-based e2ae scenarios, i.e. transparent forwarding of application (i.e. MSRP) data;

- this suffices for support of e2ae security of MSRP based media when IETF RFC 6714 [9] or draft-ietf-simple-msrp-sessmatch-10 [13] is supported by both ends (e.g. between Rel-8 onwards IMS UEs);

b) the IMS-AGW may support application-aware interworking for TLS-based e2ae scenarios, i.e. modifying the Path parameter in application (i.e. MSRP) data:

- this enables to support e2ae security of MSRP based media when neither IETF RFC 6714 [9] nor draft-ietf-simple-msrp-sessmatch-10 [13] are supported by both ends (e.g. interoperation with pre-Rel-8 IMS UEs only supporting IETF RFC 4975 [6].

Besides, the IMS-AGW and TrGW shall support application-agnostic (i.e. transparent) forwarding of TLS packets for e2e scenarios.

The MRFP is already MSRP aware prior to eMEDIASEC.

4.2 Media security for conferencing (BFCP)

4.2.1 General design considerations

IMS conferencing concepts and procedures are specified in 3GPP TS 23.228 [3], 3GPP TS 24.147 [21] and 3GPP TS 24.229 [5].

3GPP TS 33.328 [2] specify IMS media plane security mechanisms for BFCP as used in IMS conferencing for both e2ae protection and e2e protection. Integrity and confidentiality protection for BFCP media is achieved by TLS protection.

The salient points of BFCP based media security are: (see 3GPP TS 33.328 [2] for a comprehensive description):

a) e2ae security shall be supported in the same way as for MSRP (see subclause 4.1.1), with only the following differences:

   - e2ae security for BFCP uses individual indications "e2ae-security for BFCP supported by the UE" and "e2ae-security for BFCP supported by the network" during the IMS registration;

   - In the SDP, security for a BFCP media stream is specified by using the transport "TCP/TLS/BFCP".

b) e2e protection of BFCP media may be supported between the IMS UE and MRFP (conference server) in a similar way as for MSRP-based traffic, i.e. using a TLS tunnel established with MIKEY-TICKET .

4.2.2 Assumptions and limitations for BFCP support

BFCP as used for IMS conferencing is supported as specified in 3GPP TS 24.147 [21] and 3GPP TS 24.229 [5], i.e. using:

- from Rel-7 onwards:

  - the Binary Floor Control Protocol (BFCP) as defined in IETF RFC 4582 [16];

  - the Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams as defined in IETF RFC 4583 [17] (mandatory support).

IETF RFC 4583 [17] also enables support of BFCP clients located behind firewalls by enabling the SIP/SDP level negotiation of the TCP connection setup direction (by using the IETF RFC 4145 [12] "a=setup:" and "a=connection:" SDP attributes).

IETF RFC 4582 [16] and IETF RFC 4583 [17] require that the SDP offerer acts as the TLS client, the SDP answerer as the TLS server, regardless of its role (initiator or responder) in the TCP establishment procedure.

IETF RFC 4582 [16]:

> "Which party, the client or the floor control server, acts as the TLS server depends on how the underlying TCP connection is established. For example, when the TCP connection is established using an SDP offer/answer exchange [7], the answerer (which may be the client or the floor control server) always acts as the TLS server."

IETF RFC 4583 [17]:

> "When TLS is used, once the underlying TCP connection is established, the answerer acts as the TLS server regardless of its role (passive or active) in the TCP establishment procedure."

The SDP answerer can be the Conference Server/MRFC (e.g. user calling into a conference) or the UE (e.g. user getting invited to a conference). As a result, the IMS-AGW (for e2ae media security) and the Conference Server (for e2e media security) may act as a TLS server or TLS client, depending on which entity initiates the SDP Offer.

Figure 4.2.2.1 aims to provide an overview over related IETF standards.

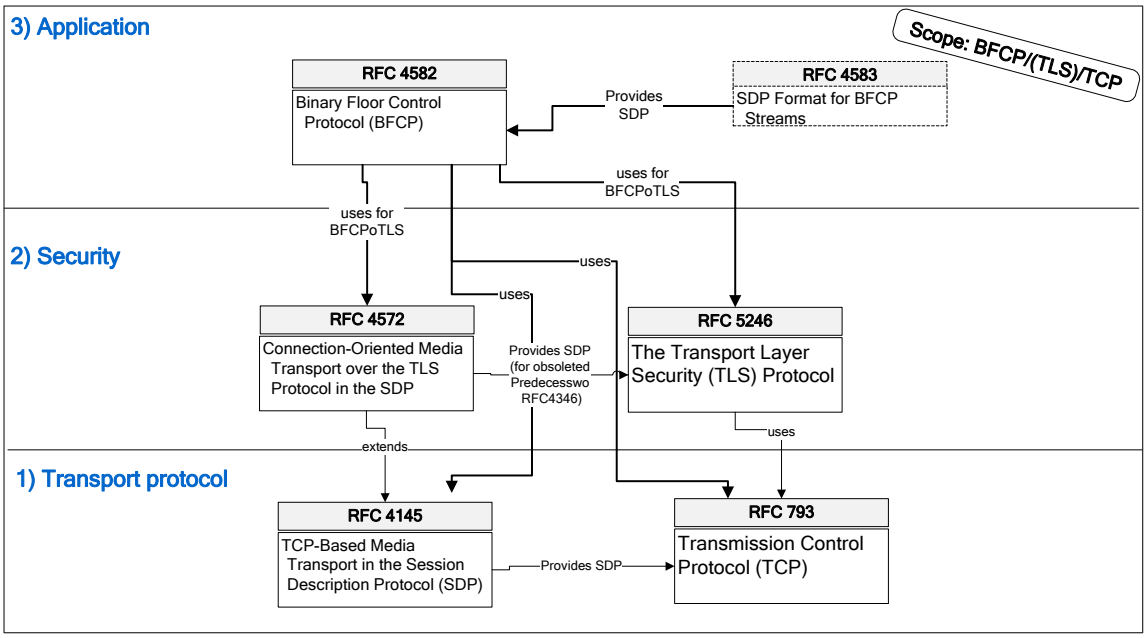

Figure 4.2.2.1: Overview of IETF document concerning NAT-T supported BFCP-(over-TLS-)over-TCP services, as typically used in SIP-based application control signalling

The present study will investigate e2ae and e2e security for BFCP implementations supporting IETF RFC 4582 [16] in combination with IETF RFC 4583 [17] ("SDP Format for BFCP streams").

4.2.3 Scenarios in scope

The same scenarios and requirements apply for BFCP-based media security as described for MSRP-based media security in subclause 4.1.3, with only the following differences:

- this corresponds to a BFCP session between an IMS UE and an MRFP, i.e. and never a session between two UEs;
- only the IMS UE (with e2ae or e2e security applied) may be located behind a remote firewall/NAT device, i.e. the use case where both peers are behind a NAT is not considered.

I.e. the following BFCP-based media security scenarios shall be supported:

a) TLS to non-TLS interworking for e2ae protection of BFCP-based media (at the IMS-AGW);

b) Transparent TLS packets forwarding for e2e protection of BFCP-based media (at the IMS-AGW or TrGW);

c) TLS to non-TLS interworking for e2e protection of BFCP-based media (at the MRFP).

4.2.4 BFCP-agnostic vs BFCP-aware mode

The IMS-AGW shall support application-agnostic interworking for TLS-based e2ae scenarios, i.e. transparent forwarding of application (i.e. BFCP) data.

The IMS-AGW and TrGW shall support application-agnostic (i.e. transparent) forwarding of TLS packets for e2e scenarios.

The MRFP is already BFCP aware prior to eMEDIASEC.

4.3 TLS procedures

Editor's Note: will address general considerations on TLS session control procedures, direction of TLS session establishment, the TLS profile & versions to be supported …

4.3.1 Introduction – Media/transport security sessions at Mb

The (H.248 controlled IP) bearer is generally comprised by an IP *security session* and an underlying TCP-based IP *transport connection* in case of media/transport security (at e.g. IMS Mb).

The bearer establishment is divided in the two main phases (Fig. 4.3.1.1) of (I) *TCP connection establishment* and (II) *IP security session establishment*, particularly in case of connection-oriented transport protocols (such as TCP) or/and IP bearer path coupled security control protocols (such as key exchange protocols, TLS).

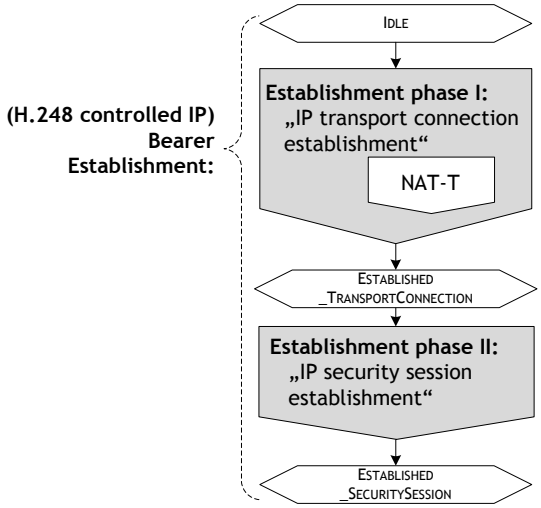

Figure 4.3.1.1: Successful establishment of IP security sessions (at Mb)

It could be noted:

- Precondition of (II) IP security session establishment (see subclause 4.3.3) is a successfully established IP transport connection (NOTE).
- Establishment of the (I) TCP connection (see clause 4.4) implies optional NAT traversal (NAT-T) support (see clause 4.4), under the condition of remote NAT devices in the IP bearer path.

NOTE: IETF RFC 793 [20] allows the TCP sender to deliver data already during the TCP connection establishment phase, which could be a TLS *ClientHello* message here. The MGW can principally buffer or discard such initial TCP data. The "buffer option" is not recommended due to well-known TCP security attack scenarios. Thus, the option of "early" TLS session establishment can be supported, but is discouraged due to the indicated security issues, TCP NAT traversal, etc.

4.3.2 H.248 bearer type indication "TLS"

The MGW needs to be indicated to apply bearer type "TLS" in order to reserve and prepare TLS resources associated with the H.248 termination or stream endpoint.

NOTE 1: This procedure is similar to the Q.1950 defined BNC procedure (at Mc / Mn).

NOTE 2: This indication can be combined with an indication about the underlying transport protocol and the application protocol (e.g. if the "transport" parameter of the SDP "m="-line is used to encode this indication).

4.3.3 TLS security session establishment

4.3.3.1 TLS client/server role assignment

4.3.3.1.1 General

TLS is a client/server protocol, i.e. there are different state transitioning behaviours (and hence procedures) at client and server side during the establishment phase of a TLS security session.

A MGW that terminates the TLS protocol layer (i.e., a TLS endpoint) thus either needs to be indicated to act as TLS client or TLS server.

Furthermore, TLS is designed to be independent from IP transport protocols (IETF RFC 5246 [7]) (e.g., TLS-over-TCP, TLS-over-SCTP). Thus, any (if at all) client/server role usage at IP transport protocol layer is basically independent of the TLS role usage.

4.3.3.1.2 Application agnostic TLS-over-TCP

Status: there is not yet any signalling element at application control protocol level for the indication/negotiation of TLS client/server roles between the two TLS endpoints. The basic RFC for SDP for TLS security session control (IETF RFC 4572 [14]) is silent on the TLS client/server role assignments and TLS security session establishment directions.

In the present study it will be assumed for MSRP that the TCP related SDP "a=setup" attribute is used in SIP/SDP signalling to determine the TLS client and server roles in addition to the TCP client and server roles, see subclause 4.3.3.1.3.

Editor's Note: This working assumption is to be confirmed by CT1.

NOTE: IETF RFC 5763 [15] (DTLS-SRTP) uses the IETF RFC 4145 [12] SDP "a=setup" attribute to determine the DTLS client and server roles, has been quoted as additional argument for this solution, although that RFC is not applicable for TLS over TCP.

4.3.3.1.3 Application aware scenario "MSRP-over-TLS-over-TCP"

MSRP itself is a client/server protocol at application protocol level.

Status: the core RFC for MSRP IETF RFC 4975 [6] describes MSRP-over-TLS usage and supports a TLS peer-to-peer authentication model (clause 14.4) besides TLS client/server relationship, but the RFC is lacking information on TLS security session establishment.

In the present study it will be assumed that the TCP related SDP "a=setup" attribute is used in SIP/SDP signaling to determine the TLS client and server roles for MSRP in addition to the TCP client and server roles.

NOTE: Clients only supporting MSRP according to RFC IETF RFC 4975 [6] will not use the SDP "a=setup" attribute, but will assign the TCP client role to the SDP offerer. However, in 3GPP, OMA and GSMA the support of IETF RFC 6135 [8] ("COMEDIA for MSRP") is mandated, and the "a=setup" attribute will thus be used.

Editor's Note: It was noted that there are multiple different positions how the IETF RFCs could be interpreted. There's agreement about an existing gap with the RFC situation. SA3 and/or CT1 have been contacted with the request to provide some clarifications at least within the scope of 3GPP specifications, and to confirm the working assumption that TCP related SDP "a=setup" attribute is used in SIP/SDP signaling to determine the TLS client and server roles for MSRP.

4.3.3.1.4 Application aware scenario "BFCP-over-TLS-over-TCP"

BFCP itself is a client/server protocol at application protocol level (with the floor control client and floor control server roles).

IETF RFC 4583 [17] (SDP Format for BFCP Streams) contains an explicit TLS server role assignment for the SDP answerer in Clause 8; "*When TLS is used, once the underlaying TCP connection is established, the answerer acts as the TLS server regardless of its role (passive or active) in the TCP establishment procedure.*"

NOTE: IETF RFC 4583 [17] uses the TCP related IETF RFC 4145 [12] SDP "a=setup" attribute only to determine the TCP client and server roles.

In recent discussions at the IETF MMUSIC mailing list, it was commented that the implications of this rule for opposite direction offer-answer renegotiations while a TLS session is established are unclear (should a new TLS session with reversed roles be established?).

Editor's Note: SA3 and/or CT1 have been contacted with the request to provide some clarifications at least within the scope of 3GPP specifications.

4.3.3.2 Start of TLS security session establishment

There are two fundamental options:

1. The start of TLS security session establishment is *immediately* initiated by the TLS client side as soon as the underlying IP transport connection is successfully established (i.e., when the local TCP connection endpoint is transitioned to TCP state "ESTAB").
   There are two variants in case of Iq, Ix and Mp:
   - The MGW notifies firstly the MGC, which then triggers the MGW for TLS security session establishment (if TLS client side);
   - The MGW autonomously starts TLS security session establishment (if TLS client side), and optionally notifies additionally the MGC (if requested);
2. The start of TLS security session establishment is decoupled from the underlying TCP connection establishment (e.g., TLS establishment might be principally delayed (by the MGC) versus TCP connection establishment, or TLS usage could be principally enabled during active communication, i.e. a later point in time).

See clause 5.1.1.1 concerning the required variant for Rel-12.

4.3.4 TLS security session release

4.3.4.1 TLS-to-TCP relations

There are two fundamental combinations, a TLS security session release may lead also to the release of the underlying TCP transport connection:

1. Release of TLS plus TCP: normal case, the end-to-end communication service is terminated.
2. Release of TLS without TCP, e.g., due to
   a. TLS failure scenario (see TLS alert protocol) with immediate TLS session release;
   b. TLS session resumption scenarios;
   c. TCP connection reuse.

Option 1 is the supported variant for Rel-12.

4.3.4.2 MGW: stimuli for TLS security session release

The trigger for TLS security session release may origin from multiple sources from perspective of the MGW, such as the MGC, the remote TLS endpoint, from the underlying TCP layer, or due to TLS protocol failures.

All options are supported for Rel-12.

4.4 TCP procedures

Editor's Note: will address general considerations on TCP procedures e.g. to which extent TCP bearer control procedures or the type of TCP protocol handling for TCP endpoints need to be specified, direction(s) of bearer establishment / setup attribute, NAT and NAT-T considerations, …

Editor's Note: It is FFS if the TCP and TLS setup directions are determined independently.

4.4.1 H.248 bearer type indication "TCP"

The MGW needs to be indicated to apply bearer type "TCP" in order to reserve and prepare TCP resources associated with the H.248 termination or stream endpoint.

NOTE 1: This procedure is similar to the Q.1950 defined BNC procedure (at Mc / Mn).

NOTE 2: This indication can be combined with an indication about the application protocol (e.g. if the "transport" parameter of the SDP "m="-line is used to encode this indication).

4.4.2 TCP connection establishment

4.4.2.1 TCP client/server role assignment

Editor's Note: a couple of items were observed (at the CT4#62 meeting) which needs clarification:
1) **Terminology**: "TCP endpoint" (not defined by RFC 793) and "terminating TCP protocol"
=> there are two entities: a) the remote TCP connection endpoint, and b) the local, TCP-enabled H.248 stream endpoint.
2) **Call model wrt TCP connection establishment**
=> "half-call model" and "end-to-end model"
=> the text so far is focusing on the half-call model, i.e., TCP connection establishment from perspective of a single TCP-enabled H.248 stream endpoint
=> e2e model introduced the H.248 context view of two associated TCP-enabled H.248 stream endpoints, i.e., the internal control of e2e TCP connection establishment
3) **MGW internal TCP handling during TCP connection establishment**
=> different TCP modes of operation by the MGW, see new clause 4.4.4

4.4.2.1.1 SIP level negotiation of TCP server and client role by MGC

Editor's Note: following text is for further study:

A MGC (e.g. a MRFC) that controls a MGW that terminates the TCP protocol may need to determine if the MGW shall act as TCP client or server. (alternative text proposal: A MGC (e.g. a MRFC) that controls a MGW with TCP-enabled (H.248) stream endpoint (SEP) may need to determine for each SEP whether it shall act as TCP client or server).

NOTE 1: There are a number of TCP related MGW functions which are not really dependent on TCP role awareness. E.g., a MGW that only modifies port numbers (i.e. port translation (PT)) when forwarding TCP packets would be TCP aware (due to the implicit, TCP specific checksum udate), but does not require information about the TCP client and server role. The MGW just requires to know how to apply autonomously incoming/outgoing TCP connection establishment procedures.

The MGC controlling a MGW that needs to be explicitly configured for TCP connection establishment procedures uses the IETF RFC 4145 [12] SDP "a=setup" attribute in SIP/SDP signaling to determine the client and server role; if the "a=setup" attribute is omitted by the SDP offerer, the offerer (which could be the MGC) automatically becomes the TCP client (i.e., the MGC would then signal "TCP client" side TCP connection establishment procedures to the MGW, see next sub-clause).

MSRP clients only supporting MSRP according to RFC IETF RFC 4975 [6] will not use the SDP "a=setup" attribute, but will assign the TCP client role to the SDP offerer. However, in 3GPP, OMA and GSMA the support of IETF RFC 6135 [8] ("COMEDIA for MSRP") is mandated, and the "a=setup" attribute will thus be used.

NOTE 2: The IETF RFC 4145 [12] SDP "a=connection" attribute shall not be used according to IETF RFC 6135 [8].

According to IETF RFC 4583 [17], "the management of the TCP connection used to transport BFCP is performed using the 'setup' and 'connection' (SDP) attributes".

Editor's Note: the TCP endpoint in a MGW is either TCP client or TCP server. Whether the MGC is always able to indicate the TCP role to the MGW is subject of discussion (E.g., a default role such as TCP server (in order to be prepared for TCP Passive Open; or based on a MGC local policy if information could not be derived from call control signalling, etc.).

Editor's Note: following text is for further study:

In the SDP offer, "a=setup:actpass" may be used to indicate the ability to serve both as TCP client and server; the SDP answerer will then select either the TCP server or client role and indicate its choice in the SDP answer. Thus, the SDP offerer side needs to be prepared to receive incoming TCP connection setups when offering "a=setup:actpass". If an MGC uses "a=setup:actpass" in the SDP offer, it can configure the MGW to act as TCP server. If the answerer then selects "a=setup:pass", the MGC needs to reconfigure the MGW to act as TCP client.

TS 24.229 [18] does not define any IMS-ALG procedures to modify the "a=setup" attribute. According to current specifications, it can thus not change the directionality of TCP connection setups between interconnected SDP offer/answer entities.

Editor's Note: It will be further studied in subclause 4.4.4 if changing the directionality of TCP connection setups requires extra MGW resources and adversely impact the TCP connection performance.
(Comment: there could be firstly a TCP merge or relay mode before behaving as TCP proxy).

4.4.2.1.2 H.248 control of TCP connection establishment at MGC by MGW

Editor's Note: following text is for further study:

TCP is a client/server protocol, i.e. there are different state transitioning behaviours (and hence procedures) at client and server side during the establishment phase of a TCP transport connection. The TCP client/server role assignment is of temporary nature only because coupled with the transient phase of TCP connection state transitioning from CLOSED to ESTAB (see Figure 6 in IETF RFC 793 [20]). Whether the local TCP-enabled (H.248) stream endpoint (at the MGW) provides a TCP client or server behaviour (during establishment phase) is primarily of interest for the MGC (from perspective of SIP signalling).

What need to be controlled (configured) in the MGW by the MGC is rather

a) whether an incoming or outgoing TCP bearer establishment needs to be provided and

b) when TCP bearer establishment should be started in incoming or outgoing directions (e.g., there might be initial TCP security attacks which should be blocked as long as SIP level SDP offer/answer is not yet settled).

The MGC decision baseline for above MGW indications is elaborated in subclause 4.5.

4.4.2.2 Start of TCP connection establishment

There are inherent different establishment scenarios for each TCP endpoint, primarily due to its properties of connection-orientation and client/server asymmetry. The different TCP establishment steps follow different state transitioning scenarios (TCP passive open, active open, simultaneous), see IETF RFC 793 [20].

The MGC controls the start of TCP connection establishment (see clause 4.4.2.1). The start is normally tightly coupled to the creation of local TCP resources, but could be also delayed, e.g. in order

- to address possible TCP security attack scenarios,
- to support a resourcement management concept in separating the reservation and preparation phase of local TCP resources from the phase of TCP connection establishment,

NOTE 1: SIP level SDP offer/answer procedures might be decoupled from gateway control procedures.

NOTE 2: The "two-stage resource reservation" procedures as defined by ETSI TS 183 018 [22], clause 5.17.1.11, could be principally applied.

- to support NAT-T scenarios (due to end-to-end TCP connectivity aspects) or/and

NOTE 3: Example, a H.248 connection model with two TCP enabled stream endpoints. The start of TCP connection establishment at one termination shall be delayed as long as a parallel L3/L4 NAT-T procedure at the other termination is ongoing.

- others.

Editor's Note: It is for further studies whether the "delayed" establishment option needs to be supported in Rel-12.

4.4.2.3 L3/L4 level NAT traversal support

In order to reach end-to-end TCP connectivity, remote NAT traversal (NAT-T) support by the MGW might be required. The two major L3/L4 NAT-T mechanisms for TCP (from H.248 MGW perspective) are:

1. *Latching* on remote IP source transport address information (according ITU-T H.248.37 [23]); and

2. *TCP merge mode* (in order to support TCP simultaneous open procedures from end-to-end perspective (according ITU-T H.248.84 [24]).

Both NAT-T variants are orthogonal and may be applied individually or combined. The dedicated usage is dependent on a number of service and network properties, such as

- existence and position of remote NAT devices in the media plane;

- single or multiple NAT devices;

- type of remote NAT devices (e.g., the distinction between "BEHAVE-compliant" and "legacy" types by IETF WG BEHAVE);

NOTE 1: IETF working group BEHAVE (*Behavior Engineering for Hindrance Avoidance*, see http://tools.ietf.org/wg/behave/)

- the level of information by the MGC about the media plane "NAT architecture"; and

- end-to-end application control.

NOTE 2: It has to be noted that above information reflects the status of Rel-12 only. E.g., the IMS firewall traversal studies by 3GPP TR 33.830 [25], future media multiplexing models, additional support of ICE-based NAT-T (see 3GPP TS 23.228 [3] Annex G), bearer-level application gateway support, etc. may demand for further NAT-T capabilities in future 3GPP releases.

Editor's Note: required capabilities for Rel-12 are still under study.

4.4.3 TCP connection release

4.4.3.1 TLS-to-TCP relations

There are TCP connection segments with and without TLS from MGW perspective. The overlying TLS protocol (in case of H.248 TLS/TCP stream endpoint/termination) may impact TCP connection release, see subclause 4.3.4.1.

4.4.3.2 MGW: stimuli for TCP connection release

The trigger for TCP connection release may origin from multiple sources from perspective of the MGW, such as the MGC, the remote TCP endpoint and the overlying TLS endpoint.

4.4.4 TCP Interworking in the MGW

Editor's Note: following text is for further study:

The previous subclause focus on aspects of single TCP-enabled stream endpoint, i.e. from perspective of the MGW on the external bearer interface. IMS H.248 profiles support (IP,IP and (IP, IP, IP) in case of Iq, which relates effectively to (TCP, TCP) and (TCP, TCP, TCP) connection models. There's consequently MGW internal interworking between the TCP enabled stream endpoints. There are some high level TCP interworking models known, - TCP relay, TCP merge and TCP proxy mode -, which characterizes some TCP functions to be provided by the MGW. Etc

Editor's Note: following text is for further study:

It is desirable that a MGW interconnecting two TCP terminations forwards TCP flow control related information between the terminations in order to avoid negative impacts on the end-to-end TCP throughput, and to avoid delays caused by buffering of TCP payloads. The details of related procedures can be left to the MGW implementation.

Editor's Note: It is ffs if an end-to-end TCP flow control is feasible if the TCP setup direction is reversed between interconnected terminations.
Further comment: there are always the two options: a) keeping a single e2e TCP connection or b) a partitioning in two TCP connection segments. The SN/AN number space would be global in case of (a), and segment specific in (b) …

4.5 MGC information baseline for gateway control decisions

The SIP/SDP signalling provides the primary information for gateway control decisions (H.248 signalling) by the MGC. Additional MGC-local policies may provide complementary information for TCP (and TLS) bearer control.

5 IMS-ALG/ IMS-AGW interface (Iq)

5.1 Requirements

Editor's Note: this clause intends to capture stage 2 requirements for the Iq profile. Contents of this clause are expected to be moved to 3GPP TS 23.334 once stable.

5.1.1 End-to-access edge security for TCP-based media using TLS

5.1.1.1 General requirements

5.1.1.2 Specific requirements for session based messaging (MSRP)

5.1.1.3 Specific requirements for conferencing (BFCP)

5.1.2 End-to-end security for TCP-based media using TLS

5.1.2.1 General requirements

5.1.2.2 Specific requirements for session based messaging (MSRP)

5.1.2.3 Specific requirements for conferencing (BFCP)

5.2 Procedures

Editor's Note: this clause intends to capture stage 2 procedures for the Iq profile. The procedures will show the H.248 interactions for the main call flows. Contents of this clause are expected to be moved to 3GPP TS 23.334 once stable.

5.2.1 End-to-access edge security for TCP-based media using TLS

5.2.1.1 Generic procedures

5.2.1.2 Specific procedures for session based messaging (MSRP)

5.2.1.3 Specific procedures for conferencing (BFCP)

5.2.2 End-to-end security for TCP-based media using TLS

5.2.2.1 Generic procedures

5.2.2.2 Specific procedures for session based messaging (MSRP)

5.2.2.3 Specific procedures for conferencing (BFCP)

6 IBCF/ TrGW interface (Ix)

Editor's Note: References to the Iq clause should be made wherever requirements & procedures are common across profiles, rather than duplicating text.

6.1 Requirements

Editor's Note: this clause intends to capture stage 2 requirements for the Ix profile. Contents of this clause are expected to be moved to 3GPP TS 29.162 once stable.

6.1.1 End-to-end security for TCP-based media using TLS

6.1.1.1 General requirements

6.1.1.2 Specific requirements for session based messaging (MSRP)

6.1.1.3 Specific requirements for conferencing (BFCP)

6.2 Procedures

Editor's Note: this clause intends to capture stage 2 procedures for the Ix profile. The procedures will show the H.248 interactions for the main call flows. Contents of this clause are expected to be moved to 3GPP TS 29.162 once stable.

6.2.1 End-to-end security for TCP-based media using TLS

6.2.1.1 Generic procedures

6.2.1.2 Specific procedures for session based messaging (MSRP)

6.2.1.3 Specific procedures for conferencing (BFCP)

7 MRFC/ MRFP interface (Mp)

Editor's Note: References to the Iq clause should be made wherever requirements & procedures are common across profiles, rather than duplicating text.

7.1 Requirements

Editor's Note: this clause intends to capture stage 2 requirements for the Mp profile. Contents of this clause are expected to be moved to 3GPP TS 23.333 once stable.

7.1.1 End-to-end security for TCP-based media using TLS

7.1.1.1 General requirements

7.1.1.2 Specific requirements for session based messaging (MSRP)

7.1.1.3 Specific requirements for conferencing (BFCP)

7.2 Procedures

Editor's Note: this clause intends to capture stage 2 procedures for the Mp profile. The procedures will show the H.248 interactions for the main call flows. Contents of this clause are expected to be moved to 3GPP TS 23.333 once stable.

7.2.1 End-to-end security for TCP-based media using TLS

7.2.1.1 Generic procedures

7.2.1.2 Specific procedures for session based messaging (MSRP)

7.2.1.3 Specific procedures for conferencing (BFCP)

8 3GPP- ITU-T H.248 requirements gap analysis

Editor's Note: this clause will review the work in progress in ITU-T related to support of TLS for media security, identify the ITU-T extensions necessary to fulfill the 3GPP requirements, and identify any potential missing gaps that should be taken into account by ITU-T Q3/16.

9 Conclusions and Recommendations

Annex A (informative): Impacts to Existing Specifications

Annex B (informative): Release 12 requirements and procedures for extended media security

The Rel-12 requirements from 3GPP TS 33.328 [2] version 12.3.0, regarding extended media security are copied and Rel-12 new text additions are shown in this Annex as underlined text. For completeness, in some chapters, the text of 3GPP TS 33.328, version 11.0.0 is shown without underlines.

Note that this Annex will not be updated to align with possible future versions of 3GPP TS 33.328 [2]. 3GPP TS 33.328 [2] overrides any text in this Annex.

This Annex shows the subclause numbers and titles of 3GPP TS 33.328 [2], which contain relevant requirements for this TR.

NOTE: The requirements and procedure descriptions in this annex, which are covered in the main body of this TR, will be marked with yellow background.

Editor's Note: The color marking of covered text will be included in the next version of this TR.

33.328: 1 Scope

The media plane security for MSRP, used in session-based messaging, is based on TLS. TLS is also used to protect BFCP. Key management solutions for MSRP and BFCP security are defined in this specification.

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

33.328: 2 References

…

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

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

[23] IETF RFC 4582: "The Binary Floor Control Protocol (BFCP)".

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

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

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

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

33.328: 4 IMS media plane security overview,
33.328: 4.1.1 General

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

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

33.328: 4.1.2.1 SDES based solution

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

33.328: 4.1.2.3 Certificate fingerprints based solution for TLS

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

This approach is specified in RFC 4975 [21]. "TCP/TLS/MSRP" is used as the protocol identifier in the m-line of the SDP, and the "a=fingerprint" attribute is used to provide the fingerprint of the certificate.

33.328: 4.2 IMS media plane security architecture
33.328: 4.2.1 General

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

33.328: 5 IMS media plane security features
33.328: 5.1 General

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

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

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

33.328: 5.2 Media integrity protection

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

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

33.328: 5.3 Media confidentiality protection

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

33.328: 5.4.1 Authentication and authorization for e2ae protection

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

(Rel-12 additions in **33.328, 5.4.2** do not seem related to extended media security.)

33.328: 5.5.4 Security properties for e2ae protection using TLS

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

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

33.328: 6.1.2 Media security mechanisms for session based messaging (MSRP)

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

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

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

The following requirements are applicable for e2ae session based messaging (MSRP).

33.328: 6.2.1 Key management mechanisms for e2ae protection
33.328: 6.2.1.1 Endpoints for e2ae protection

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

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

33.328: 6.2.1.2 Key management protocol for e2ae protection

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

33.328: 6.2.1.3.2 Functional extension of the Iq interface for e2ae protection for MSRP

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

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

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

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

33.328: 6.2.3 Key management mechanisms for e2e protection using KMS
33.328: 6.2.3.1 General

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

33.328: 6.2.3.5 Authentication of public identities in REQUEST_INIT and RESOLVE_INIT

Rel-12 additions in 33.328, 6.2.3.5 do not seem related to extended media security covered by this TR, but copied here for completeness.

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

33.328: 7.1.1 Indication of support for e2ae security for RTP based media

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

33.328: 7.1.2 Indication of support for e2ae security for MSRP

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

NOTE 1: The policies of the IMS UE and the network concerning the use of e2ae security for MSRP are independent from the policies concerning the use of e2ae security for RTP based media.

NOTE 2: For compatibility with RCS 5.1, the indication of support for e2ae security during registration is not a necessary prerequisite for the use of e2ae security, but it helps to avoid certain error cases, cf. Clause 7.2.1 and Clause 7.3.1.

The requirements for the procedures of **e2ae** session based messaging (subclause 5.2.1.2 in this TR) are specified in 33.328.

33.328: 7.2.1 IMS UE originating procedures for e2ae

… If both IMS UE and network indicated support for e2ae security for MSRP during registration, then the IMS UE shall request e2ae security for MSRP media streams to be established as described in this clause, unless the IMS UE initiates a procedure for e2e security for an MSRP media stream.

In Step 1: For e2ae protection of MSRP the cryptographic information contained in the SDP Offer consists of the fingerprint of the certificate of IMS UE A in accordance to RFC 4975 [21].

In Step 2: For each media stream that uses transport "RTP/SAVP", "RTP/SAVPF" or "TCP/TLS/MSRP", the P-CSCF (IMS-ALG) checks for the presence of the indication "e2ae-security requested by UE".
If the indication is present and the P-CSCF (IMS-ALG) indicated support of e2ae-security for the respective protocol (RTP and/or MSRP) during registration, the P-CSCF (IMS-ALG) allocates the required resources, includes the IMS Access GW in the media path and proceeds as specified in this clause. If the indication is not present for an SRTP media stream the P-CSCF (IMS-ALG) proceeds for this media stream as described in clause 7.2.2 or clause 7.2.3 of the present specification.

If the indication is not present for an MSRP media stream offered with transport "TCP/TLS/MSRP", the P-CSCF (IMS-ALG) proceeds for this media stream as described in clause 7.2.3 of the present specification or in TS 23.228 [3] and skips the further steps in the present subclause.

In Step 3. The P-CSCF (IMS-ALG) modifies the SDP offer before sending it towards the S-CSCF. …
For e2ae protection of MSRP, the P-CSCF (IMS-ALG) shall change the transport from "TCP/TLS/MSRP" to "TCP/MSRP" in the SDP Offer (cf., however, NOTE 4), stores the received fingerprint of the IMS UE A certificate and removes it as well as the indication "e2ae-security requested by UE" from the description of the media stream in the SDP Offer if present.

In Step 7. The P-CSCF (IMS-ALG) and the IMS Access GW exchange the cryptographic information.
For e2ae protection of MSRP the cryptographic information communicated by the P-CSCF (IMS-ALG) to the IMS Access GW consists of the fingerprint of the UE´s certificate in accordance to RFC 4975 [21]. The P-CSCF (IMS-ALG) instructs the IMS Access GW to verify during the subsequent TLS handshake with the IMS UE (see step 9) that the fingerprint of the certificate passed by the IMS UE during this TLS handshake matches the fingerprint passed by the P-CSCF (IMS-ALG) to the IMS Access GW. In turn, the IMS Access GW communicates the fingerprint of the certificate it is going to use for setting up protection for this media stream to the P-CSCF (IMS-ALG).

In Step 8. The P-CSCF (IMS-ALG) modifies the SDP Answer before sending it to the IMS UE A. …
For e2ae protection of MSRP, the P-CSCF (IMS-ALG) shall set the transport to "TCP/TLS/MSRP" , remove any fingerprint attributes in the SDP Answer, if present, and include the fingerprint of the IMS Access GW´s certificate in accordance to RFC 4975 [21].

In Step 9. [RTP]… In case of MSRP, when the full session setup has been completed, the TCP and TLS connection shall be established between the IMS UE and the IMS Access GW. When subsequently media are sent from or to the IMS UE, the IMS Access GW performs the required TLS specific cryptographic operations on the media.

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

33.328: 7.3.1 UE terminating procedures for e2ae

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

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

In Step 3. For each MSRP media stream offered with transport "TCP/MSRP", if both the IMS UE and P-CSCF (IMS-ALG) indicated support for e2ae-security for MSRP during registration, the P-CSCF (IMS-ALG) proceeds for this media stream as described in this clause and allocates the required resources, includes the IMS Access GW in the media path for establishing the TLS towards the IMS UE and retrieves from the IMS Access GW the fingerprint of the certificate the IMS Access GW is going to use for setting up security for this media stream. Otherwise the P-CSCF (IMS-ALG) continues as described for media streams without IMS media plane security.

For each MSRP media stream offered with transport "TCP/TLS/MSRP" the P-CSCF (IMS-ALG) proceeds as specified in clause 7.3.3 of the present specification or in TS 23.228 [3].

In Step 4. For e2ae protection of an MSRP media stream the P-CSCF (IMS-ALG) sets the transport to "TCP/TLS/MSRP" in the SDP Offer, removes any fingerprint attributes for this media stream and includes the fingerprint of the IMS Access GW´s certificate in accordance to RFC 4975 [21] as well as an indication that e2ae security is offered by the network. The P-CSCF (IMS-ALG) then sends the updated SDP Offer to IMS UE B.

In Step 5. For e2ae protection of MSRP, the IMS UE B includes in the SDP Answer the fingerprint of the UE´s certificate in accordance to RFC 4975 [21].

In Step 6. The P-CSCF (IMS-ALG) communicates the cryptographic information contained in the SDP Answer to the IMS Access GW. …
For e2ae protection of MSRP, the cryptographic information communicated to the IMS Access GW consists on the fingerprint of the IMS UE B certificate in accordance to RFC 4975 [21]. The P-CSCF (IMS-ALG) instructs the IMS Access GW to verify during the subsequent TLS handshake with the IMS UE (see step 9) that the fingerprint of the certificate passed by the IMS UE during this TLS handshake matches the fingerprint passed by the P-CSCF (IMS-ALG) to the IMS Access GW.].

In Step 7. The P-CSCF (IMS-ALG) modifies the SDP Answer before sending it to the S-CSCF. …
For e2ae protection of MSRP, the P-CSCF (IMS-ALG) changes the transport from "TCP/TLS/MSRP" to

"TCP/MSRP" in the SDP Answer (cf., however, NOTE 4). Further, it removes the fingerprint of the IMS UE B certificate. The P-CSCF (IMS-ALG) then sends the SDP Answer to the S-CSCF.

In Step 9. In case of MSRP, when the full session setup has been completed, the TCP and TLS connection shall be established between the IMS UE and the IMS Access GW. When subsequently media are sent from or to the IMS UE, the IMS Access GW performs the required TLS specific cryptographic operations on the media.

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

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

The requirements for the procedures of **e2e** session based messaging (subclause 5.2.2.1 and 5.2.2.2 in this TR) and e2e conferencing (subclause 5.2.2.3 in this TR) are specified in 33.328.

33.328: 7.2.3 IMS UE originating procedures for e2e using KMS

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

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

33.328: 7.3.3 IMS UE terminating procedures for e2e using KMS

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

33.328: Annex B (Normative): KMS based key management
33.328: B.1 UE originating procedures

In Step 10. … In the RTP case, the number of Crypto Sessions included in the TRANSFER_INIT message should match the number of RTP streams (both incoming and outgoing) as described in RFC 4567 [12]. The protocol type in the Crypto Session shall be set to SRTP.

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

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

33.328: B.2 UE terminating procedures

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

33.328: Annex F (normative): IMS media plane security for immediate messaging
33.328: F.2 Security for immediate messaging based on SIP signalling security

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

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

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

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

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

33.328: Annex G (normative): IMS media plane security for conferencing
33.328: G.1 General aspects

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

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

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

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

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

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

33.328: G.2 Security for conferencing based on SIP signalling security

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

e2ae security:

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

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

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

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

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

e2e security:

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

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

It is outside the scope of the solution in the present clause whether the conference server supports TLS for MSRP according to RFC 4975 [21] and/or for BFCP according to RFC 4582 [23].

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

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

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

33.328: G.3 Security for conferencing based on MIKEY-TICKET
33.328: G.3.1 Conference creation and policy control

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

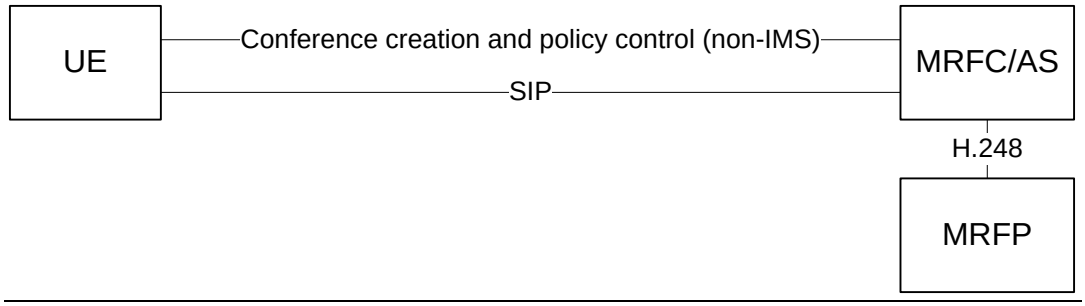

Figure Y1: Conference creation and policy control via external interface

33.328: G.3.2 User joining a secure conference

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

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

33.328: G.3.3 Subscribing to conference event package

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

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

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

33.328: H.1 The TLS Prot Type

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

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
!     CS ID     !   Prot type   !S!     #P      ! Ps (OPTIONAL) ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
!      Session Data Length      !    Session Data (OPTIONAL)    ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
!  SPI Length   !                SPI (OPTIONAL)                 ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- CS ID (8 bits): defines the CS ID to be used for the crypto session
- Prot Type (8 bits): defines the security protocol to be used for the crypto session. Shall be set to TLS.
- S (1 bit): flag that MAY be used by the Session Data. This flag is not used for the Prot Type TLS. The value 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 and the value is therefore TBD.

33.328: H.2 Establishing a TLS connection

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

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

33.328: H.3 Usage with SDP

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

RFC 5246 describes how the key-mgmt attribute is used to perform a MIKEY-TICKET exchange in SDP and how an m-line can be mapped to set of SRTP CSs (one for each SSRC). If the key-mgmt attribute is used at session level then the MIKEY-TICKET exchange contains CSs for all the m-lines in the SDP and the mapping is based on the order of the m-lines. If the key-mgmt attribute is used at the media level then the CSB only contains the CSs for that m-line. Mixing of session and media level attributes is allowed by 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 there is exactly one CS per m-line.

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

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

33.328: Annex J: IANA considerations

33.328: J.1 IANA assignments

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

Table J: Prot Type (Additions)

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

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

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

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

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

Annex C (informative): Change History

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2013-05	CT4#61	C4-130836			TR skeleton		0.0.0
2013-05	CT4#61	C4-131062			Implementation of C4-130837, C4-130838, C4-131038, C4-131039.	0.0.0	0.1.0
2013-06	CT#60				TR number allocated	0.1.0	0.1.1
2013-08	CT4#62	C4-131517			Implementation of C4-131079, C4-131438, C4-131439, C4-131440, C4-131441, C4-131442, C4-131467, C4-131468, C4-131477, C4-131501, C4-131502, C4-131503, C4-131504, C4-131505, C4-131516	0.1.1	0.2.0