**3GPP TSG-SA3 Meeting # 112 *draft\_S3-234337-r1***

**Gothenburg, Sweden, 14 -18 August 2023**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.328** | **CR** | **0071** | **rev** | - | **Current version:** | **17.1.0** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **X** | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | CR on security aspects of NG RTC |
|  |  |
| ***Source to WG:*** | Huawei, HiSilicon |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | NG\_RTC\_SEC |  | ***Date:*** | 2023-08-14 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** | Rel-18 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | It's proposed to agree the security aspects of next generation real time communication services. |
|  |  |
| ***Summary of change:*** | Add the security aspects of data channel usage and SBA in IMS. |
|  |  |
| ***Consequences if not approved:*** | Incomplete work for the phase 2 NG RTC features. |
|  |  |
| ***Clauses affected:*** | 1, 2, 3.3, 4.1.1, 4.1.2.3, 4.1.2.X (new), 4.1.2.Y (new), 4.2.1, 4.2.2, 4.2.4, 4.2.X (new), 4.2.Y (new), 5.1., 5.2, 5.3, 5.4.1, 5.4.X (new), 5.4.Y (new), 5.5.4, 5.5.X (new), 5.5.Y (new), 6.1.X (new), 6.2.1.3.2, 6.2.X (new), 6.2.X.1 (new), 6.2.X.2 (new), 6.2.X.3 (new), 6.2.X.3.1 (new), 7.1.X (new), 7.2.1, 7.2.2, 7.2.3, 7.2.X (new), 7.2.Y (new), 7.3.1, 7.3.2, 7.3.3, 7.3.X (new), 7.3.Y (new), Annex N, Annex N.1, Annex N.3, Annex N.3.1, Annex N.3.2, Annex N.3.Y (new), Annex N.3.X (new), Annex X (New clause). |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

\*\*\*\* Start of Changes\*\*\*\*

# 1 Scope

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

1. to provide security for media usable across all access networks
2. to provide an end-to-end (e2e) media security solution for RTP and data channel-based media to satisfy major user categories
3. to provide end-to-end (e2e) media security for important user groups like enterprises, National Security and Public Safety (NSPS) organizations and different government authorities who may have weaker trust in the inherent IMS security and/or may desire to provide their own key management service.

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

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

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

\*\*\*\* Next Changes\*\*\*\*

# 2 References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[17] Void

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

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

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

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

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

[23] Void

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

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

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

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

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

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

[30] Void

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

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

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

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

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

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

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

[38] Void

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

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

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

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

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

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

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

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

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

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

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

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

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

\*\*\*\* Next Changes\*\*\*\*

## 3.3 Abbreviations

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

BFCP Binary Floor Control Protocol

DCSF Data Channel Signalling Function

DCMF Data Channel Media Function

DTLS Datagram Transport Layer Security

DTLS-SRTP DTLS Extension to Establish Keys for SRTP

e2ae End-to-access edge

e2DCeEnd-to-Data-Channel edge

e2e End-to-end

GW Gateway

IMS-ALG IMS Application Level Gateway

IMS UE IMS User Equipment

KMS Key Management Service

MIKEY Multimedia Internet KEYing

MSRP Message Session Relay Protocol

NAF Network Application Function

RTP Real-time Transport Protocol

SRTP Secure Real-time Transport Protocol

TEK Traffic Encryption Key

TGK TEK Generation Key

TLS Transport Layer Security

WebRTC Web Real-Time Communication

\*\*\*\* Next Changes\*\*\*\*

# 4 IMS media plane security overview

## 4.1 Introduction

### 4.1.1 General

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

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

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

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

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

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

\*\*\*\* Next Changes\*\*\*\*

#### 4.1.2.3 Certificate fingerprints based solution for e2ae TLS/DTLS

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

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

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

\*\*\*\* Next Changes\*\*\*\*

#### 4.1.2.X Certificate fingerprints based solution for e2DCe DTLS

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

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

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

\*\*\*\* Next Changes\*\*\*\*

#### 4.1.2.Y Certificate fingerprints based solution for e2e DTLS

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

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

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

\*\*\*\* Next Changes\*\*\*\*

## 4.2 IMS media plane security architecture

### 4.2.1 General

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

1. E2ae security: here the P-CSCF (IMS-ALG), the IMS Access GW, and the Iq interface between them are impacted.

2. E2e security using SDES: minor impact on the network infrastructure (see TS 29.162 [20] for details).

3. E2e security using KMS: here, the network infrastructure needs to be enhanced with a Key Management Server, which, in turn, relies on a GBA [6] infrastructure, or an infrastructure to provide corresponding services, to be in place. Otherwise, there is minor impact on the network infrastructure (see TS 29.162 [20] for details).

4. E2DCe IMS Data Channel media plane security: The P-CSCF as well as other network functions such as S-CSCF, IMS AS, and the related interfaces Mw, ISC, DC2 are impacted. The IMS Data Channel media plane security is established between the UE and DCMF/MRF.

5. E2e IMS Data Channel media plane security: The IMS Data Channel media plane security is established between two UEs or between a UE and a Data Channel Application Server.

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

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

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

### 4.2.2 E2ae security

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

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



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

### 4.2.3 E2e security using SDES

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

### 4.2.4 E2e security using KMS

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

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

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

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

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



Figure 4.2.4-1: Reference model for key management for the KMS based solution

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

- For HSS definitions refer to [2].

- For GBA and BSF definitions including the Zh, Zn and Ub reference points refer to TS 33.220 [6].

- For how to secure Zh and Zn also refer to TS 33.220 [6].

- The KMS acts as a NAF when GBA is used for user authentication and establishment of a key shared between the KMS and an IMS UE.

- Reference point Ua uses HTTP [8] for transport of MIKEY-TICKET [14] messages. The procedures are defined in Annex A.

- Protocol details for reference points Ua and Ub are provided in TS 24.109 [19].

- Reference point Zk also uses HTTP [8] for transport of MIKEY-TICKET [14] messages. The procedures are according to Annex A with the restriction that Request-URI only can contain "requesttype" equal to "ticketresolve”. Network domain Security [5] shall be used for authentication of endpoints and protection of messages.

\*\*\*\* Next Changes\*\*\*\*

### 4.2.X E2DCe security

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

The interface between IMS AS and the Data Channel Media Function (DC2) or MRF (Mr’/Cr) needs to be able to transport parameters related to the management of DTLS cryptographic contexts. There is no impact on other parts of the network infrastructure. This is depicted in Figure 4.2.X-1. Details can be found in clauses 6.2.X, 7.2.X and 7.3.X.



Figure 4.2.X-1: IMS signalling and media plane entities relevant to e2DCe security

\*\*\*\* Next Changes\*\*\*\*

### 4.2.Y E2e security for IMS Data Channels

The end-2-end IMS Data Channel media plane security is established between two UEs or between a UE and a Data Channel Application Server. Details can be found in clauses 6.2.Y, 7.2.Y and 7.3.Y.

\*\*\*\* Next Changes\*\*\*\*

# 5 IMS media plane security features

## 5.1 General

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

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

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

For e2DCe IMS Data Channel media plane security, an IMS UE shall support the DTLS-based media plane security mechanism for IMS data channel as defined in section 4.1.2.X.

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

For e2e IMS Data Channel media plane security, an IMS UE shall support the DTLS-based media plane security mechanism as defined in section 4.1.2.Y.

## 5.2 Media integrity protection

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

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

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

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

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

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

## 5.3 Media confidentiality protection

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

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

The support for IMS media confidentiality protection is mandatory in an IMS UE supporting IMS data channel media and mandatory in IMS core network elements supporting e2e IMS Data Channel media plane security.When IMS media plane security is used, SRTP transforms with null encryption should not be used.

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

\*\*\*\* Next Changes\*\*\*\*

## 5.4 Authentication and authorization

### 5.4.1 Authentication and authorization for e2ae protection

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

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

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

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

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

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

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

\*\*\*\* Next Changes\*\*\*\*

### 5.4.X Authentication and authorization for e2DCe protection

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

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

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

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

\*\*\*\* Next Changes\*\*\*\*

### 5.4.Y Authentication and authorization for e2e protection using DTLS

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

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

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

\*\*\*\* Next Changes\*\*\*\*

### 5.5.4 Security properties for e2ae protection using TLS/DTLS

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

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

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

### 5.5.5 Security properties for e2ae protection using DTLS-SRTP

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

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

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

### 5.5.X Security properties for e2DCe protection using DTLS

Based on secure mutual authentication leveraged by the integrity protection of the SIP signalling messages (see clause 5.4.X), DTLS provides secure derivation of session keys to protect the media.

In addition to SIP signalling security, also the Mw, ISC interfaces for signalling between the P-CSCF (IMS-ALG), and the media node terminating the IMS Data Channel towards the UE, i.e. the DCMF/MRF, needs to be secured. Also, the DC2 or Mr’/Cr interface for signalling between the IMS AS and the Data Channel Media Function or MRF, respectively, needs to be secured, see clause 6.2.X.

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

\*\*\*\* Next Changes\*\*\*\*

### 6.1.X Media security mechanisms for IMS data channels

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

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

\*\*\*\* Next Changes\*\*\*\*

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

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

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

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

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

\*\*\*\* Next Changes\*\*\*\*

### 6.2.X Key management mechanisms for e2DCe protection

#### 6.2.X.1 Endpoints for e2DCe protection

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

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

#### 6.2.X.2 Key management protocol for e2DCe protection

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

#### 6.2.X.3 Functional extension of the Mw, ISC, and Mr’/Cr or DC2 interfaces for e2DCe protection

#### 6.2.X.3.1 Functional extension of the Mw, ISC, and Mr’/Cr or DC2 interfaces for e2Dce protection for IMS data channel

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

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

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

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

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

\*\*\*\* Next Changes\*\*\*\*

### 7.1.X Indication of support for e2DCe security for IMS data channel

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

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

\*\*\*\* Next Changes\*\*\*\*

## 7.2 IMS UE originating procedures

### 7.2.1 IMS UE originating procedures for e2ae

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

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



Figure 7.2.1-1: Originating call flow for e2ae case

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

\*\*\*\* Next Changes\*\*\*\*

### 7.2.2 IMS UE originating procedures for e2e using SDES

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

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

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



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

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

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

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

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

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

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

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

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

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

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

\*\*\*\* Next Changes\*\*\*\*

### 7.2.3 IMS UE originating procedures for e2e using KMS

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

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

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



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

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

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

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

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

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

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

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

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

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

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

\*\*\*\* Next Changes\*\*\*\*

### 7.2.X IMS UE originating procedures for e2DCe

Figure 7.2.X-1 shows the originating session set-up procedures for one or more media stream(s) using e2DCe security.



Figure 7.2.X-1: Originating call flow for e2DCe using DCMF/MRF case

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

The originating procedures for establishing IMS data channels with e2e security are described in clause 7.2.Y of this specification. The IMS UE may learn of a preference for e2e security for a particular session or media stream by explicit user action via the user interface or by the security policy implemented on the IMS UE.

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

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

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

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

 If the indication is present and the P-CSCF (IMS-ALG) indicated support of e2DCe-security for IMS data channel during registration, the P-CSCF (IMS-ALG) allocates the required resources, includes the IMS Access GW and Data Channel Media Function/MRF in the media path and proceeds as specified in this clause. If the indication is not present for an IMS data channel media stream, the P-CSCF (IMS-ALG) proceeds for this media stream as described in clause 7.2.Y of the present specification.

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

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

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

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

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

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

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

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

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

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

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

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

\*\*\*\* Next Changes\*\*\*\*

### 7.2.Y IMS UE originating procedures for e2e using TLS/DTLS certificate / fingerprint

Figure 7.2.Y-1 shows the originating call set-up procedures for one IMS data channel media stream using DTLS-based e2e security.

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

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

Figure 7.2.Y-1: Originating call flow for e2e case using certificate / fingerprint

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

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

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

2. If the P-CSCF supports e2ae security and/or e2DCe security, the P-CSCF (IMS-ALG) checks for the presence of the indications "e2ae-security requested by UE" and "e2DCe-security for IMS data channel requested by UE". As neither one of the indications is present, the P-CSCF forwards the SDP offer towards the S-CSCF. If an indication is present the P-CSCF proceeds as described in clauses 7.2.1 or 7.2.X of this specification, respectively.

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

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

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

6. The P-CSCF forwards the SDP Answer to IMS UE A. After receiving this message, IMS UE A completes the media security setup by either initiating DTLS handshake (if setup attribute of the SDP Answer indicated that UE A is DTLS client) or waiting for the peer to initiate DTLS handshake (if setup attribute of SDP Answer indicated that UE A is DTLS server), in accordance with RFC 8841 [XX].

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

\*\*\*\* Next Changes\*\*\*\*

## 7.3 UE terminating procedures

### 7.3.1 UE terminating procedures for e2ae

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

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



Figure7.3.1.-1: Terminating call flow for e2ae case

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

For e2ae protection of RTP the P-CSCF (IMS-ALG) changes the transport from RTP to SRTP in the SDP Offer, includes one or more SDES crypto attributes, as well as an indication that e2ae security is offered by the network. Each of these SDES crypto attributes contains at least one master key K21, and other security context parameters chosen by the P-CSCF (IMS-ALG) in accordance with RFC 4568 [13]. The optional key lifetime field shall be omitted.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

\*\*\*\* Next Changes\*\*\*\*

### 7.3.2 IMS UE terminating procedures for e2e using SDES

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

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

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



Figure7.3.2-1: Terminating call flow for e2e case using SDES

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

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

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

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

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

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

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

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

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

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

\*\*\*\* Next Changes\*\*\*\*

### 7.3.3 IMS UE terminating procedures for e2e using KMS

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

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

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



Figure7.3.3-1: Terminating call flow for e2e case using KMS

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

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

1. The S-CSCF in the terminating network receives an SDP offer for an RTP or MSRP session containing a MIKEY-TICKET offer.

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

3. The P-CSCF forwards the SDP offer to IMS UE B.

4. IMS UE B checks if it is authorized to resolve the ticket and if that is the case IMS UE B interacts with the KMS to resolve the ticket and receive keys.

5. IMS UE B replies with an SDP answer for an RTP or MSRP session, including a MIKEY-TICKET response.

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

7. The S-CSCF forwards the SDP answer towards the originating network.

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

\*\*\*\* Next Changes\*\*\*\*

### 7.3.X UE terminating procedures for e2DCe

Figure 7.3.X-1 shows the terminating session set-up procedures for one or more media streams using e2DCe security.

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



Figure 7.3.X-1: Terminating call flow for e2DCe using DCMF/MRF case

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

NOTE 2: The P-CSCF (IMS-ALG) will not establish e2DCe security for IMS data channel media if the SDP offer received from the S-CSCF indicates that e2e security is being offered, cf. clauses 7.3.2, 7.3.3, and 7.3.Y for the establishment of e2e security on the terminating side.

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

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

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

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

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

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

- if not both the IMS UE and P-CSCF (IMS-ALG) indicated support for e2DCe-security for IMS data channel during registration, the P-CSCF (IMS-ALG) should continue using e2e security, as described in clause 7.3.Y of the present specification.

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

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

For e2DCe protection of an IMS data channel media stream, the P-CSCF (IMS-ALG) keeps the transport as "UDP/DTLS/SCTP" in the SDP Offer, conveys the fingerprint, tls-id, and setup attribute information of the DCMF/MRF as well as an indication that e2DCe security is offered by the network to UE.

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

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

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

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

7. The S-CSCF communicates the cryptographic information contained in the SDP Answer to the Data Channel Media Function/MRF.

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

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

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

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

\*\*\*\* Next Changes\*\*\*\*

### 7.3.Y IMS UE terminating procedures for e2e using TLS/DTLS certificate / fingerprint

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

\*\*\*\* Next Changes\*\*\*\*

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

# N.1 General

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

# N.2 Media security for RTP

## N.2.1 General

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

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

## N.2.2 e2ae security for RTP using DTLS-SRTP

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

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

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

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

NOTE: Void

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



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

# N.3 Media security for WebRTC and IMS data channels

## N.3.1 General

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

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

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

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

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

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



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

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



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

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



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

## N.3.2 e2ae security for WebRTC data channels

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

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

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

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



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

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

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

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

## N.3.Y e2DCe security for IMS data channels

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

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

## N.3.X e2e security for IMS data channels

E2e security for IMS Data Channels for DCMTSI clients is achieved in a similar way as for e2DCe security. See clause N.3.Y. In both cases, certificate fingerprints need to be exchanged over SDP between the peers and certificates are exchanged through DTLS handshake in-band on the media path. The media may be anchored in IMS by inserting a gateway on the media path. To ensure the integrity of the certificate fingerprint, the signalling path is assumed to be protected.



Figure N.3.X-1: E2E protection of IMS Data Channels

\*\*\*\* Next Changes\*\*\*\*

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

# X.1 Security aspects of SBA in IMS media control interface

## X.1.1 General

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

## X.1.2 Protection at the network or transport layer

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

## X.1.3 Authentication and authorization

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

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

\*\*\* END of Changes \*\*\*