**3GPP TSG-SA3 Meeting #105-e *S3-214306***

e-meeting, 8 - 19 November 2021

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** |  | **rev** |  | **Current version:** |  |  |
|  |
| *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:***  | Security updates for algorithms and protocols for 33.328 |
|  |  |
| ***Source to WG:*** | Ericsson |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | eCryptPr |  | ***Date:*** | 2021-11-01 |
|  |  |  |  |  |
| ***Category:*** | B |  | ***Release:*** | Rel-17 |
|  | *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:*** | 3GPP should not rely on obsolete standards. This is especially true for security standards.- RFC 5751 (S/MIME 3.2) has been obsoleted by RFC 8551 (S/MIME 4.0). The new version includes updated security considerations.- RFC 4582 (BFCP) has been obsoleted by RFC 8855. The new RFC includes corrections and updated security considerations.- RFC 4566 (SDP) has been obsoleted by RFC 8866. The new RFC includes corrections.The abbreviations clause has not been updated for a long time and is missing several terms.Incorrect references to RFC 4771 and RFC 5246Several parts of IMS media security make use of SHA-1 which is weak and no longer recommended to use. All uses of SHA-1 should be phased out long-term.SDES has a large number of weaknesses and is no longer recommended to use. SDES should be phased out long-term and the profile is therefore not updated.<https://datatracker.ietf.org/doc/draft-mattsson-dispatch-sdes-dont-dont-dont/>Best current practice for securing RTP media signaled with SIP is to mandate support of DTLS-SRTP. 33.328 already mandate support of DTLS-SRTP for WebRTC UEs. DTLS-SRTP is also very similar to the the mandated protection for MSRP. DTLS-SRTP is well supported.<https://datatracker.ietf.org/doc/html/rfc8862> |
|  |  |
| ***Summary of change:*** | - References to obsolete RFCs voided and updated.- Abbreviations updated.- Incorrect references corrected.- The SHA-1 based algorithms MIKEY-1 and HMAC-SHA-1-160 are not mandatory to support for MIKEY-TICKET.- “SRTP\_AEAD\_AES\_128\_GCM” mandatory to support for DTLS-SRTP- DTLS-SRTP is mandatory to support for e2ae RTP based RTP Media Signaled with SIP. |
|  |  |
| ***Consequences if not approved:*** | IMS media security use weak algorithms and protocols which are no longer recommended by other SDOs and governments. |
|  |  |
| ***Clauses affected:*** | 2, 3.3, 4.1.1, 4.1.2.1, 4.2.2, 5.1, 5.2, 5.4.1, 5.5.X (new), 6.1.1, 6.2.1.2, 6.2.1.3.1Annexes C, D.2A, D.4, F.3.1, G.2, H.3, I, N.2.2, O |
|  |  |
|  | **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:*** |  |

\*\*\* BEGIN 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".

[X1] IETF RFC 7714: "AES-GCM Authenticated Encryption in the Secure Real-time Transport Protocol (SRTP)".

[X2] IETF RFC 8851: "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification".

[X3] IETF RFC 8855: "The Binary Floor Control Protocol (BFCP)".

[X4] IETF RFC 8866: "SDP: Session Description Protocol".

\*\*\* NEXT CHANGE \*\*\*

## 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

DTLS Datagram Transport Layer Security

DTLS-SRTP DTLS Extension to Establish Keys for SRTP

e2ae End-to-access edge

e2e End-to-end

GW Gateway

IMS-ALG IMS Application Level Gateway

IMS UE IMS User Equipment

KMS Key Management Service

MIKEY Multimedia Internet KEYing

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 CHANGE \*\*\*

### 4.1.1 General

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

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

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

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

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

\*\*\* NEXT CHANGE \*\*\*

#### 4.1.2.1 SDES based solution

SDES (Session Description Protocol Security Descriptions for Media Streams, cf. RFC 4568 [13]), is a simple key management protocol for media streams, which are to be secured by means of SRTP [9]. SDES defines a Session Description Protocol (SDP) RFC 8866 [X4] cryptographic attribute for unicast media streams. The attribute describes a cryptographic key and other parameters that serve to configure security for a unicast media stream in either a single message or a roundtrip exchange. The attribute can be used with a variety of SDP media transports, and RFC 4568 [13] defines how to use it for the SRTP unicast media streams. The SDP crypto attribute requires the services of a data security protocol to secure the SDP message. For the use of SDES in IMS, the SIP signalling security mechanisms defined for IMS shall be used, for more details cf. clause 5.5.

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

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

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

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

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

\*\*\* NEXT CHANGE \*\*\*

### 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 and TLS protecting MSRP. 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 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.

\*\*\* NEXT CHANGE \*\*\*

## 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.

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 DTLS-SRTP or 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.

\*\*\* NEXT CHANGE \*\*\*

## 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 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.

\*\*\* NEXT CHANGE \*\*\*

### 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 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.

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 CHANGE \*\*\*

### 5.5.X Security properties for e2ae protection using DTLS-SRTP

Based on secure mutual authentication leveraged by the integrity protection of the SIP signalling messages (cf. 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, cf. clause 6.2.1.3.

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

\*\*\* NEXT CHANGE \*\*\*

### 6.1.1 Media security mechanisms for real-time traffic

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

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

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

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

\*\*\* NEXT CHANGE \*\*\*

#### 6.2.1.2 Key management protocol for e2ae protection

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

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

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

\*\*\* NEXT CHANGE \*\*\*

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

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

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

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

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

\*\*\* NEXT CHANGE \*\*\*

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

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

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

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

\*\*\* NEXT CHANGE \*\*\*

# D. 2A Keys, RANDs and algorithms

A KMS based IMS media plane security default implementation:

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

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

- Shall support the PRF-HMAC-SHA-256 in all HDR and TP payloads.

- May support PRFs MIKEY-1 in all HDR and TP payloads.

- Shall for KEMAC protection support AES-CM-128 and AES-CM-256 encryption algorithms and the NULL authentication algorithm.

- Shall support HMAC-SHA-256-256 as authentication algorithm in V payloads.

- May support HMAC-SHA-1-160 as authentication algorithm in V payloads.

\*\*\* NEXT CHANGE \*\*\*

# D.4 Profiling of tickets

The default ticket for KMS based IMS media plane security

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

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

- Shall for KEMAC protection support AES-CM-128 and AES-CM-256 as encryption algorithm and the NULL Authentication algorithm.

- Shall support HMAC-SHA-256-256 as authentication algorithm in V payloads.

- May support HMAC-SHA-1-160 as authentication algorithm in V payloads.

- Shall support timestamps of type NTP-UTC-32.

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

- Has ticket type value 2 (defined in MIKEY-TICKET).

- Has subtype value 0 (zero) and version value 0 (zero).

- E flag shall have value 1 due to forking.

- F flag shall have value 1 due to forking.

- G flag shall have value 1.

- H flag shall have value 1.

- I flag shall have value 1 prescribing forking.

- L flag shall have value 0.

- M flag shall have value 0.

- N flag shall have value 1 prescribing that no extensions are used.

- O flag shall have value 1 prescribing that no extensions are used.

- All sub-payloads specified shall be present.

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

- THDR: the first 48bits of the THDR Data shall contain a globally unique identifier of the issuing KMS.

- IDRpsk: shall contain B-TID if the ticket is generated by the initiator. If the KMS generates the ticket it is implementation specific.

\*\*\* NEXT CHANGE \*\*\*

## F.3.1 UE sends a SIP MESSAGE

A UE prepares a protected SIP message as described in TS 24.247 [28], with the difference that S/MIME is applied for content protection. Here S/MIME refers to the pre-shared-key variant of S/MIME defined in Annex I of this TS, and not the RFC 8551 [X2] definition of S/MIME. This variant of S/MIME encrypts and authenticates the MIME content using a symmetric key that is transported inside a TRANSFER\_INIT message. An example of a protected MESSAGE is shown below.

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

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

<Base64 encoded TRANSFER\_INIT message>

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

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

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

- The message is sent to another user using an IMPU in the To header field. The UEs registered under that IMPU are the intended recipients of the content.

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

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

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

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

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

\*\*\* NEXT CHANGE \*\*\*

# G.2 Security for conferencing based on SIP signalling security

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

*e2ae security:*

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

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

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

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

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

*e2e security:*

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

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

It is outside the scope of the solution in the present clause whether the conference server supports TLS for MSRP according to RFC 4975 [21] and/or for BFCP according to RFC 8855 [X3].

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.

\*\*\* NEXT CHANGE \*\*\*

# H.3 Usage with SDP

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

RFC 4567 [12] describes how the key-mgmt attribute is used to perform a MIKEY-TICKET exchange in SDP and how an m-line can be mapped to set of SRTP CSs (one for each SSRC). If the key-mgmt attribute is used at session level then the MIKEY-TICKET exchange contains CSs for all the m-lines in the SDP and the mapping is based on the order of the m-lines. If the key-mgmt attribute is used at the media level then the CSB only contains the CSs for that m-line. Mixing of session and media level attributes is allowed by 4567 [12] 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.

\*\*\* NEXT CHANGE \*\*\*

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

Secure/Multipurpose Internet Mail Extensions (S/MIME), defined in IETF RFC 8551 [X2], is a standard for encryption and signing of MIME encoded data. S/MIME uses Cryptographic Message Syntax (CMS), defined in IETF RFC 5652 [31], to cryptographically protect MIME entities. Unfortunately, S/MIME was designed for public key cryptography and does not specify how a MIME entity can be encrypted and authenticated using a pre-shared key. However, extending S/MIME to support symmetric crypto is not a major issue since CMS already defines the necessary message constructs and algorithms.

# I.1 The smime-type parameter

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

Table I.1: smime-type (addition)

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

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

# I.2 The Auth-Enveloped S/MIME type

## I.2.1 General

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

Table I.2: Authenticated encryption algorithms

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

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

Table I.3: Key encryption algorithms

|  |  |
| --- | --- |
| Algorithm name | Key size |
| AES-WRAP | 128, 256 |

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

## I.2.2 Creating an Auth-Enveloped message

This Clause describes how a MIME entity is protected using the auth-envoloped S/MIME type. With the exception of the second step, the process is identical to the creation of an Enveloped-Only message in S/MIME [X2].

a) The MIME entity to be protected is prepared according to Section 3.1 in S/MIME [X2].

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

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

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

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

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

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

# I.3 Transferring KEK using MIKEY-TICKET

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

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

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

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

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

<Base64 encoded TRANSFER\_INIT message>

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

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

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

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

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

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

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

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

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

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

The Ticket Resolve exchange is unchanged

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

- The F flag shall be set to 0 indicating that TRANSFER\_RESP should not be sent

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

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

- The KEMAC payload in the TICKET shall contain a single TGK with the SPI field set to the value of S/MIME key encryption key identifier. No salt or key validity period shall be included.

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

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

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

\*\*\* NEXT CHANGE \*\*\*

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

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

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

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

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

\*\*\* NEXT CHANGE \*\*\*

## 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

\*\*\* NEXT CHANGE \*\*\*

Annex O (normative): Profiling of DTLS-SRTP

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

**SRTP Protection Profiles:**

The SRTP protection profile "AES\_CM\_128\_HMAC\_SHA1\_80", as defined in RFC 5763 [40] and the SRTP protection profile “SRTP\_AEAD\_AES\_128\_GCM”, as defined in RFC 7714 [XX] are mandatory to support. Support of other protection profiles is optional.

**SRTP Master Key Identifier (MKI):**

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

\*\*\* END OF CHANGES \*\*\*