ETSI TS 103 816-2 V1.1.1 (2021-07)

Publicly Available Specification (PAS);
CYBER;
Connecting Products based on MIKEY-SAKKE;
Part 2: One-to-One Voice Communication

CAUTION

The present document has been submitted to ETSI as a PAS produced by Secure Chorus and approved by the ETSI Technical Committee Cyber Security (CYBER).

Reference
DTS/CYBER-0065-2

Keywords
cyber security, mobile, PAS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Cyber Security (CYBER).

The present document is part 2 of a multi-part deliverable covering Connecting Products based on MIKEY-SAKKE, as identified below:

Part 1: "KMS Certificate Definition";

Part 2: "One-to-One Voice Communication";

Part 3: "One-to-One Messaging";

Part 4: "Group Voice Communication";

Part 5: "Discovery".

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document is intended to specify the one-to-one interface used for voice communications. It is intended for use in connecting products based on Multimedia Internet Keying Sakai-Kasahara Key Encryption (MIKEY-SAKKE) domains and to validate products.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document:

[1] ETSI TS 103 816-1: "Publicly Available Specification (PAS); CYBER; Connecting Products based on MIKEY-SAKKE; Part 1: KMS Certificate Definition".

[2] IETF RFC 3711 (March 2004): "The Secure Real-time Transport Protocol (SRTP)". M. Baugher, D.McGrew, M. Naslund, E. Carrara, K. Norrman.

[3] IETF RFC 3830 (August 2004): "MIKEY; Multimedia Internet KEYing". J. Arkko, E. Carrara, F. Lindholm, M. Naslund, K. Norrman.

[4] IETF RFC 4566 (July 2006): "SDP; Session Description Protocol". M. Handley, V. Jacobson, C. Perkins. .

[5] IETF RFC 6509 (February 2012): "MIKEY-SAKKE; Sakai-Kasahara Key Encryption in Multimedia Internet KEYing (MIKEY)". M. Groves.

[6] IETF RFC 7714 (December 2015): "AES-GCM; Authenticated Encryption in the Secure Real-time Transport Protocol (SRTP)". D. McGrew, K. Igoe.

[7] IETF RFC 6716 (September 2012): "Definition of the Opus Audio Codec". JM. Valin, K. Vos, T. Terriberry.

[8] IETF RFC 4568 (July 2006): "Session Description Protocol (SDP) Security Descriptions for Media Streams". F. Andreasen, M. Baugher, D. Wing.

[9] Web Real-Time Communication (WebRTC): "Media Transport and Use of RTP draft-ietf-rtcweb-rtpusage-17".

[10] IETF RFC 5124 (February 2008): "Extended Secure RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/SAVPF)". J. Ott, E. Carrara.

[11] ETSI TS 124 371: "Web Real Time Communication (WebRTC) Access to IMS".

[12] IETF RFC 3261 (June 2002): "SIP; Session Initiation Protocol". J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler.

[13] IETF RFC 4567 (July 2006): "Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP)". J. Arkko, F. Lindholm, M. Naslund, K. Norrman, E. Carrara.

[14] IETF RFC 6043 (March 2011): "MIKEY-TICKET; Ticket-Based Modes of Key Distribution in Multimedia Internet KEYing (MIKEY)". J. Mattsson, T. Tian.

[15] IANA: "General Extensions Payload Field Names".

NOTE: Available at http://www.iana.org/assignments/mikey-payloads/mikey-payloads.xhtml#mikey-payloads-36.

[16] IETF RFC 4771 (January 2007): "Integrity Transform Carrying Rollover Counter for the Secure Realtime Transport Protocol (SRTP)".

[17] IANA: "MIKEY Security Protocol Parameters".

NOTE: Available at http://www.iana.org/assignments/mikey-payloads/mikey-payloads.xhtml#mikey-payloads-25.

[18] ETSI TS 133 179 (V13.1.0): "LTE; Security of Mission Critical Push To Talk (MCPTT) over LTE (3GPP TS 33.179 version 13.1.0 Release 13)".

[19] ETSI TS 103 816-5: "Publicly Available Specification (PAS); CYBER; Part 5: Discovery".

[20] IETF RFC 4442 (March 2006): "Bootstrapping Timed Efficient Stream Loss-Tolerant Authentication (TESLA)".

[21] IETF RFC 4563 (June 2006): "The Key ID Information Type for the General Extension Payload in Multimedia Internet KEYing (MIKEY)".

[22] IETF RFC 4738 (November 2006): "MIKEY-RSA-R: An Additional Mode of Key Distribution in Multimedia Internet KEYing (MIKEY)".

[23] IETF RFC 4909 (June 2007): "Multimedia Internet KEYing (MIKEY) General Extension Payload for Open Mobile Alliance BCAST LTKM/STKM Transport". .

[24] ETSI TS 133 180 (V15.3.0): "LTE; Security of the mission critical service (3GPP TS 33.180 version 15.3.0 Release 15)".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

Not applicable.

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

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

3GPP	3rd Generation Partnership Project
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Scheme
BCAST	Broadcast
CS	Crypto Session
CSB	Crypto Session Bundle
CSB_ID	Crypto Session Bundle IDentifier
CS-ID	Crypto Session IDentifier
FEC	Forward Error Correction
GCM	Galois/Counter Mode
IANA	Internet Assigned Numbers Authority
IP	Internet Protocol
KDF	Key Derivation Function
KMS	Key Management Server
LTE	Long-Term Evolution
MCPTT	Mission-Critical Push-To-Talk
MIKEY	Multimedia Internet Keying
OMA	Open Mobile Alliance
ROC	Roll Over Counter
RTCP	RTP Control Protocol
RTP	Real-Time Protocol
SAKKE	Sakai-Kasahara Key Encryption
SAVPF	Secure Audio-Visual Profile with Feedback
SDP	Session Description Protocol
SIP	Session Initialisation Protocol
SP	Security Payload
SPI	Security Parameters Index
SRTCP	Secure RTCO
SRTP	Secure Real-time Protocol
SSRC	Synchonisation Source
TESLA	Timed Efficient Stream Loss-Tolerant Authentication
UID	Unique Identifier
URI	Uniform Resource Identifier
VoLTE	Voice-over-LTE
WebRTC	Web Real-Time Communication
WL	Window Lower
WU	Window Upper

4 Overview of One-to-one Connections

4.1 One-to-one Interface

The present document defines the client interface between networks of Vendor Products. It defines two components:

- The signalling channel used to setup the multimedia session.
- The multimedia session itself.

Initially only voice sessions shall be supported. Support for messaging, video and data sessions may be supported in future versions of the present document.

4.2 Use of the interface

It is anticipated that clients from different Vendor Products will not connect directly. Rather interoperability will occur by passing data between the independent Vendor Products networks via a Session Initialization Protocol (SIP) Trunk. The present document defines the data that will be passed between these networks. This is shown in Figure 1.

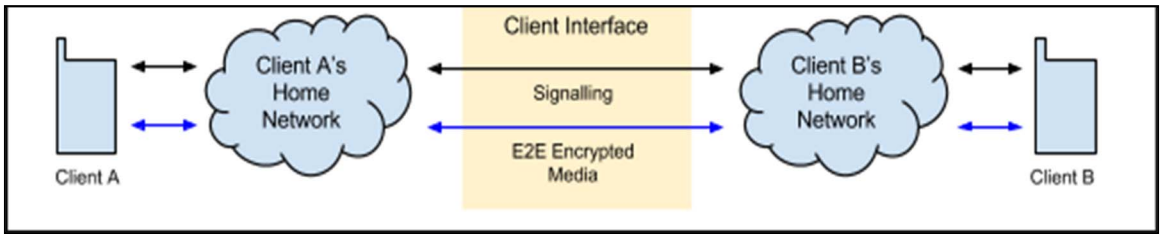

Figure 1: Use of the client interface

As the client interface for Vendor Products is an end-to-end encrypted system, the media profile defined by the present document shall be supported by all the client interface users (as network translation or re-encoding is impossible). All interface clients should also support the signalling profile. Where this is not the case, the client's home network shall translate client signalling to comply with this interface.

4.3 Communication Network

The present document assumes that signalling and session packets are to be routed between the Vendor Products networks. To provide this routing functionality, a SIP Trunk shall be used. The establishment of a client interface for Vendor Products will allow Vendor Products to establish shared infrastructure for inter-network signalling (e.g. via a hub) and for efficient session routing. Operators may use this network.

4.4 Profiles

For signalling, the clients shall support a subset of SIP and Session Description Protocol (SDP), defined in the present document.

For multimedia sessions, clients shall support Secure Real-time Protocol (SRTP). Clients should align with the Web Real-Time Communication (WebRTC) media profile defined in [9] as this will aid wider interoperability.

4.5 One-to-one communications

Client Interfaces are end-points which wish to communicate with other clients and whose identity has been authenticated and provisioned by a technology which is compliant with ETSI TS 103 816-1 [1] and ETSI TS 103 816-5 [19]. No information need be exchanged between clients prior to communication except for identities. Each client shall have been provisioned by their respective Key Management Server (KMS) with appropriate domain information, including the KMS certificate of the other client, as defined in ETSI TS 103 816-1 [1].

NOTE: It is assumed Clients have access to their "home" KMS; scenarios such as migrating a Client to "visit" another network may be considered in future.

4.6 Provisioning

It is assumed that all clients have been provisioned by a KMS. The process for provisioning is out-of-scope of the present document, however a mechanism has been specified within ETSI TS 133 179 [18].

It is also assumed that the initiating client has the KMS certificate for the domain of the receiving client, and the receiving client has the KMS certificate for the initiating client. If either of these assumptions are untrue, the client may request this information from its KMS via the KMS interface. KMS certificates are defined in ETSI TS 103 816-1 [1].

5 Inter-domain Interface

5.1 Setup

To securely communicate using Vendor Products each client of such Vendor Products shall be provisioned with keys corresponding to the client's MIKEY-SAKKE Unique Identifiers (UIDs), along with domain specific information.

Generally, the client will perform a registration process (e.g. SIP REGISTER) with the home network. This process is out of scope of the present document.

To be configured, the client creates a connection to the client's Root KMS, and the KMS verifies the identity of the client. The client makes a request to the KMS which responds with key material, domain information and local domain policy appropriate to the client's request. This process is within the domain of the client's home network and hence out-of-scope of the present document.

5.2 Signalling Flow

Figure 2 shows the basic set-up procedure for the creation of a communication between clients of Vendor Products.

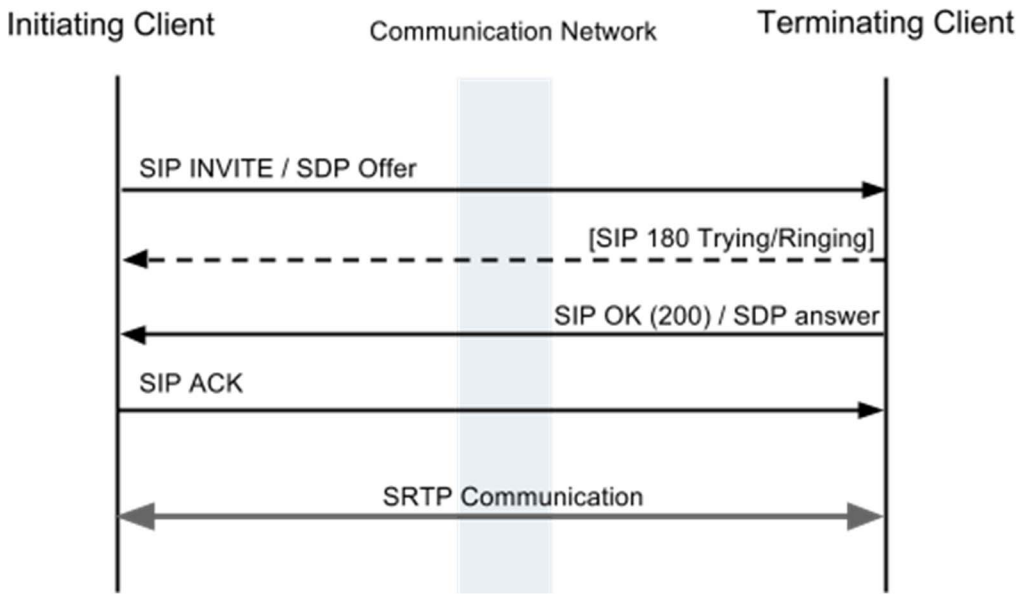

Figure 2: Setup procedure for client-to-client communications

The procedure in Figure 2 is now described step-by-step:

1) Prior to beginning this procedure it is assumed that the clients of Vendor Products have been provisioned by a KMS.

2) Prior to beginning this procedure it is assumed that the clients of Vendor Products have been registered with their serving SIP server within the communication network.

3) The initiating client of a Vendor Product generates a session key and sends a SIP INVITE to the terminating client. This message is routed via the signalling servers of the initiating client and terminating client. The message contains an SDP offer containing details for the up-coming communication. This includes a MIKEY-SAKKE I_MESSAGE as defined in IETF RFC 6509 [5], transporting the session key. The I_MESSAGE may contain a "SAKKE-to-Self" payload defined in [18].

NOTE: This message may be pre-generated to increase the efficiency of the communication.

4) The terminating client receives the message, extracts and processes the SDP offer. As part of this processing, the client checks the signature on the message and extracts the session key from the I_MESSAGE.

5) On successful setup, the terminating client returns an acknowledgement (SIP 200) containing an SDP Answer.

6) The initiating client receives the SIP OK response. If the parameters provided are acceptable, the initiating client returns an ACK.

7) The clients begin an SRTP multimedia communication using the shared session key to key the SRTP session.

6 Signalling Profile

6.1 SIP Profile

The clients shall use SIP as defined in IETF RFC 3261 [12]. The following sections define the subset of SIP which shall be used for Vendor Products.

6.2 SIP Requests

The client shall support the following SIP requests:

- INVITE
- ACK
- CANCEL
- OPTIONS
- BYE

6.3 SIP INVITE

SIP INVITEs shall be addressed to a SIP URI including the domain of the user.

The SIP INVITE message shall include an SDP Offer message which shall include a MIKEY message, specifically a MIKEY-SAKKE I_MESSAGE.

6.4 SIP Responses

Clients shall support the following responses (as defined in Section 21 of IETF RFC 3261 [12]):

- Trying
- Ringing
- OK
- Not found
- Temporarily not available
- Busy here
- Server internal error
- Decline

NOTE: It was originally proposed that the SIP OK (200) responses may include an SDP Answer message which may include a response MIKEY message, specifically a MIKEY-SAKKE I_MESSAGE, but this introduces unnecessary complexity and vulnerabilities.

6.5 SDP Profile

The clients shall use SDP as defined in IETF RFC 4566 [4]. Clients should follow the Voice-over-Long-Term-Evolution (VoLTE) profile defined in ETSI 124 371 [11].

MIKEY-SAKKE messages shall be included using the "key-mgmt" SDP extension defined in IETF RFC 4567,[13].

6.6 Supported SDP Fields

The following SDP fields shall be supported:

- Codec (audio)
- IP
- Port
- key-mgmt (mikey)

Clients shall not use the SDP key field ("k=") defined in IETF RFC 4566 [4].

Clients shall not use the security descriptions field ("a=crypto") defined in IETF RFC 4568 [8].

Only the MIKEY protocol shall be used within the "key-mgmt" SDP extension defined in IETF RFC 4567 [13], any non-MIKEY protocols shall not be supported. If unsupported security fields are received within an SDP message, the client shall reject the session.

6.7 MIKEY Profile

The SDP offer shall include a MIKEY-SAKKE I_MESSAGE defined as in IETF RFC 6509 [5] (containing the fields HDR, T, RAND, [IDRi], [IDRr], [IDRkmsi], [IDRkmsr], [CERT], {SP}, SAKKE, SIGN as described in that document) but with the following clarifications and modifications:

- The HDR payload shall be the first MIKEY payload. See also Annex A "GENERIC ID Map Type"
- The SIGN payload shall be the last MIKEY payload. The MIKEY message shall not include any unsigned content.
- Other MIKEY payloads may occur in any order.

NOTE 1: Payload ordering is implied in IETF RFC 6509 [5] but not mandated; each payload identifies what is in the next payload, therefore a defined order is not needed.

- All IDR payloads shall be included, i.e. IDRi, IDRr, IDRkmsi and IDRkmsr.

NOTE 2: IDR payloads are optional in IETF RFC 6509 [5], but are needed here.

- The IDRkmsi and IDRkmsr shall be the KmsUri as defined in ETSI TS 103 816-1 [1].
- GEN-EXT payloads may be used, but need not be parsed.

NOTE 3: Optional GEN-EXT payloads are mentioned in IETF RFC 3830 [3], but not in IETF RFC 6509 [5].

- The Security Payload (SP) may be omitted or left blank. In this case, the communication shall use the default SRTP security profile.

NOTE 4: If present, the client expects there to be only 1 SP payload.

- The CS-ID map type shall be GENERIC-ID (Value 2) as defined in IETF RFC 6043 [14].
- Within the timestamp payload T, TS-type "0" and "1" shall be supported.
- The optional CERT payload is not used and shall be ignored.

On receipt of an I_MESSAGE, clients should evaluate the time within the MIKEY Timestamp payload (T) against a validity window around the current time (C), upper bounded by WU and lower bounded by WL. If T > C + WU or T < C - WL, then the message should be flagged as being outside of the validity window. It should be that WU = WL = 300 seconds.

NOTE 5: Client behaviour on detecting the I_MESSAGE is outside of the validity window is implementation-specific. It is expected that either the user will be warned, or the communication will be rejected (IETF RFC 6509 [5] expects the latter for replay protection).

7 SRTP Profile

7.1 Media Profile

All clients shall support the RTP/ Secure Audio-Visual Profile with Feedback (SAVPF) Profile as defined in IETF RFC 5124 [10].

Real-Time Control Protocol (RTCP)/ Secure Real-Time Control Protocol (SRTCP) may be supported.

Clients shall establish a SRTP session, as defined in IETF RFC 3711 [2].

Clients shall ignore unknown SRTP header extensions.

NOTE: Clients may align with the RTP/RTCP profile defined for WebRTC [9]. Clients may support the VoLTE RTP/RTCP profile defined in ETSI 124 371 [11].

7.2 Security Profiles

Clients shall use the SRTP encryption profile "AEAD_AES_128_GCM" as defined in IETF RFC 7714 [6] as the default SRTP security profile. See Annex A for further details.

The Key Derivation Function shall be applied on the 12-byte salt provided by AES-GCM without any additional padding.

NOTE: The interpretation of Master Salt used in the Key Derivation Function (KDF) defined in IETF RFC 3711 [2] was taken to mean the Master Salt defined by AEAD_AES_128_GCM such that the KDF is applied on the 12-byte salt provided by AES-GCM without any additional padding, despite the default master salt length in IETF RFC 3711 [2] being defined as 14 octets and the salt provided by AES-GCM being 12 bytes long. This is contrary to many popular implementations, which instead choose to pad the 12-byte salt up to 14 bytes prior to its input into the KDF algorithm, so as to ensure the KDF is identical to that for Advanced Encryption Scheme (AES) in Counter Mode. This approach was formally adopted in errata to IETF RFC 3711 [2] but to avoid backwards compatibility problems the KDF for AES-GCM uses a shorter input salt compared to that of AES in Counter Mode.

7.3 Audio Codecs

Where a client supports audio communications, the client shall support the following audio codec:

- Opus as defined in IETF RFC 6716 [7].

Additional codecs may be supported and a given network may operate solely using these additional codecs but Opus is the codec used for proving interoperability of two or more Vendor Products.

Annex A (normative): Further details

A.1 Vendor use of GEN-EXT payloads

For reference, the payload format is specified in [3] page 50, and IANA's assigned values are given in [15], which (at the time of writing) allow the use of values 241 - 255:

Table A.1: IANA values (for use in GEN-EXT Payload)

Value	Type	Reference
0	VendorID	IETF RFC 3830 [3]
1	SDP IDs	IETF RFC 3830 [3]
2	TESLA I-Key	IETF RFC 4442 [20]
3	Key ID	IETF RFC 4563 [21]
4	CSB_ID	IETF RFC 4738 [22]
5	OMA BCAST	IETF RFC 4909 [23]
6	SAKKE-to-self	ETSI TS 133 180 [24]
6 - 240	Unassigned	
241 - 255	Reserved for Private Use	

NOTE: This may change based on current work in 3GPP regarding GEN-EXT types for Mission Critical Push-To-Talk (MCPTT).

A.2 GENERIC ID Map Type

Clarification of valid values for GENERIC ID Map Type attributes (see IETF RFC 6043 [14] page 33):

Table A.2: Generic ID Map Attributes

Attribute	Valid Values	Reference	Notes
CS ID	1,2	IETF RFC 3830 [3]	HDR payload shall contain TWO GENERIC ID, which correspond to CS ID 1 and 2
Prot type	0	Section 6.10 of IETF RFC 3830 [3]	SRTP
S	0	IETF RFC 6043 [14]	
#P	0,1	IETF RFC 6043 [14]	0 if no SP payload, or 1 if SP payload defined
Ps	See statements below this table	IETF RFC 6043 [14]	If present, matches SP payload policy number
Session Data Length	4	IETF RFC 6043 [14]	4 bytes to match the length of SSRC contained within Session Data
Session Data	See statements below this table	IETF RFC 6043 [14]	Contains SSRC
SPI Length	0	IETF RFC 6043 [14]	
SPI	Not used		

Each GENERIC ID shall specify the same #P and Ps, otherwise the HDR and therefore I_MESSAGE is invalid.

If an invalid GENERIC ID value is found, the I_MESSAGE shall be regarded as invalid.

A.3 Meaning of CS ID

CS ID: 1 equates to Initiator Tx.

CS ID: 2 equates to Initiator Rx.

A.4 MIKEY Security Protocol Parameters

Clarification of valid values for SRTP Types (see [17]).

Table A.3: SRTP Type Clarification

SRTP Type	Meaning	Ref.	Default Value	Description/ Reference	Valid Values	Notes
0	Encryption algorithm	[3]	6	AES-GCM [6]	6	
1	Session Encryption key lenght	[3]	16	16 bytes [6]	16	
2	Authentication algorithm	[3]	0	NULL [6]	0	
3	Session Authentication key length	[3]	N/A	Not Applicable [6]	None	Invalid if specified
4	Session Salt key length	[3]	12	12 bytes [6]	12	
5	SRTP Pseudo Random Function	[3]	0	AES-GCM [6]	0	
6	Key derivation rate	[3]	0		0	Keys are not re-derived based on the SRTP sequence number
7	SRTP encryption off/on	[3]	1	ON [3]	1	
8	SRTCP encryption off/on	[3]	1	ON [3]	1	
9	Sender's FEC order	[3]	0	First FEC, then SRTP [3] and [2]	0	
10	SRTP authentication off/on	[3]	1	ON [3]	1	Potentially not applicable due to AEAD authentication
11	Authentication tag Length	[3]	N/A	Not Applicable [6]	None	Invalid if specified
12	SRTP prefix length	[3]	0		0	Potentially not applicable due to AEAD authentication
13	ROC transmission rate	[16]	N/A		None	Invalid if specified
14	SRTP Authentication algorithm	[16]	N/A		None	Invalid if specified
15	SRTCP Authentication algorithm	[16]	N/A		None	Invalid if specified
16	SRTP Session Authentication key length	[16]	N/A		None	Invalid if specified
17	SRTCP Session Authentication key length	[16]	N/A		None	Invalid if specified
18	SRTP Authentication tag length	[16]	N/A		None	Invalid if specified
19	SRTCP Authentication tag length	[16]	N/A		None	Invalid if specified
20	AEAD authentication tag length	[6]	16	16 bytes [6]	8, 12, or 16	< 16 is not supported by IETF RFC 7714 [6]
21 - 240	Unassigned					
241 - 255	Reserved					

A.5 General Notes (I_MESSAGE SP Payload)

All parameters are considered to be optional, i.e. SP payload may contain 0 to many, or not included at all in I_MESSAGE.

If any parameter is considered invalid, then the entire I_MESSAGE is considered invalid.

History

Document history		
V1.1.1	July 2021	Publication