**3GPP TSG-CT WG1 Meeting #135-eC1-222682\_r1**

**E-Meeting, 6th – 12th April 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.229** | **CR** | **6554** | **rev** | **1** | **Current version:** | **17.6.1** |  |
|  | | | | | | | | |
| *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:*** | Support of e2ae security using DTLS-SRTP for non WebRTC sessions | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eCryptPr | | | | |  | ***Date:*** | | | 2022-03-28 |
|  |  | | | |  | |  | | |  |
| ***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 can be 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:*** | | SA3 added support of end-to-access-edge security for RTP based media using DTLS-SRTP for non WebRTC sessions, as specified in TS 33.328.  Support of e2ae security using DTLS-SRTP for non WebRTC sessions needs to be added in this specification in similar way as it is currently specified for WebRTC sessions. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Clause 4.2B.2: specified new "End-to-access-edge media security using DTLS-SRTP" mechanism.  Clauses 6.1.2, 6.1.3 and 6.7.2.2: specified procedures for the end-to-access-edge media security for RTP media using DTLS-SRTP and certificate fingerprints.  Clauses 7.2A.7.2.2 and 7.2A.7.4.n6: specified new "dtls-srtp" security mechanism which can be labelled by the "mediasec" header field parameter.  Clause A.1.3: new role with respect to security mechanism "End-to-access-edge media security for RTP media using DTLS-SRTP and certificate fingerprints" added in table A.3D.  Clauses A.2.1.2 and A.2.2.2: added that "mediasec header field parameter for marking security mechanisms related to media" capability also applies to end-to-access-edge media security for RTP media using DTLS-SRTP and certificate fingerprints.  Clauses A.3.2.1 and A.3.3.1: added new "end-to-access-edge media security for RTP media using DTLS-SRTP and certificate fingerprints" capability.  Clause A.3.2.2: in table A.319 updated condition c22 that applies to 3GPP\_e2ae-security-indicator (a=3ge2ae). | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | End-to-access-edge security for RTP based media using DTLS-SRTP for non WebRTC sessions will not be supported. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.2B.2, 6.1.2, 6.1.3, 6.7.2.2, 7.2A.7.2.2, 7.2A.7.4.n6 (new), A.1.3, A.2.1.2, A.2.2.2, A.3.2.1, A.3.2.2, A.3.3.1 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\*\*\* First Change \*\*\*

### 4.2B.2 Media security

3GPP TS 33.328 [19C] defines mechanisms for support of security on the media plane.

This document defines the required elements for signalling the support of media security.

The media security mechanisms are summarised as shown in table 4-2.

Table 4-2: Summary of media security mechanisms to the IM CN subsystem

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mechanism | Applicable to media | Support required by UE | Support required by IM CN subsystem entities | Network support outside IM CN subsystem entities |
| End-to-access-edge media security using SDES. | RTP based media only. | Support RFC 3329 additions specified in subclause 7.2A.7 and SDP extensions specified in table A.317, items A.317/34, A.317/36 and A.317/37. | P-CSCF (IMS-ALG) is required.  P-CSCF support of RFC 3329 additions specified in subclause 7.2A.7 and SDP extensions specified in table A.317, items A.317/34, A.317/36 and A.317/37.  (NOTE) | Not applicable. |
| End-to-access-edge media security using DTLS-SRTP. | RTP based media only. | Support RFC 3329 additions specified in subclause 7.2A.7 and SDP extensions specified in table A.317, items A.317/51 and A.317/55. | P-CSCF (IMS-ALG) is required.  P-CSCF support of RFC 3329 additions specified in subclause 7.2A.7 and SDP extensions specified in table A.317, items A.317/51 and A.317/55.  (NOTE) | Not applicable. |
| End-to-access-edge media security for MSRP using TLS and certificate fingerprints. | MSRP based media only. | Support RFC 3329 additions specified in subclause 7.2A.7 and SDP extensions specified in table A.317, items A.317/40, A.317/40A, A.317/51 and A.317/37A. | P-CSCF (IMS-ALG) is required.  P-CSCF support of RFC 3329 additions specified in subclause 7.2A.7 and SDP extensions specified in table A.317, items A.317/40, A.317/40A, A.317/51 and A.317/37A.  (NOTE) | Not applicable. |
| End-to-access-edge media security for BFCP using TLS and certificate fingerprints. | BFCP based media only. | Support RFC 3329 additions specified in subclause 7.2A.7 and SDP extensions specified in table A.317, items A.317/28, A.317/51 and A.317/37B. | P-CSCF (IMS-ALG) is required.  P-CSCF support of RFC 3329 additions specified in subclause 7.2A.7 and SDP extensions specified in table A.317, items A.317/28, A.317/51 and A.317/37B.  (NOTE) | Not applicable. |
| End-to-access-edge media security for UDPTL using DTLS and certificate fingerprints. | UDPTL based media only. | Support RFC 3329 additions specified in subclause 7.2A.7 and SDP extensions specified in table A.317, items A.317/52, A.317/51 and A.317/37C. | P-CSCF (IMS-ALG) is required.  P-CSCF support of RFC 3329 additions specified in subclause 7.2A.7 and SDP extensions specified in table A.317, items A.317/52, A.317/51 and A.317/37C.  (NOTE) | Not applicable. |
| End-to-end media security using SDES. | RTP based media only. | Support SDP extensions specified in table A.317, items A.317/34 and A.317/36. | Not applicable. | Not applicable. |
| End-to-end media security using KMS. | RTP based media only. | Support SDP extensions specified in table A.317, items A.317/34 and A.317/35. | Not applicable. | GBA and KMS support required. |
| End-to-end media security for MSRP using TLS and KMS. | MSRP based media only. | Support SDP extensions specified in table A.317, items A.317/40, A.317/40A and A.317/35, and support RFC 4279 [218]. | Not applicable. | GBA and KMS support required. |
| NOTE: Support of end-to-access-edge media security is determined entirely by the network operator of the P-CSCF, which need not be the same network operator as that of the S-CSCF. | | | | |

For RTP media security using SDES, the UE supports the SDES key management protocol and optionally the KMS key management protocol as defined in 3GPP TS 33.328 [19C] and SRTP as defined in RFC 3711 [169] for secure transport of media.

For end-to-access-edge media security of RTP media using DTLS-SRTP, the UE supports DTLS‑SRTP as defined in RFC 5763 [222] and RFC 5764 [223] with certificate fingerprints as defined in 3GPP TS 33.328 [19C].

For end-to-access-edge media security for MSRP using TLS and certificate fingerprints, the UE supports MSRP over TLS as defined in RFC 4975 [178] and RFC 6714 [214] with certificate fingerprints as defined in 3GPP TS 33.328 [19C].

For end-to-access-edge media security for BFCP using TLS and certificate fingerprints, the UE supports BFCP over TLS as defined in RFC 4583 [108] with certificate fingerprints as defined in 3GPP TS 33.328 [19C].

For end-to-access-edge media security for UDPTL using DTLS and certificate fingerprints, the UE supports UDPTL over DTLS as defined in RFC 7345 [217] and RFC 8842 [240], with certificate fingerprints as defined in 3GPP TS 33.328 [19C].

For end-to-end media security for MSRP using TLS and KMS, the UE supports MSRP over TLS as defined in RFC 4975 [178] and RFC 6714 [214] with pre-shared key ciphersuites as defined in RFC 4279 [218] and the KMS key management protocol as defined in 3GPP TS 33.328 [19C]. The certificate fingerprints are not indicated.

There is no support for media security in the MGCF, because there would be no end-to-end media security support on calls interworked with the CS domain and the CS user. In this release of this document, there is no support for media security in the MRF. End-to-access-edge media security is not impacted by this absence of support.

For emergency calls, it is not expected that PSAPs would support end-to-end media security and therefore the procedures of this document do not allow the UE to establish such sessions with end-to-end media security. End-to-access-edge media security is not impacted and can be used on emergency calls.

When the UE performs the functions of an external attached network (e.g. an enterprise network):

- where end-to-access-edge media security is used, the UE functionality is expected to be in the gateway of the external attached network, and support for further media security is outside the scope of this document; and

- where end-to-end media security is used, the UE functionality is expected to be supported by the endpoints in the attached network.

\*\*\* Next Change \*\*\*

### 6.1.2 Handling of SDP at the originating UE

An INVITE request generated by a UE shall contain a SDP offer and at least one media description. This SDP offer shall reflect the calling user's terminal capabilities and user preferences for the session.

If the desired QoS resources for one or more media streams have not been reserved at the UE when constructing the SDP offer, the UE:

- shall indicate the related local preconditions for QoS as not met, using the segmented status type, as defined in RFC 3312 [30] and RFC 4032 [64], as well as the strength-tag value "mandatory" for the local segment and the strength-tag value either "optional" or as specified in RFC 3312 [30] and RFC 4032 [64] for the remote segment, if the UE uses the precondition mechanism (see subclause 5.1.3.1); and

- if the UE uses the precondition mechanism (see subclause 5.1.3.1), shall not request confirmation for the result of the resource reservation (as defined in RFC 3312 [30]) at the terminating UE.

NOTE 1: Previous versions of this document mandated the use of the SDP inactive attribute. This document does not prohibit specific services from using direction attributes to implement their service-specific behaviours.

If the UE uses the precondition mechanism (see subclause 5.1.3.1), and the desired QoS resources for one or more media streams are available at the UE when the SDP offer is sent, the UE shall indicate the related local preconditions as met, using the segmented status type, as defined in RFC 3312 [30] and RFC 4032 [64], as well as the strength-tag value "mandatory" for the local segment and the strength-tag value either "optional" or as specified in RFC 3312 [30] and RFC 4032 [64] for the remote segment and shall not request confirmation for the result of the resource reservation (as defined in RFC 3312 [30]) at the terminating UE.

NOTE 2: If the originating UE does not use the precondition mechanism (see subclause 5.1.3.1), it will not include any precondition information in the SDP message body.

If the UE indicated support for end-to-access-edge media security using SDES during registration, and the P-CSCF indicated support for end-to-access-edge media security using SDES during registration, then upon generating an SDP offer with an RTP based media, for each RTP based media except those for which the UE requests an end-to-end media security mechanism, the UE shall:

- offer SRTP transport protocol according to RFC 3711 [169] and the profile defined in 3GPP TS 33.328 [19C];

- include the SDP crypto attribute according to RFC 4568 [168] and the profile defined in 3GPP TS 33.328 [19C]; and

- include an SDP "a=3ge2ae:requested" attribute.

If the UE indicated support for the end-to-access-edge media security for RTP media using DTLS-SRTP and certificate fingerprints during registration, and the P-CSCF indicated support for the end-to-access-edge media security for RTP media using DTLS-SRTP and certificate fingerprints during registration, then upon generating an SDP offer with an RTP based media, for each RTP based media except those for which the UE requests an end-to-end media security mechanism, the UE shall:

- offer "UDP/TLS/RTP/SAVP" or "UDP/TLS/RTP/SAVPF" as the transport protocol according to RFC 5763 [222] and RFC 5764 [223] and the profile defined in 3GPP TS 33.328 [19C];

- include the SDP fingerprint attribute according to RFC 8122 [241] and the profile defined in 3GPP TS 33.328 [19C];

- include the SDP "a=3ge2ae:requested" attribute; and

- include the SDP tls-id attribute according to RFC 8842 [240].

If the UE indicated support for the end-to-access-edge media security for MSRP using TLS and certificate fingerprints during registration, and the P-CSCF indicated support for the end-to-access-edge media security for MSRP using TLS and certificate fingerprints during registration, then upon generating an SDP offer with an MSRP based media, for each MSRP based media except those for which the UE requests an end-to-end security mechanism, the UE shall:

- offer MSRP over TLS transport protocol according to RFC 4975 [178], RFC 6714 [214] and the profile defined in 3GPP TS 33.328 [19C];

- include the SDP fingerprint attribute according to RFC 8122 [241] and the profile defined in 3GPP TS 33.328 [19C]; and

- include the SDP "a=3ge2ae:requested" attribute.

NOTE 3: TLS client role and TLS server role are determined according to RFC 6135 [215] (referenced by RFC 6714 [214]). If the SDP answer contains the SDP setup attribute with "active" attribute value, the answerer performs the TLS client role. If the SDP answer contains the SDP setup attribute with "passive" attribute value, the offerer performs the TLS client role.

If the UE indicated support for the end-to-access-edge media security for BFCP using TLS and certificate fingerprints during registration, and the P-CSCF indicated support for the end-to-access-edge media security for BFCP using TLS and certificate fingerprints during registration, then upon generating an SDP offer with an BFCP based media, for each BFCP based media except those for which the UE requests an end-to-end security mechanism, the UE shall:

- offer BFCP over TLS transport protocol according to RFC 4583 [108] and the profile defined in 3GPP TS 33.328 [19C];

- include the SDP fingerprint attribute according to RFC 8122 [241] and the profile defined in 3GPP TS 33.328 [19C]; and

- include the SDP "a=3ge2ae:requested" attribute.

Unless a new TLS session is negotiated, subsequent SDP offers and answers shall not impact the previously negotiated TLS roles.

NOTE 4: RFC 4583 [108] specifies that the SDP answerer will act as the TLS server but leaves the impact of SDP renegotiation on TLS unspecified.

If the UE indicated support for the end-to-access-edge media security for UDPTL using DTLS and certificate fingerprints during registration, and the P-CSCF indicated support for the end-to-access-edge media security for UDPTL using DTLS and certificate fingerprints during registration, then upon generating an SDP offer with an UDPTL based media, for each UDPTL based media except those for which the UE requests an end-to-end security mechanism, the UE shall:

- offer UDPTL over DTLS transport protocol according to RFC 7345 [217], RFC 8842 [240] and the profile defined in 3GPP TS 33.328 [19C];

- include the SDP fingerprint attribute according to RFC 8122 [241] and the profile defined in 3GPP TS 33.328 [19C];

- include the SDP "a=3ge2ae:requested" attribute; and

- include the SDP tls-id attribute according to RFC 8842 [240].

If the P-CSCF did not indicate support for end-to-access-edge media security using neither DTLS-SRTP nor SDES during registration, the UE shall not include an SDP "a=3ge2ae:requested" attribute in any RTP based media in any SDP offer.

If the P-CSCF did not indicate support for the end-to-access-edge media security for MSRP using TLS and certificate fingerprints during registration, the UE shall not include an SDP "a=3ge2ae:requested" attribute in any MSRP based media in any SDP offer.

If the P-CSCF did not indicate support for the end-to-access-edge media security for BFCP using TLS and certificate fingerprints during registration, the UE shall not include an SDP "a=3ge2ae:requested" attribute in any BFCP based media in any SDP offer.

If the P-CSCF did not indicate support for the end-to-access-edge media security for UDPTL using DTLS and certificate fingerprints during registration, the UE shall not include an SDP "a=3ge2ae:requested" attribute in any UDPTL based media in any SDP offer.

The UE shall not include an SDP "a=3ge2ae:requested" attribute in any media other than RTP based, MSRP based, BFCP based and UDPTL based in any SDP offer.

Upon generating an SDP offer with an MSRP based media protected by the end-to-end media security for MSRP using TLS and KMS, the UE shall:

- offer MSRP over TLS transport protocol according to RFC 4975 [178], RFC 6714 [214] and the profile defined in 3GPP TS 33.328 [19C]; and

- include the SDP key-mgmt attribute according to RFC 4567 [167] and the profile defined in 3GPP TS 33.328 [19C];

NOTE 5: SDP fingerprint attribute is not included.

Upon receiving an SDP answer to the SDP offer with the MSRP based media protected by the end-to-end media security for MSRP using TLS and KMS, and if the MSRP based media is accepted and associated with the SDP key-mgmt attribute as described in RFC 4567 [167] and the profile defined in 3GPP TS 33.328 [19C] in the SDP answer, then the UE indicate the pre-shared key ciphersuites according to RFC 4279 [218] and the profile defined in 3GPP TS 33.328 [19C] in TLS handshake of TLS connection transporting the MSRP based media.

When the UE detects that an emergency call is being made, the UE shall not include end-to-end media security on any media in the SDP offer.

Upon generating the SDP offer for an INVITE request generated after receiving a 488 (Not Acceptable Here) response, as described in subclause 5.1.3.1, the SDP offer shall contain a subset of the allowed media types, codecs and other parameters from the SDP message bodies of all 488 (Not Acceptable Here) responses so far received for the same session establishment attempt (i.e. a set of INVITE requests used for the same session establishment). For each media line, the UE shall order the codecs in the SDP offer according to the order of the codecs in the SDP message bodies of the 488 (Not Acceptable Here) responses.

NOTE 6: The UE can attempt a session establishment through multiple networks with different policies and potentially can need to send multiple INVITE requests and receive multiple 488 (Not Acceptable Here) responses from different CSCF nodes. The UE therefore takes into account the SDP message bodies of all the 488 (Not Acceptable Here) responses received related to the same session establishment when building a new INVITE request.

Upon confirming successful local resource reservation, the UE shall create an SDP offer in which the related local preconditions are set to met, using the segmented status type, as defined in RFC 3312 [30] and RFC 4032 [64].

Upon receiving an SDP answer, which includes more than one codec per media stream, excluding the in-band DTMF codec, as described in subclause 6.1.1, the UE shall:

- send an SDP offer at the first possible time, selecting only one codec per media stream; or

- if the UE is participant in a multi-stream multiparty multimedia conference session using simulcast (indicated by the presence of "a=simulcast" SDP attribute(s) in the SDP answer, as defined in RFC 8853 [249]), apply the procedures defined in 3GPP TS 26.114 [9B] annex S.

If the UE sends an initial INVITE request that includes only an IPv6 address in the SDP offer, and receives an error response (e.g., 488 (Not Acceptable Here) with 301 Warning header field) indicating "incompatible network address format", the UE shall send an ACK as per standard SIP procedures. Subsequently, the UE may acquire an IPv4 address or use an existing IPv4 address, and send a new initial INVITE request to the same destination containing only the IPv4 address in the SDP offer.

\*\*\* Next Change \*\*\*

### 6.1.3 Handling of SDP at the terminating UE

Upon receipt of an initial SDP offer in which no precondition information is available, the terminating UE shall in the SDP answer:

- if, prior to sending the SDP answer the desired QoS resources have been reserved at the terminating UE, set the related media streams in the SDP answer to:

- active mode, if the offered media streams were not listed as inactive; or

- inactive mode, if the offered media streams were listed as inactive.

If the terminating UE had previously set one or more media streams to inactive mode and the QoS resources for those media streams are now ready, the UE shall set the media streams to active mode by applying the procedures described in RFC 4566 [39] with respect to setting the direction of media streams.

Upon sending a SDP answer to an SDP offer (which included one or more media lines which was offered with several codecs) the terminating UE shall:

- select exactly one codec per media line and indicate only the selected codec for the related media stream. In addition, the UE may indicate support of the in-band DTMF codec, as described in subclause 6.1.1; or

- if the UE is participant in a multi-stream multiparty multimedia conference session using simulcast (indicated by the presence of "a=simulcast" SDP attribute(s) in the SDP answer, as defined in RFC 8853 [249]), apply the procedures defined in 3GPP TS 26.114 [9B] annex S.

If the terminating UE does not support any of the offered codecs, or there are other parameters not acceptable to the UE, the UE shall send a 488 (Not Acceptable Here) response and shall in the response include an SDP in the message body containing the codecs and parameters supported by the UE.

Upon sending an SDP answer to an SDP offer, with the SDP answer including one or more media streams for which the originating side did indicate its local preconditions as not met, if the precondition mechanism is used by the terminating UE (see subclause 5.1.4.1), the terminating UE shall indicate its local preconditions and request the confirmation for the result of the resource reservation at the originating end point.

NOTE 1: If the terminating UE does not use the precondition mechanism (see subclause 5.1.4.1), it will ignore any precondition information received from the originating UE.

Upon receiving an initial INVITE request that includes the SDP offer containing an IP address type (in the "c=" parameter) that is not supported by the UE, the UE shall:

- if the UE is a UE performing the functions of an external attached network and

1) if the received SDP offer contains an "altc" SDP attribute indicating an alternative and supported IP address; and

2) the UE supports the "altc" SDP attribute;

select an IP address type in accordance with RFC 6947 [228]; or

- otherwise respond with a 488 (Not Acceptable Here) response including a 301 Warning header field indicating "incompatible network address format".

NOTE 2: Upon receiving an initial INVITE request that does not include an SDP offer, the UE can accept the request and include an SDP offer in the first reliable response. The SDP offer will reflect the called user's terminal capabilities and user preferences for the session.

If the UE receives an SDP offer that specifies different IP address type for media (i.e. specify it in the "c=" parameter of the SDP offer) that the UE is using for signalling, and if the UE supports both IPv4 and IPv6 addresses simultaneously, the UE shall accept the received SDP offer. Subsequently, the UE shall either acquire an IP address type or use an existing IP address type as specified in the SDP offer, and include it in the "c=" parameter in the SDP answer.

NOTE 3: Upon receiving an initial INVITE request, that includes an SDP offer containing connection addresses (in the "c=" parameter) equal to zero, the UE will select the media streams that is willing to accept for the session, reserve the QoS resources for accepted media streams, and include its valid connection address in the SDP answer.

If the UE supports the end-to-access-edge media security using SDES, upon receiving an SDP offer containing an RTP based media:

- transported using the SRTP transport protocol as defined in RFC 3711 [169];

- with an SDP crypto attribute as defined in RFC 4568 [168]; and

- with the SDP "a=3ge2ae:applied" attribute;

and if the UE accepts the RTP based media, then the UE shall generate the SDP answer with the related RTP based media:

- transported using the SRTP transport protocol according to RFC 3711 [169] and the profile defined in 3GPP TS 33.328 [19C]; and

- including an SDP crypto attribute according to RFC 4568 [168] and the profile defined in 3GPP TS 33.328 [19C].

If the UE supports the end-to-access-edge media security for RTP media using DTLS-SRTP and certificate fingerprints, upon receiving an SDP offer containing an RTP based media:

- transported using the "UDP/TLS/RTP/SAVP" or "UDP/TLS/RTP/SAVPF" as the transport protocol according to RFC 5763 [222] and RFC 5764 [223];

- with the SDP fingerprint attribute as defined in RFC 8122 [241]; and

- with the SDP "a=3ge2ae:applied" attribute;

and if the UE accepts the RTP based media, then the UE shall generate the SDP answer with the related RTP based media:

- transported using "UDP/TLS/RTP/SAVP" or "UDP/TLS/RTP/SAVPF" as the transport protocol according to RFC 5763 [222] and RFC 5764 [223] and the profile defined in 3GPP TS 33.328 [19C];

- including the SDP fingerprint attribute according to RFC 8122 [241] and the profile defined in 3GPP TS 33.328 [19C]; and

- including the SDP tls-id attribute according to RFC 8842 [240].

If the UE supports the end-to-access-edge media security for MSRP using TLS and certificate fingerprints, upon receiving an SDP offer containing an MSRP based media:

- transported using the MSRP over TLS transport protocol as defined in RFC 4975 [178] and RFC 6714 [214];

- with the SDP fingerprint attribute as defined in RFC 8122 [241]; and

- with the SDP "a=3ge2ae:applied" attribute;

and if the UE accepts the MSRP based media, then the UE shall generate the SDP answer with the related MSRP based media:

- transported using the MSRP over TLS transport protocol according to RFC 4975 [178], RFC 6714 [214] and the profile defined in 3GPP TS 33.328 [19C]; and

- including the SDP fingerprint attribute according to RFC 8122 [241] and the profile defined in 3GPP TS 33.328 [19C].

NOTE 4: TLS client role and TLS server role are determined according to RFC 6135 [215] (referenced by RFC 6714 [214]). If the SDP answer contains the SDP setup attribute with "active" attribute value, the answerer performs the TLS client role. If the SDP answer contains the SDP setup attribute with "passive" attribute value, the offerer performs the TLS client role.

If the UE supports the end-to-access-edge media security for BFCP using TLS and certificate fingerprints, upon receiving an SDP offer containing an BFCP based media:

- transported using the BFCP over TLS transport protocol as defined in RFC 4583 [108];

- with the SDP fingerprint attribute as defined in RFC 8122 [241]; and

- with the SDP "a=3ge2ae:applied" attribute;

and if the UE accepts the BFCP based media, then the UE shall generate the SDP answer with the related BFCP based media:

- transported using the BFCP over TLS transport protocol according to RFC 4583 [108] and the profile defined in 3GPP TS 33.328 [19C]; and

- including the SDP fingerprint attribute according to RFC 8122 [241] and the profile defined in 3GPP TS 33.328 [19C].

Unless a new TLS session is negotiated, subsequent SDP offers and answers shall not impact the previously negotiated TLS roles.

NOTE 5: RFC 4583 [108] specifies that the SDP answerer will act as the TLS server but leaves the impact of SDP renegotiation on TLS unspecified.

If the UE supports the end-to-access-edge media security for UDPTL using DTLS and certificate fingerprints, upon receiving an SDP offer containing an UDPTL based media:

- transported using the UDPTL over DTLS transport protocol as defined in RFC 7345 [217] and RFC 8842 [240];

- with the SDP fingerprint attribute as defined in RFC 8122 [241]; and

- with the SDP "a=3ge2ae:applied" attribute;

and if the UE accepts the UDPTL based media, then the UE shall generate the SDP answer with the related UDPTL based media:

- transported using the UDPTL over DTLS transport protocol according to RFC 7345 [217], RFC 8842 [240] and the profile defined in 3GPP TS 33.328 [19C];

- including the SDP fingerprint attribute according to RFC 8122 [241] and the profile defined in 3GPP TS 33.328 [19C]; and

- including the SDP tls-id attribute according to RFC 8842 [240].

Upon receiving an SDP offer containing an MSRP based media:

- transported using the MSRP over TLS transport protocol as defined in RFC 4975 [178] and RFC 6714 [214]; and

- with the SDP key-mgmt attribute according to RFC 4567 [167] and the profile defined in 3GPP TS 33.328 [19C];

and if the UE accepts the MSRP based media, the UE shall:

1) generate the SDP answer with the related MSRP based media:

a) transported using the MSRP over TLS transport protocol according to RFC 4975 [178], RFC 6714 [214] and the profile defined in 3GPP TS 33.328 [19C]; and

b) include the SDP key-mgmt attribute according to RFC 4567 [167] and the profile defined in 3GPP TS 33.328 [19C]; and

NOTE 6: SDP fingerprint attribute is not included.

2) indicate the pre-shared key ciphersuites according to RFC 4279 [218] and the profile defined in 3GPP TS 33.328 [19C] in TLS handshake of TLS connection transporting the MSRP based media.

If the terminating UE uses the precondition mechanism (see subclause 5.1.4.1), if the desired QoS resources for one or more media streams have not been reserved at the terminating UE when constructing the SDP offer, the terminating UE shall indicate the related local preconditions for QoS as not met, using the segmented status type, as defined in RFC 3312 [30] and RFC 4032 [64], as well as the strength-tag value "mandatory" for the local segment and the strength-tag value either "optional" or as specified in RFC 3312 [30] and RFC 4032 [64] for the remote segment.

NOTE 7: It is out of scope of this specification which media streams are to be included in the SDP offer.

If the terminating UE uses the precondition mechanism (see subclause 5.1.4.1) and if the desired QoS resources for one or more media streams are available at the terminating UE when the SDP offer is sent, the UE shall indicate the related local preconditions as met, using the segmented status type, as defined in RFC 3312 [30] and RFC 4032 [64], as well as the strength-tag value "mandatory" for the local segment and the strength-tag value either "optional" or as specified in RFC 3312 [30] and RFC 4032 [64] for the remote segment.

If the terminating UE sends an UPDATE request to remove one or more media streams negotiated in the session for which a final response to the INVITE request has not been sent yet, the terminating UE sets the ports of the media streams to be removed from the session to zero in the new SDP offer.

NOTE 8: Upon receiving an initial INVITE request with one or more media streams which the terminating UE supports and one or more media streams which the UE does not support, the UE is not expected to reject the INVITE request just because of the presence of the unsupported media stream.

NOTE 9: Previous versions of this document mandated the use of the SDP inactive attribute in the SDP offer if the desired QoS resources for one or more media streams had not been reserved at the originating UE when constructing the SDP offer unless the originating UE knew that the precondition mechanism was supported by the remote UE. The use can still occur when interoperating with devices based on earlier versions of this document.

\*\*\* Next Change \*\*\*

#### 6.7.2.2 IMS-ALG in P-CSCF for media plane security

When the P-CSCF acts as an IMS-ALG, it acts as a B2BUA and modifies the SDP as described as described in 3GPP TS 23.334 [7F].

If the P-CSCF indicated support for end-to-access-edge media security using SDES during registration:

1) upon receiving an SDP offer from the served UE containing an end-to-access-edge protected RTP based media, i.e. a RTP media stream:

- transported using the SRTP transport protocol as defined in RFC 3711 [169];

- with an SDP crypto attribute as defined in RFC 4568 [168]; and

- with the SDP "a=3ge2ae:requested" attribute;

the P-CSCF shall invoke IMS-ALG procedures, will act as defined in 3GPP TS 23.334 [7F] as far as SDP and SRTP is concerned, and shall:

- if the SDP offer contains a Transport Protocol Capability SDP attribute (see RFC 5939 [137]) offering:

a) "RTP/SAVPF" transport, e.g. "a=tcap:*x* RTP/SAVPF", replace this transport with "RTP/AVPF" within that attribute; and

b) "RTP/SAVP" transport, e.g. "a=tcap:*x* RTP/SAVP", replace this transport with "RTP/AVP" within that attribute; and

- strip the SDP "a=3ge2ae:requested" attribute and the SDP crypto attribute from the end-to-access-edge protected RTP based media of the received SDP offer; and

2) upon sending an SDP answer to the SDP offer from the served UE, for each end-to-access-edge protected RTP based media of the SDP offer from the served UE which is accepted in the SDP answer, the P-CSCF will act as defined in 3GPP TS 23.334 [7F] as far as SDP and SRTP is concerned and shall:

- indicate the SRTP transport protocol according to RFC 3711 [169] and the profile defined in 3GPP TS 33.328 [19C]; and

- include a SDP crypto attribute according to RFC 4568 [168] and the profile defined in 3GPP TS 33.328 [19C].

If the served UE indicated support for end-to-access-edge media security using SDES, during registration, and the P-CSCF indicated support for end-to-access-edge 2ae-media security using SDES during registration:

1) upon receiving an SDP offer from remote user with an RTP based media, for each end-to-access-edge protected RTP based media, i.e. a RTP based media except those for which the result of the SDP offer / answer exchange results in the application of an end-to-end media security mechanism, the P-CSCF shall invoke IMS-ALG procedures, will act as defined in 3GPP TS 23.334 [7F] as far as SDP and RTP is concerned, and shall:

- remove any SDP crypto attribute and any "a=acap:*x* crypto" SDP attribute (see RFC 5939 [137]);

- if the SDP offer contains any potential configuration(s) using "RTP/SAVPF" transport or "RTP/SAVP" transport, as offered in corresponding Transport Protocol Capability SDP attribute(s) (see RFC 5939 [137]), (e.g. "a=tcap:*x* RTP/AVPF a=pcfg:*y* t=*x*"), remove those potential configuration(s);

NOTE: Keeping the related "RTP/SAVPF" transport or "RTP/SAVP" transport within a Transport Protocol Capability SDP attribute that also contains other transports avoids a potential need to renumber other transports and adjust other potential configurations in the SDP offer and the actual configuration in the SDP answer accordingly.

- if the SDP offer contains a Transport Protocol Capability SDP attribute (see RFC 5939 [137]) offering:

a) "RTP/AVPF" transport (e.g. "a=tcap:*x* RTP/AVPF"), replace this transport with "RTP/SAVPF" within that attribute; and

b) "RTP/AVP" transport (e.g. "a=tcap:*x* RTP/AVP"), replace this transport with "RTP/SAVP" within that attribute;

- if the SDP offer contains any potential configuration(s) with delete-attribute parameter(s) (see RFC 5939 [137]), (e.g. "a=pcfg:1 a=-sm:1"), remove those potential configuration(s);

- offer SRTP transport protocol according to RFC 3711 [169] and the profile defined in 3GPP TS 33.328 [19C];

- include a SDP crypto attribute according to RFC 4568 [168] and the profile defined in 3GPP TS 33.328 [19C]; and

- include a SDP "a=3ge2ae:applied" attribute; and

2) upon receiving an SDP answer to the SDP offer from remote user, for each accepted end-to-access-edge protected RTP based media, the P-CSCF will act as defined in 3GPP TS 23.334 [7F] as far as SDP and RTP is concerned, and shall remove the SDP crypto attribute.

If the P-CSCF indicated support for the end-to-access-edge media security for RTP media using DTLS-SRTP and certificate fingerprints during registration:

1) upon receiving an SDP offer from the served UE containing an end-to-access-edge protected RTP based media, i.e. an RTP based media:

- transported using "UDP/TLS/RTP/SAVP" or "UDP/TLS/RTP/SAVPF" as the transport protocol according to RFC 5763 [222] and RFC 5764 [223];

- with the SDP fingerprint attribute as defined in RFC 8122 [241];

- with the SDP "a=3ge2ae:requested" attribute; and

- with the SDP tls-id attribute as defined in RFC 8842 [240];

the P-CSCF shall invoke IMS-ALG procedures, will act as defined in 3GPP TS 23.334 [7F] as far as SDP and "RTP/AVP" or "RTP/AVPF" over UDP is concerned, and shall strip the SDP "a=3ge2ae:requested" attribute, the SDP fingerprint attribute and the SDP tls-id attribute from the RTP based media of the received SDP offer; and

2) upon sending an SDP answer to the SDP offer from the served UE, for each end-to-access-edge protected RTP based media of the SDP offer from the served UE that is accepted in the SDP answer, the P-CSCF will act as defined in 3GPP TS 23.334 [7F] as far as SDP and "RTP/AVP" or "RTP/AVPF" over UDP is concerned and shall:

- indicate the "UDP/TLS/RTP/SAVP" or "UDP/TLS/RTP/SAVPF" as the transport protocol according to RFC 5763 [222], RFC 5764 [223] and the profile defined in 3GPP TS 33.328 [19C];

- include the SDP fingerprint attribute according to RFC 8122 [241] and the profile defined in 3GPP TS 33.328 [19C]; and

- include the SDP tls-id attribute as defined in RFC 8842 [240].

If the served UE indicated support for the end-to-access-edge media security for RTP media using DTLS-SRTP and certificate fingerprints during registration, and the P-CSCF indicated support for the end-to-access-edge media security for RTP media using DTLS-SRTP and certificate fingerprints during registration:

1) upon receiving an SDP offer from remote UE with an RTP based media, for each end-to-access-edge protected RTP based media, i.e. an RTP based media except those for which the result of the SDP offer / answer exchange results in the application of an end-to-end security mechanism, the P-CSCF shall invoke IMS-ALG procedures, will act as defined in 3GPP TS 23.334 [7F] as far as SDP and "RTP/AVP" or "RTP/AVPF" over UDP is concerned, and shall:

- remove any SDP fingerprint attribute;

- remove any SDP tls-id attribute;

- offer "UDP/TLS/RTP/SAVP" or "UDP/TLS/RTP/SAVPF" as the transport protocol according to RFC 5763 [222], RFC 5764 [223] and the profile defined in 3GPP TS 33.328 [19C];

- if the SDP offer contains any potential configuration(s) with delete-attribute parameter(s) (see RFC 5939 [137]), (e.g. "a=pcfg:1 a=-sm:1"), remove those potential configuration(s);

- include the SDP fingerprint attribute according to RFC 8122 [241] and the profile defined in 3GPP TS 33.328 [19C];

- include the SDP "a=3ge2ae:applied" attribute; and

- include the SDP tls-id attribute as defined in RFC 8842 [240]; and

2) upon receiving an SDP answer to the SDP offer from remote user, for each accepted end-to-access-edge protected RTP based media, the P-CSCF will act as defined in 3GPP TS 23.334 [7F] as far as SDP and "RTP/AVP" or "RTP/AVPF" over UDP is concerned, and shall remove the SDP fingerprint attribute and SDP tls-id attribute.

If the P-CSCF indicated support for the end-to-access-edge media security for MSRP using TLS and certificate fingerprints during registration:

1) upon receiving an SDP offer from the served UE containing an end-to-access-edge protected MSRP based media, i.e. an MSRP based media:

- transported using the MSRP over TLS transport protocol as defined in RFC 4975 [178] and RFC 6714 [214];

- with the SDP fingerprint attribute as defined in RFC 8122 [241]; and

- with the SDP "a=3ge2ae:requested" attribute;

the P-CSCF shall invoke IMS-ALG procedures, will act as defined in 3GPP TS 23.334 [7F] as far as SDP and MSRP is concerned, and shall strip the SDP "a=3ge2ae:requested" attribute and the SDP fingerprint attribute from the end-to-access-edge protected MSRP based media of the received SDP offer; and

2) upon sending an SDP answer to the SDP offer from the served UE, for each end-to-access-edge protected MSRP based media of the SDP offer from the served UE which is accepted in the SDP answer, the P-CSCF will act as defined in 3GPP TS 23.334 [7F] as far as SDP and MSRP is concerned and shall:

- indicate the MSRP over TLS transport protocol according to RFC 4975 [178], RFC 6714 [214] and the profile defined in 3GPP TS 33.328 [19C]; and

- include the SDP fingerprint attribute according to RFC 8122 [241] and the profile defined in 3GPP TS 33.328 [19C].

If the served UE indicated support for the end-to-access-edge media security for MSRP using TLS and certificate fingerprints during registration, and the P-CSCF indicated support for the end-to-access-edge media security for MSRP using TLS and certificate fingerprints during registration:

1) upon receiving an SDP offer from remote user with an MSRP based media, for each end-to-access-edge protected MSRP based media, i.e. an MSRP based media except those for which the result of the SDP offer / answer exchange results in the application of an end-to-end security mechanism, the P-CSCF shall invoke IMS-ALG procedures, will act as defined in 3GPP TS 23.334 [7F] as far as SDP and MSRP is concerned, and shall:

- remove any SDP fingerprint attribute;

- offer MSRP over TLS transport protocol according to RFC 4975 [178], RFC 6714 [214] and the profile defined in 3GPP TS 33.328 [19C];

- if the SDP offer contains any potential configuration(s) with delete-attribute parameter(s) (see RFC 5939 [137]), (e.g. "a=pcfg:1 a=-sm:1"), remove those potential configuration(s);

- include the SDP fingerprint attribute according to RFC 8122 [241] and the profile defined in 3GPP TS 33.328 [19C]; and

- include the SDP "a=3ge2ae:applied" attribute; and

2) upon receiving an SDP answer to the SDP offer from remote user, for each accepted end-to-access-edge protected MSRP based media, the P-CSCF will act as defined in 3GPP TS 23.334 [7F] as far as SDP and MSRP is concerned, and shall remove the SDP fingerprint attribute.

If the P-CSCF indicated support for the end-to-access-edge media security for BFCP using TLS and certificate fingerprints during registration:

1) upon receiving an SDP offer from the served UE containing an end-to-access-edge protected BFCP based media, i.e. a BFCP based media:

- transported using the BFCP over TLS transport protocol as defined in RFC 4583 [108];

- with the SDP fingerprint attribute as defined in RFC 8122 [241]; and

- with the SDP "a=3ge2ae:requested" attribute;

the P-CSCF shall invoke IMS-ALG procedures, will act as defined in 3GPP TS 23.334 [7F] as far as SDP and BFCP is concerned, and shall strip the SDP "a=3ge2ae:requested" attribute and the SDP fingerprint attribute from the BFCP based media of the received SDP offer; and

2) upon sending an SDP answer to the SDP offer from the served UE, for each end-to-access-edge protected BFCP based media of the SDP offer from the served UE which is accepted in the SDP answer, the P-CSCF will act as defined in 3GPP TS 23.334 [7F] as far as SDP and BFCP is concerned and shall:

- indicate the BFCP over TLS transport protocol according to RFC 4583 [108] and the profile defined in 3GPP TS 33.328 [19C]; and

- include the SDP fingerprint attribute according to RFC 8122 [241] and the profile defined in 3GPP TS 33.328 [19C].

If the served UE indicated support for the end-to-access-edge media security for BFCP using TLS and certificate fingerprints during registration, and the P-CSCF indicated support for the end-to-access-edge media security for BFCP using TLS and certificate fingerprints during registration:

1) upon receiving an SDP offer from remote UE with an BFCP based media, for each end-to-access-edge protected BFCP based media, i.e. a BFCP based media except those for which the result of the SDP offer / answer exchange results in the application of an end-to-end security mechanism, the P-CSCF shall invoke IMS-ALG procedures, will act as defined in 3GPP TS 23.334 [7F] as far as SDP and BFCP is concerned, and shall:

- remove any SDP fingerprint attribute;

- offer BFCP over TLS transport protocol according to RFC 4583 [108] and the profile defined in 3GPP TS 33.328 [19C];

- if the SDP offer contains any potential configuration(s) with delete-attribute parameter(s) (see RFC 5939 [137]), (e.g. "a=pcfg:1 a=-sm:1"), remove those potential configuration(s);

- include the SDP fingerprint attribute according to RFC 8122 [241] and the profile defined in 3GPP TS 33.328 [19C]; and

- include the SDP "a=3ge2ae:applied" attribute; and

2) upon receiving an SDP answer to the SDP offer from remote user, for each accepted end-to-access-edge protected BFCP based media, the P-CSCF will act as defined in 3GPP TS 23.334 [7F] as far as SDP and BFCP is concerned, and shall remove the SDP fingerprint attribute.

If the P-CSCF indicated support for the end-to-access-edge media security for UDPTL over DTLS and certificate fingerprints during registration:

1) upon receiving an SDP offer from the served UE containing an end-to-access-edge protected UDPTL based media, i.e. a UDPTL based media:

- transported using the UDPTL over DTLS transport protocol as defined in RFC 7345 [217] and RFC 8842 [240];

- with the SDP fingerprint attribute as defined in RFC 8122 [241];

- with the SDP "a=3ge2ae:requested" attribute; and

- with the SDP tls-id attribute as defined in RFC 8842 [240];

the P-CSCF shall invoke IMS-ALG procedures, will act as defined in 3GPP TS 23.334 [7F] as far as SDP and UDPTL is concerned, and shall strip the SDP "a=3ge2ae:requested" attribute and the SDP fingerprint attribute and the SDP tls-id attribute from the UDPTL based media of the received SDP offer; and

2) upon sending an SDP answer to the SDP offer from the served UE, for each end-to-access-edge protected UDPTL based media of the SDP offer from the served UE which is accepted in the SDP answer, the P-CSCF will act as defined in 3GPP TS 23.334 [7F] as far as SDP and UDPTL is concerned and shall:

- indicate the UDPTL over DTLS transport protocol according to RFC 7345 [217], RFC 8842 [240] and the profile defined in 3GPP TS 33.328 [19C];

- include the SDP fingerprint attribute according to RFC 8122 [241] and the profile defined in 3GPP TS 33.328 [19C]; and

- include the SDP tls-id attribute as defined in RFC 8842 [240].

If the served UE indicated support for the end-to-access-edge media security for UDPTL using DTLS and certificate fingerprints during registration, and the P-CSCF indicated support for the end-to-access-edge media security for UDPTL using DTLS and certificate fingerprints during registration:

1) upon receiving an SDP offer from remote UE with an UDPTL based media, for each end-to-access-edge protected UDPTL based media, i.e. a UDPTL based media except those for which the result of the SDP offer / answer exchange results in the application of an end-to-end security mechanism, the P-CSCF shall invoke IMS-ALG procedures, will act as defined in 3GPP TS 23.334 [7F] as far as SDP and UDPTL is concerned, and shall:

- remove any SDP fingerprint attribute;

- remove any SDP tls-id attribute;

- offer UDPTL over DTLS transport protocol according to RFC 7345 [217], RFC 8842 [240] and the profile defined in 3GPP TS 33.328 [19C];

- if the SDP offer contains any potential configuration(s) with delete-attribute parameter(s) (see RFC 5939 [137]), (e.g. "a=pcfg:1 a=-sm:1"), remove those potential configuration(s);

- include the SDP fingerprint attribute according to RFC 8122 [241] and the profile defined in 3GPP TS 33.328 [19C];

- include the SDP "a=3ge2ae:applied" attribute; and

- include the SDP tls-id attribute as defined in RFC 8842 [240]; and

2) upon receiving an SDP answer to the SDP offer from remote user, for each accepted end-to-access-edge protected UDPTL based media, the P-CSCF will act as defined in 3GPP TS 23.334 [7F] as far as SDP and UDPTL is concerned, and shall remove the SDP fingerprint attribute and SDP tls-id attribute.

\*\*\* Next Change \*\*\*

##### 7.2A.7.2.2 "mediasec" header field parameter

The "mediasec" header field parameter may be used in the Security- Client, Security-Server, or Security-Verify header fields defined in RFC 3329 [48] to indicate that a header field applies to the media plane. Any one of the media plane security mechanisms supported by both client and server, if any, may be applied when a media stream is started. Or, a media stream may be set up without security.

Values in the Security-Client, Security-Server, or Security-Verify header fields labelled with the "mediasec" header field parameter are specific to the media plane and specific to the secure media transport protocol used on the media plane.

EXAMPLE: Security-Client: sdes-srtp;mediasec

Usage of the "mediasec" header field parameter in mech-parameters rule of RFC 3329 [48] and the syntax of the "mediasec" header field parameter is shown in table 7.2A.7.2.2-1.

Table 7.2A.7.2.2-1

mech-parameters =/ mediasec-param

mediasec-param = "mediasec"

The security mechanisms which can be labelled by the "mediasec" header field parameter are listed in the table 7.2A.7.2.2-2, where each line (other than the first line) indicates a token and a media security mechanism for which the token indicates support.

Table 7.2A.7.2.2-2

mechanism-name =/ ( sdes-srtp-name / msrp-tls-name / bfcp-tls-name / udptl-dtls-name /   
 dtls-srtp-name / token )

sdes-srtp-name = "sdes-srtp" ; End-to-access-edge media security using SDES.

msrp-tls-name = "msrp-tls" ; End-to-access-edge media security for MSRP using TLS and certificate fingerprints.

bfcp-tls-name = "bfcp-tls" ; End-to-access-edge media security for BFCP using TLS and certificate fingerprints.

udptl-dtls-name = "udptl-dtls" ; End-to-access-edge media security for UDPTL using DTLS and certificate fingerprints.

dtls-srtp-name = "dtls-srtp" ; End-to-access-edge media security for RTP using DTLS-SRTP and certificate fingerprints.

\*\*\* Next Change \*\*\*

##### 7.2A.7.4.n6 " dtls-srtp" security mechanism

Editor's note: [WI: eCryptPr, CR#6554] This subclause forms the basis for IANA registration of the value for the mediasec header field parameter. The registration should be performed by MCC when the registry for mediasec parameter values has been created by IANA.

NOTE: This subclause contains information to be provided to IANA for the registration of the media plane security indicator header field parameter.

Contact name, email address, and telephone number:

3GPP Specifications Manager

3gppContact@etsi.org

+33 (0)492944200

The mechanism-name token:

dtls-srtp

The published RFC describing the details of the corresponding security mechanism:

This mechanism is defined in 3GPP TS 24.229.

\*\*\* Next Change \*\*\*

## A.1.3 Roles

Table A.2: Roles

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item | Roles | Reference | RFC status | Profile status |
| 1 | User agent | [26] | o.1 | o.1 |
| 2 | Proxy | [26] | o.1 | o.1 |
| o.1: It is mandatory to support exactly one of these items. | | | | |
| NOTE: For the purposes of the present document it has been chosen to keep the specification simple by the tables specifying only one role at a time. This does not preclude implementations providing two roles, but an entirely separate assessment of the tables shall be made for each role. | | | | |

Table A.3: Roles specific to this profile

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item | Roles | Reference | RFC status | Profile status |
| 1 | UE | 5.1 | n/a | o.1 |
| 1A | UE containing UICC | 5.1 | n/a | c5 |
| 1B | UE without UICC | 5.1 | n/a | c5 |
| 2 | P-CSCF | 5.2 | n/a | o.1 |
| 2A | P-CSCF (IMS-ALG) | [7] | n/a | c6 |
| 3 | I-CSCF | 5.3 | n/a | o.1 |
| 3A | void |  |  |  |
| 4 | S-CSCF | 5.4 | n/a | o.1 |
| 5 | BGCF | 5.6 | n/a | o.1 |
| 6 | MGCF | 5.5 | n/a | o.1 |
| 7 | AS | 5.7 | n/a | o.1 |
| 7A | AS acting as terminating UA, or redirect server | 5.7.2 | n/a | c2 |
| 7B | AS acting as originating UA | 5.7.3 | n/a | c2 |
| 7C | AS acting as a SIP proxy | 5.7.4 | n/a | c2 |
| 7D | AS performing 3rd party call control | 5.7.5 | n/a | c2 |
| 8 | MRFC | 5.8 | n/a | o.1 |
| 8A | MRB | 5.8A | n/a | o.1 |
| 9 | IBCF | 5.10 | n/a | o.1 |
| 9A | IBCF (THIG) | 5.10.4 | n/a | c4 |
| 9B | IBCF (IMS-ALG) | 5.10.5, 5.10.7 | n/a | c4 |
| 9C | IBCF (Screening of SIP signalling) | 5.10.6 | n/a | c4 |
| 9D | IBCF (Privacy protection) | 5.10.8 | n/a | c4 |
| 10 | Additional routeing functionality | Annex I | n/a | c3 |
| 11 | E-CSCF | 5.11 | n/a | o.1 |
| 11A | E-CSCF acting as UA | 5.11.1, 5.11.2, 5.11.3 | n/a | c7 |
| 11B | E-CSCF acting as a SIP Proxy | 5.11.1, 5.11.2 | n/a | c7 |
| 12 | LRF | 5.12 | n/a | o.1 |
| 13 | ISC gateway function | 5.13 | n/a | o.1 |
| 13A | ISC gateway function (THIG) | 5.13.4 | n/a | c8 |
| 13B | ISC gateway function (IMS-ALG) | 5.13.5 | n/a | c8 |
| 13C | ISC gateway function (Screening of SIP signalling) | 5.13.6 | n/a | c8 |
| 14 | Gm based WIC | [8Z] | n/a | o.1 |
| 15 | Transit function | I.3 | n/a | c9 |
| c2: IF A.3/7 THEN o.2 ELSE n/a - - AS.  c3: IF A.3/3 OR A.3/4 OR A.3/5 OR A.3/6 OR A.3/9 THEN o ELSE o.1 - - I-CSCF, S-CSCF, BGCF, MGCF, IBCF.  c4: IF A.3/9 THEN o.3 ELSE n/a - - IBCF.  c5: IF A.3/1 THEN o.4 ELSE n/a - - UE.  c6: IF A.3/2 THEN o ELSE n/a - - P-CSCF.  c7: IF A.3/11 THEN o.5 ELSE n/a - - E-CSCF.  c8: IF A.3/13 THEN o ELSE n/a - - ISC gateway function.  c9 IF A.3/3 OR A.3/4 OR A.3/5 OR A.3/6 OR A.3/9 THEN o ELSE o.1 - - I-CSCF, S-CSCF, BGCF, MGCF, IBCF.  o.1: It is mandatory to support exactly one of these items.  o.2: It is mandatory to support at least one of these items.  o.3: It is mandatory to support at least one of these items.  o.4 It is mandatory to support exactly one of these items.  o.5: It is mandatory to support exactly one of these items. | | | | |
| NOTE: For the purposes of the present document it has been chosen to keep the specification simple by the tables specifying only one role at a time. This does not preclude implementations providing two roles, but an entirely separate assessment of the tables shall be made for each role. | | | | |

Table A.3A: Roles specific to additional capabilities

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item | Roles | Reference | RFC status | Profile status |
| 1 | Presence server | 3GPP TS 24.141 [8A] | n/a | c1 |
| 2 | Presence user agent | 3GPP TS 24.141 [8A] | n/a | c2 |
| 3 | Resource list server | 3GPP TS 24.141 [8A] | n/a | c3 |
| 4 | Watcher | 3GPP TS 24.141 [8A] | n/a | c4 |
| 11 | Conference focus | 3GPP TS 24.147 [8B] | n/a | c11 |
| 12 | Conference participant | 3GPP TS 24.147 [8B] | n/a | c6 |
| 21 | CSI user agent | 3GPP TS 24.279 [8E] | n/a | c7 |
| 22 | CSI application server | 3GPP TS 24.279 [8E] | n/a | c8 |
| 31 | Messaging application server | 3GPP TS 24.247 [8F] | n/a | c5 |
| 32 | Messaging list server | 3GPP TS 24.247 [8F] | n/a | c5 |
| 33 | Messaging participant | 3GPP TS 24.247 [8F] | n/a | c2 |
| 33A | Page-mode messaging participant | 3GPP TS 24.247 [8F] | n/a | c2 |
| 33B | Session-mode messaging participant | 3GPP TS 24.247 [8F] | n/a | c2 |
| 34 | Session-mode messaging intermediate node | 3GPP TS 24.247 [8F] | n/a | c5 |
| 50 | Multimedia telephony service participant | 3GPP TS 24.173 [8H] | n/a | c2 |
| 50A | Multimedia telephony service application server | 3GPP TS 24.173 [8H] | n/a | c9 |
| 51 | Message waiting indication subscriber UA | 3GPP TS 24.606 [8I] | n/a | c2 |
| 52 | Message waiting indication notifier UA | 3GPP TS 24.606 [8I] | n/a | c3 |
| 53 | Advice of charge application server | 3GPP TS 24.647 [8N] | n/a | c8 |
| 54 | Advice of charge UA client | 3GPP TS 24.647 [8N] | n/a | c2 |
| 55 | Ut reference point XCAP server for supplementary services | 3GPP TS 24.623 [8P] | n/a | c3 |
| 56 | Ut reference point XCAP client for supplementary services | 3GPP TS 24.623 [8P] | n/a | c2 |
| 57 | Customized alerting tones application server | 3GPP TS 24.182 [8Q] | n/a | c8 |
| 58 | Customized alerting tones UA client | 3GPP TS 24.182 [8Q] | n/a | c2 |
| 59 | Customized ringing signal application server | 3GPP TS 24.183 [8R] | n/a | c8 |
| 60 | Customized ringing signal UA client | 3GPP TS 24.183 [8R] | n/a | c2 |
| 61 | SM-over-IP sender | 3GPP TS 24.341 [8L] | n/a | c2 |
| 62 | SM-over-IP receiver | 3GPP TS 24.341 [8L] | n/a | c2 |
| 63 | IP-SM-GW | 3GPP TS 24.341 [8L] | n/a | c1 |
| 71 | IP-SM-GW | 3GPP TS 29.311 [15A] | n/a | c10 |
| 81 | MSC Server enhanced for ICS | 3GPP TS 24.292 [8O] | n/a | c12 |
| 81A | MSC server enhanced for SRVCC using SIP interface | 3GPP TS 24.237  [8M] | n/a | c12 |
| 81B | MSC server enhanced for DRVCC using SIP interface | 3GPP TS 24.237 [8M] | n/a | c12 |
| 82 | ICS user agent | 3GPP TS 24.292 [8O] | n/a | c2 |
| 83 | SCC application server | 3GPP TS 24.292 [8O] | n/a | c9 |
| 84 | EATF | 3GPP TS 24.237 [8M] | n/a | c12 |
| 85 | In-dialog overlap signalling application server | Annex N.2, Annex N.3.3 | n/a | c9 |
| 86 | In-dialog overlap signalling UA client | Annex N.2, Annex N.3.3 | n/a | c2 |
| 87 | Session continuity controller UE | 3GPP TS 24.337 [8ZC] | n/a | c2 |
| 88 | ATCF (proxy) | 3GPP TS 24.237 [8M] | n/a | c13 (note 4) |
| 89 | ATCF (UA) | 3GPP TS 24.237 [8M] | n/a | c12 (note 4) |
| 91 | Malicious communication identification application server | 3GPP TS 24.616 [8S] | n/a | c9 |
| 92 | USSI UE | 3GPP TS 24.390 [8W] | n/a | c2 |
| 92A | USSI UE supporting user-initiated USSD operations | 3GPP TS 24.390 [8W] | n/a | c17 |
| 92B | USSI UE supporting network-initiated USSD operations | 3GPP TS 24.390 [8W] | n/a | c17 |
| 93 | USSI AS | 3GPP TS 24.390 [8W] | n/a | c3 |
| 93A | USSI AS supporting user-initiated USSD operations | 3GPP TS 24.390 [8W] | n/a | c18 |
| 93B | USSI AS supporting network-initiated USSD operations | 3GPP TS 24.390 [8W] | n/a | c18 |
| 94 | TP UE | 3GPP TS 24.103 [7G] | n/a | c14 |
| 95 | eP-CSCF (P-CSCF enhanced for WebRTC) | 3GPP TS 24.371 [8Z] | n/a | c15 |
| 101 | Business trunking in static mode of operation application server | 3GPP TS 24.525 [8ZA] | n/a | c16 |
| 102 | MCPTT client | 3GPP TS 24.379 [8ZE] | n/a | c19 |
| 103 | MCPTT server | 3GPP TS 24.379 [8ZE] | n/a | c20 |
| c1: IF A.3/7A AND A.3/7B THEN o ELSE n/a - - AS acting as terminating UA, or redirect server and AS acting as originating UA.  c2: IF A.3/1 THEN o ELSE n/a - - UE.  c3: IF A.3/7A THEN o ELSE n/a - - AS acting as terminating UA, or redirect server.  c4: IF A.3/1 OR A.3/7B THEN o ELSE n/a - - UE or AS acting as originating UA.  c5: IF A.3/7D AND A.3/8 THEN o ELSE n/a - - AS performing 3rd party call control and MRFC (note 2).  c6: IF A.3/1 OR A.3A/11 THEN o ELSE n/a - - UE or conference focus.  c7: IF A.3/1 THEN o ELSE n/a - - UE.  c8: IF A.3/7D THEN o ELSE n/a - - AS performing 3rd party call control.  c9: IF A.3/7A OR A.3/7B OR A.3/7C OR A.3/7D THEN o ELSE n/a - - AS acting as terminating UA, or redirect server, AS acting as originating UA, AS acting as a SIP proxy, AS performing 3rd party call control.  c10: IF A.3/7A OR A.3/7B OR A.3/7D THEN o ELSE n/a - - AS acting as terminating UA, or redirect server, AS acting as originating UA, AS performing 3rd party call control.  c11: IF A.3/7D THEN o ELSE n/a - - AS performing 3rd party call control.  c12: IF A.2/1 THEN o ELSE n/a - - UA.  c13: IF A.2/2 THEN o ELSE n/a - - proxy.  c14: IF A.3/1 OR A.3A/11 THEN o ELSE n/a - - UE or conference focus.  c15: IF A.3/2A THEN o ELSE n/a - - P-CSCF (IMS-ALG).  c16: IF A.3/7A OR A.3/7B THEN o ELSE n/a - - AS acting as terminating UA, or redirect server, AS acting as originating UA.  c17: IF A.3A/92 THEN o.1 ELSE n/a - - USSI UE.  c18: IF A.3A/93 THEN o.2 ELSE n/a - - USSI AS.  c19: IF A.3/1 THEN o ELSE n/a - - UE.  c20: IF A.3/7 THEN o ELSE n/a - - AS.  o.1: It is mandatory to support at least one of these items.  o.2: It is mandatory to support at least one of these items. | | | | |
| NOTE 1: For the purposes of the present document it has been chosen to keep the specification simple by the tables specifying only one role at a time. This does not preclude implementations providing two roles, but an entirely separate assessment of the tables shall be made for each role.  NOTE 2: The functional split between the MRFC and the AS for page-mode messaging is out of scope of this document and they are assumed to be collocated.  NOTE 3: A.3A/63 is an AS providing the IP-SM-GW role to support the transport level interworking defined in 3GPP TS 24.341 [8L]. A.3A/71 is an AS providing the IP-SM-GW role to support the service level interworking for messaging as defined in 3GPP TS 29.311 [15A].  NOTE 4: An ATCF shall support both the ATCF (proxy) role and the ATCF (UA) role. | | | | |

Table A.3B: Roles with respect to access technology

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item | Value used in P-Access-Network-Info header field | Reference | RFC status | Profile status |
| 1 | 3GPP-GERAN | [52] 4.4 | o | c1 |
| 2 | 3GPP-UTRAN-FDD | [52] 4.4 | o | c1 |
| 3 | 3GPP-UTRAN-TDD | [52] 4.4 | o | c1 |
| 4 | 3GPP2-1X | [52] 4.4 | o | c1 |
| 5 | 3GPP2-1X-HRPD | [52] 4.4 | o | c1 |
| 6 | 3GPP2-UMB | [52] 4.4 | o | c1 |
| 7 | 3GPP-E-UTRAN-FDD | [52] 4.4 | o | c1 |
| 8 | 3GPP-E-UTRAN-TDD | [52] 4.4 | o | c1 |
| 8A | 3GPP-E-UTRAN-ProSe-UNR | subclause 7.2A.4 | n/a | c1 |
| 8B | 3GPP-NR-FDD | subclause 7.2A.4 | n/a | c1 |
| 8C | 3GPP-NR-TDD | subclause 7.2A.4 | n/a | c1 |
| 8D | 3GPP-NR-U-FDD | subclause 7.2A.4 | n/a | c1 |
| 8E | 3GPP-NR-U-TDD | subclause 7.2A.4 | n/a | c1 |
| 8W | 3GPP-NR-SAT | subclause 7.2A.4 | n/a | c1 |
| 9 | 3GPP2-1X-Femto | [52] 4.4 | o | c1 |
| 11 | IEEE-802.11 | [52] 4.4 | o | c1 |
| 12 | IEEE-802.11a | [52] 4.4 | o | c1 |
| 13 | IEEE-802.11b | [52] 4.4 | o | c1 |
| 14 | IEEE-802.11g | [52] 4.4 | o | c1 |
| 15 | IEEE-802.11n | [52] 4.4 | o | c1 |
| 16 | IEEE-802.11ac | [52] 4.4 | o | c1 |
| 21 | ADSL | [52] 4.4 | o | c1 |
| 22 | ADSL2 | [52] 4.4 | o | c1 |
| 23 | ADSL2+ | [52] 4.4 | o | c1 |
| 24 | RADSL | [52] 4.4 | o | c1 |
| 25 | SDSL | [52] 4.4 | o | c1 |
| 26 | HDSL | [52] 4.4 | o | c1 |
| 27 | HDSL2 | [52] 4.4 | o | c1 |
| 28 | G.SHDSL | [52] 4.4 | o | c1 |
| 29 | VDSL | [52] 4.4 | o | c1 |
| 30 | IDSL | [52] 4.4 | o | c1 |
| 31 | xDSL | subclause 7.2A.4 | o | c1 |
| 41 | DOCSIS | [52] 4.4 | o | c1 |
| 51 | DVB-RCS2 | [52] 4.4 | o | c1 |
| 52 | 3GPP-UTRAN | [52] 4.4 | o | c2 |
| 53 | 3GPP-E-UTRAN | [52] 4.4 | o | c2 |
| 54 | 3GPP-WLAN | [52] 4.4 | o | c2 |
| 55 | 3GPP-GAN | [52] 4.4 | o | c2 |
| 56 | 3GPP-HSPA | [52] 4.4 | o | c2 |
| 57 | 3GPP2 | [52] 4.4 | o | c2 |
| 58 | untrusted-non-3GPP-VIRTUAL-EPC | subclause 7.2A.4 | n/a | c2 |
| 59 | VIRTUAL-no-PS | subclause 7.2A.4 | n/a | c2 |
| 60 | WLAN-no-PS | subclause 7.2A.4 | n/a | c2 |
| 61 | 3GPP-NR | Subclause 7.2A.4 | n/a | c2 |
| 62 | 3GPP-NR-U | Subclause 7.2A.4 | n/a | c2 |
| 63 | 3GPP-NR-SAT | Subclause 7.2A.4 | n/a | c2 |
| c1: If A.3/1 OR A.3/2 THEN o.1 ELSE n/a - - UE or P-CSCF.  c2: If A.3/2 THEN o.1 ELSE n/a - - P-CSCF.  o.1: It is mandatory to support at least one of these items. | | | | |

Table A.3C: Modifying roles

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item | Roles | Reference | RFC status | Profile status |
| 1 | UE performing the functions of an external attached network | 4.1 |  |  |
| 2 | UE performing the functions of an external attached network operating in static mode | 4.1 |  |  |
| NOTE: This table identifies areas where the behaviour is modified from that of the underlying role. Subclause 4.1 indicates which underlying roles are modified for this behaviour. | | | | |

Table A.3D: Roles with respect to security mechanism

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item | Security mechanism | Reference | RFC status | Profile status |
| 1 | IMS AKA plus IPsec ESP | clause 4.2B.1 | n/a | c1 |
| 2 | SIP digest plus check of IP association | clause 4.2B.1 | n/a | c2 |
| 3 | SIP digest plus Proxy Authentication | clause 4.2B.1 | n/a | c2 |
| 4 | SIP digest with TLS | clause 4.2B.1 | n/a | c2 |
| 5 | NASS-IMS bundled authentication | clause 4.2B.1 | n/a | c2 |
| 6 | GPRS-IMS-Bundled authentication | clause 4.2B.1 | n/a | c2 |
| 7 | Trusted node authentication | clause 4.2B.1 | n/a | c3 |
| 8 | SIP over TLS with client certificate authentication | clause 4.2B.1 | n/a | c6 |
| 20 | End-to-end media security using SDES | clause 4.2B.2 | o | c5 |
| 20A | End-to-access-edge media security for MSRP using TLS and certificate fingerprints | clause 4.2B.2 | n/a | c4 |
| 20B | End-to-access-edge media security for BFCP using TLS and certificate fingerprints | clause 4.2B.2 | n/a | c4 |
| 20C | End-to-access-edge media security for UDPTL using DTLS and certificate fingerprints | clause 4.2B.2 | n/a | c4 |
| 21 | End-to-end media security using KMS | clause 4.2B.2 | o | c5 |
| 22 | End-to-end media security for MSRP using TLS and KMS | clause 4.2B.2 | o | c5 |
| 30 | End-to-access-edge media security using SDES | clause 4.2B.2 | n/a | c4 |
| 31 | End-to-access-edge media security for RTP media using DTLS-SRTP and certificate fingerprints | clause 4.2B.2 | n/a | c7 |
| c1: IF (A.3/1A OR A.3/2 OR A.3/3 OR A.3/4) THEN m ELSE IF A.3/1B THEN o ELSE n/a - - UE containing UICC or P-CSCF or I-CSCF or S-CSCF, UE without UICC.  c2: IF (A.3/1 OR A.3/2 OR A.3/3 OR A.3/4) THEN o ELSE n/a - - UE or P-CSCF or I-CSCF or S-CSCF.  c3: IF (A.3/3 OR A.3/4) THEN o ELSE n/a - - I-CSCF or S-CSCF.  c4: IF (A.3/1 OR A.3/2A) THEN o ELSE n/a - - UE or P-CSCF (IMS-ALG).  c5: IF A.3/1 THEN o - - UE.  c6: IF A.3C/2 THEN m ELSE o - - UE performing the functions of an external attached network operating in static mode.  c7: IF (A.3/14 OR A.3A/95) THEN m ELSE IF (A.3/1 OR A.3/2A) THEN o ELSE n/a - - Gm based WIC or eP-CSCF or UE or P-CSCF (IMS-ALG). | | | | |

\*\*\* Next Change \*\*\*

### A.2.1.2 Major capabilities

Table A.4: Major capabilities

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Item | Does the implementation support | | Reference | RFC status | Profile status |
|  | **Capabilities within main protocol** | |  |  |  |
| 1 | client behaviour for registration? | | [26] subclause 10.2 | o | c3 |
| 2 | registrar? | | [26] subclause 10.3 | o | c4 |
| 2A | registration of multiple contacts for a single address of record | | [26] 10.2.1.2, 16.6 | o | o |
| 2B | initiating a session? | | [26] subclause 13 | o | o |
| 2C | initiating a session which require local and/or remote resource reservation? | | [30] | o | c43 |
| 3 | client behaviour for INVITE requests? | | [26] subclause 13.2 | c18 | c18 |
| 4 | server behaviour for INVITE requests? | | [26] subclause 13.3 | c18 | c18 |
| 5 | session release? | | [26] subclause 15.1 | c18 | c18 |
| 6 | timestamping of requests? | | [26] subclause 8.2.6.1 | o | o |
| 7 | authentication between UA and UA? | | [26] subclause 22.2, [287] | c34 | c34 |
| 8 | authentication between UA and registrar? | | [26] subclause 22.2, [287] | o | c74 |
| 8A | authentication between UA and proxy? | | [26] 20.28, 22.3, [287] | o | c75 |
| 9 | server handling of merged requests due to forking? | | [26] 8.2.2.2 | m | m |
| 10 | client handling of multiple responses due to forking? | | [26] 13.2.2.4 | m | m |
| 11 | insertion of date in requests and responses? | | [26] subclause 20.17 | o | o |
| 12 | downloading of alerting information? | | [26] subclause 20.4 | o | o |
|  | **Extensions** | |  |  |  |
| 13 | SIP INFO method and package framework? | | [25] | o | c100 |
| 13A | legacy INFO usage? | | [25] 2, 3 | o | c90 |
| 14 | reliability of provisional responses in SIP? | | [27] | c19 | c44 |
| 15 | the REFER method? | | [36] | o | c33 |
| 15A | clarifications for the use of REFER with RFC6665? | | [231] | c121 | c121 |
| 15B | explicit subscriptions for the REFER method? | | [232] | o | o |
| 16 | integration of resource management and SIP? | | [30] [64] | c19 | c44 |
| 17 | the SIP UPDATE method? | | [29] | c5 | c44 |
| 19 | SIP extensions for media authorization? | | [31] | o | c14 |
| 20 | SIP specific event notification? | | [28] | o | c13 |
| 22 | acting as the notifier of event information? | | [28] | c2 | c15 |
| 22A | a clarification on the use of GRUUs in the SIP event notification framework? | | [233] | c122 | c122 |
| 23 | acting as the subscriber to event information? | | [28] | c2 | c16 |
| 24 | session initiation protocol extension header field for registering non-adjacent contacts? | | [35] | o | c6 |
| 25 | private extensions to the Session Initiation Protocol (SIP) for network asserted identity within trusted networks? | | [34] | o | m |
| 26 | a privacy mechanism for the Session Initiation Protocol (SIP)? | | [33] | o | m |
| 26A | request of privacy by the inclusion of a Privacy header indicating any privacy option? | | [33] | c9 | c11 |
| 26B | application of privacy based on the received Privacy header? | | [33] | c9 | n/a |
| 26C | passing on of the Privacy header transparently? | | [33] | c9 | c12 |
| 26D | application of the privacy option "header" such that those headers which cannot be completely expunged of identifying information without the assistance of intermediaries are obscured? | | [33] 5.1 | c10 | c27 |
| 26E | application of the privacy option "session" such that anonymization for the session(s) initiated by this message occurs? | | [33] 5.2 | c10 | c27 |
| 26F | application of the privacy option "user" such that user level privacy functions are provided by the network? | | [33] 5.3 | c10 | c27 |
| 26G | application of the privacy option "id" such that privacy of the network asserted identity is provided by the network? | | [34] 7 | c10 | n/a |
| 26H | application of the privacy option "history" such that privacy of the History-Info header is provided by the network? | | [66] 7.2 | c37 | c37 |
| 27 | a messaging mechanism for the Session Initiation Protocol (SIP)? | | [50] | o | c7 |
| 28 | session initiation protocol extension header field for service route discovery during registration? | | [38] | o | c17 |
| 29 | compressing the session initiation protocol? | | [55] | o | c8 |
| 30 | private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP)? | | [52] | o | m |
| 30A | act as first entity within the trust domain for asserted identity? | | [34] | c96 | c97 |
| 30B | act as entity within trust network that can route outside the trust network? | | [34] | c96 | c97 |
| 30C | act as entity passing on identity transparently independent of trust domain? | | [34] | c96 | c98 |
| 31 | the P-Associated-URI header extension? | | [52] 4.1, [52A] 4 | c21 | c22 |
| 32 | the P-Called-Party-ID header extension? | | [52] 4.2, [52A] 4 | c21 | c23 |
| 33 | the P-Visited-Network-ID header extension? | | [52] 4.3, [52A] 4 | c21 | c24 |
| 34 | the P-Access-Network-Info header extension? | | [52] 4.4, [52A] 4, [234] 2 | c21 | c25 |
| 35 | the P-Charging-Function-Addresses header extension? | | [52] 4.5, [52A] 4 | c21 | c26 |
| 36 | the P-Charging-Vector header extension? | | [52] 4.6, [52A] 4 | c21 | c26 |
| 37 | security mechanism agreement for the session initiation protocol? | | [48] | o | c20 |
| 37A | mediasec header field parameter for marking security mechanisms related to media? | | Subclause 7.2A.7 | n/a | c101 |
| 38 | the Reason header field for the session initiation protocol? | | [34A] | o | c68 |
| 38A | carrying Q.850 codes in reason header fields in SIP (Session Initiation Protocol) responses? | | [130] | o | c82 |
| 38B | the location parameter for the SIP Reason header field? | | [255] | o | c131 |
| 39 | an extension to the session initiation protocol for symmetric response routeing? | | [56A] | o | c62 |
| 40 | caller preferences for the session initiation protocol? | | [56B] | C29 | c29 |
| 40A | the proxy-directive within caller-preferences? | | [56B] 9.1 | o.5 | o.5 |
| 40B | the cancel-directive within caller-preferences? | | [56B] 9.1 | o.5 | o.5 |
| 40C | the fork-directive within caller-preferences? | | [56B] 9.1 | o.5 | o.5 |
| 40D | the recurse-directive within caller-preferences? | | [56B] 9.1 | o.5 | o.5 |
| 40E | the parallel-directive within caller-preferences? | | [56B] 9.1 | o.5 | o.5 |
| 40F | the queue-directive within caller-preferences? | | [56B] 9.1 | o.5 | o.5 |
| 41 | an event state publication extension to the session initiation protocol? | | [70] | o | c30 |
| 42 | SIP session timer? | | [58] | c19 | c19 |
| 43 | the SIP Referred-By mechanism? | | [59] | o | c33 |
| 44 | the Session Inititation Protocol (SIP) "Replaces" header? | | [60] | c19 | c38 (note 1) |
| 45 | the Session Inititation Protocol (SIP) "Join" header? | | [61] | c19 | c19 (note 1) |
| 46 | the callee capabilities? | | [62] | o | c35 |
| 47 | an extension to the session initiation protocol for request history information? | | [66] | o | o |
| 47A | application of the "mp" optional header field parameter? | | [66] | o | o |
| 47B | application of the "rc" optional header field parameter? | | [66] | o | o |
| 47C | application of the "np" optional header field parameter? | | [66] | o | o |
| 48 | Rejecting anonymous requests in the session initiation protocol? | | [67] | o | o |
| 49 | session initiation protocol URIs for applications such as voicemail and interactive voice response? | | [68] | o | o |
| 49A | Session Initiation Protocol (SIP) cause URI parameter for service number translation? | | [230] | c118 | c118 |
| 50 | Session Initiation Protocol's (SIP) non-INVITE transactions? | | [84] | m | m |
| 51 | the P-User-Database private header extension? | | [82] 4 | o | c94 |
| 52 | a uniform resource name for services? | | [69] | n/a | c39 |
| 53 | obtaining and using GRUUs in the Session Initiation Protocol (SIP)? | | [93] | o | c40 (note 2) |
| 55 | the Stream Control Transmission Protocol (SCTP) as a Transport for the Session Initiation Protocol (SIP)? | | [96] | o | c42 |
| 56 | the SIP P-Profile-Key private header extension? | | [97] | n/a | n/a |
| 57 | managing client initiated connections in SIP? | | [92] | o | c45 |
| 58 | indicating support for interactive connectivity establishment in SIP? | | [102] | o | c46 |
| 59 | multiple-recipient MESSAGE requests in the session initiation protocol? | | [104] | c47 | c48 |
| 60 | SIP location conveyance? | | [89] | o | c49 |
| 60A | the Location Source parameter for the SIP Geolocation header field? | | [xxx] | o | c134 |
| 61 | referring to multiple resources in the session initiation protocol? | | [105] | c50 | c50 |
| 62 | conference establishment using request-contained lists in the session initiation protocol? | | [106] | c51 | c52 |
| 63 | subscriptions to request-contained resource lists in the session initiation protocol? | | [107] | c53 | c53 |
| 64 | dialstring parameter for the session initiation protocol uniform resource identifier? | | [103] | o | c19 |
| 65 | the P-Answer-State header extension to the session initiation protocol for the open mobile alliance push to talk over cellular? | | [111] | o | c60 |
| 66 | the SIP P-Early-Media private header extension for authorization of early media? | | [109] 8 | o | c58 |
| 67 | number portability parameters for the 'tel' URI? | | [112] | o | c54 |
| 67A | assert or process carrier indication? | | [112] | o | c55 |
| 67B | local number portability? | | [112] | o | c57 |
|  |  | |  |  |  |
| 69 | extending the session initiation protocol Reason header for preemption events | | [115] | c69 | c69 |
| 70 | communications resource priority for the session initiation protocol? | | [116] | o | c70 |
| 70A | inclusion of MESSAGE, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol? | | [116] 4.2 | c72 | c72 |
| 70B | inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol? | | [116] 4.2 | c72 | c72 |
| 71 | addressing an amplification vulnerability in session initiation protocol forking proxies? | | [117] | o | c87 |
| 72 | the remote application identification of applying signalling compression to SIP | | [79] 9.1 | o | c8 |
| 73 | a session initiation protocol media feature tag for MIME application subtypes? | | [120] | o | c59 |
| 74 | SIP extension for the identification of services? | | [121] | o | c61 |
| 75 | a framework for consent-based communications in SIP? | | [125] | c76 | c76 |
| 75A | a relay within the framework for consent-based communications in SIP? | | [125] | c77 | c78 |
| 75B | a recipient within the framework for consent-based communications in SIP? | | [125] | c80 | c79 |
| 76 | a mechanism for transporting user-to user-call control information in SIP? | | [126] | o | c81 |
| 76A | interworking ISDN call control user information with SIP? | | [126A] | c109 | c109 |
| 77 | The SIP P-Private-Network-Indication private-header (P-Header)? | | [134] | o | o |
| 78 | the SIP P-Served-User private header for the 3GPP IM CN subsystem? | | [133] 6 | o | c93 |
| 79 | the SIP P-Served-User header extension for Originating CDIV session case? | | [239] 4 | c126 | c127 |
| 80 | marking SIP messages to be logged? | | [140] | o | c85 |
| 81 | the 199 (Early Dialog Terminated) response code) | | [142] | o | c86 |
| 82 | message body handling in SIP? | | [150] | m | m |
| 83 | indication of support for keep-alive | | [143] | o | c88 |
| 84 | SIP Interface to VoiceXML Media Services? | | [145] | o | c89 |
| 85 | common presence and instant messaging (CPIM): message format? | | [151] | o | c91 |
| 86 | instant message disposition notification? | | [157] | o | c91 |
| 87 | requesting answering modes for SIP? | | [158] | o | c60 |
| 89 | the early session disposition type for SIP? | | [74B] | o | o |
| 91 | The Session-ID header? | | [162] | o | c102 |
| 92 | correct transaction handling for 2xx responses to Session Initiation Protocol INVITE requests? | | [163] | c18 | c18 |
| 93 | addressing Record-Route issues in the Session Initiation Protocol (SIP)? | | [164] | n/a | n/a |
| 94 | essential correction for IPv6 ABNF and URI comparison in RFC3261? | | [165] | m | m |
| 95 | suppression of session initiation protocol REFER method implicit subscription? | | [173] | o | c99 |
| 96 | Alert-Info URNs for the Session Initiation Protocol? | | [175] | o | o |
| 97 | multiple registrations? | | Subclause 3.1 | n/a | c103 |
| 98 | the SIP P-Refused-URI-List private-header? | | [183] | o | c104 |
| 99 | request authorization through dialog Identification in the session initiation protocol? | | [184] | o | c105 |
| 100 | indication of features supported by proxy? | | [190] | o | c106 |
| 101 | registration of bulk number contacts? | | [191] | o | c107 |
| 102 | media control channel framework? | | [146] | o | c108 |
| 103 | S-CSCF restoration procedures? | | Subclause 4.14 | n/a | c110 |
| 104 | SIP overload control? | | [198] | o | c112 |
| 104A | feedback control? | | [199] | c113 | c113 |
| 104B | distribution of load filters? | | [201] | c113 | c114 |
| 105 | handling of a 380 (Alternative service) response? | | Subclauses 5.1.2A.1.1, 5.1.3.1, 5.1.6.8, and 5.2.10 | n/a | c111 |
| 106 | indication of adjacent network in the Via "received-realm" header field parameter? | | [208] | o | c115 |
| 107 | PSAP callback indicator? | | [209] | o | c116 |
| 108 | SIP URI parameter to indicate traffic leg? | | [225] | o | c117 |
| 109 | PCF or PCRF based P-CSCF restoration? | | Subclause 4.14.2 | n/a | c119 |
| 110 | UDM/HSS or HSS based P-CSCF restoration? | | Subclause 4.14.2 | n/a | c120 |
| 111 | the Relayed-Charge header field extension? | | Subclause 7.2.12 | n/a | c123 |
| 112 | resource sharing? | | Subclause 4.15 | n/a | c124 |
| 113 | the Cellular-Network-Info header extension? | | Subclause 7.2.15 | n/a | c125 |
| 114 | the Priority-Share header field extension? | | Subclause 7.2.16 | n/a | c128 |
| 115 | the Response-Source header field extension? | | Subclause 7.2.17 | n/a | o |
| 116 | authenticated identity management in the Session Initiation Protocol? | | [252] | o | c129 |
| 117 | a SIP response code for unwanted calls extension? | | [254] | o | o |
| 118 | the 3GPP PS data off extension | | Subclause 4.17 | n/a | c130 |
| 119 | Content-ID header field in Session Initiation Protocol (SIP)? | | [256] | o | o |
| 120 | Next-Generation Pan-European eCall emergency service? | | [244] | o | c62 |
| 121 | the Attestation-Info header field extension? | Subclause 7.2.18 | | n/a | c132 |
| 122 | the Origination-Id header field extension? | Subclause 7.2.19 | | n/a | c132 |
| 123 | Dynamic services interactions? | Subclause 4.18 | | n/a | c133 |
| 124 | the Additional-Identity header field extension? | Subclause 7.2.20 | | n/a | c135 |
| 125 | RLOS? | Subclause 4.19 | | n/a | c136 |
| 126 | the Priority-Verstat header field extension? | Subclause 7.2.21 | | n/a | c72 |
| c2: IF A.4/20 THEN o.1 ELSE n/a - - SIP specific event notification extension.  c3: IF A.3/1 OR A.3/4 OR A.3A/81 THEN m ELSE n/a - - UE or S-CSCF functional entity or MSC Server enhanced for ICS.  c4: IF A.3/4 THEN m ELSE IF A.3/7 THEN o ELSE n/a - - S-CSCF or AS functional entity.  c5: IF A.4/16 THEN m ELSE o - - integration of resource management and SIP extension.  c6: IF A.3/4 OR A.3/1 OR A.3A/81 THEN m ELSE n/a. - - S-CSCF or UE or MSC Server enhanced for ICS.  c7: IF A.3/1 OR A.3/4 OR A.3/7A OR A.3/7B OR A.3/7D OR A.3/9B OR A.3/13B OR A.3A/83 OR A.3A/89 THEN m ELSE n/a - - UA or S-CSCF or AS acting as terminating UA or AS acting as originating UA or AS performing 3rd party call control or IBCF (IMS-ALG), ISC gateway function (IMS-ALG), SCC application server, ATCF (UA).  c8: IF A.3/1 THEN (IF (A.3B/1 OR A.3B/2 OR A.3B/3 OR A.3B/4 OR A.3B/5 OR A.3B/6 OR A.3B/7 OR A.3B/8 OR A.3B/11 OR A.3B/12 OR A.3B/13 OR A.3B/14 OR A.3B/15) THEN m ELSE o) ELSE n/a - - UE behaviour (based on P-Access-Network-Info usage).  c9: IF A.4/26 THEN o.2 ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  c10: IF A.4/26B THEN o.3 ELSE n/a - - application of privacy based on the received Privacy header.  c11: IF A.3/1 OR A.3/6 OR A.3A/81 OR A.3A/81A OR A.3A/81B THEN o ELSE IF A.3/9B OR A.3/13B THEN m ELSE n/a - - UE or MGCF, IBCF (IMS-ALG), ISC gateway function (IMS-ALG), MSC Server enhanced for ICS, MSC server enhanced for SRVCC using SIP interface, MSC server enhanced for DRVCC using SIP interface.  c12: IF A.3/7D OR A3A/84 OR A.3A/89 THEN m ELSE n/a - - AS performing 3rd-party call control, EATF, ATCF (UA).  c13: IF A.3/1 OR A.3/2 OR A.3/4 OR A.3/9B OR A.3/11 OR A.3/12 OR A.3/13B OR A.3A/81 THEN m ELSE o - - UE or S-CSCF or IBCF (IMS-ALG) or E-CSCF or LRF or ISC gateway function (IMS-ALG) or MSC Server enhanced for ICS.  c14: IF A.3/1 AND A4/2B AND (A.3B/1 OR A.3B/2 OR A.3B/3) THEN m ELSE IF A.3/2 THEN o ELSE n/a – UE and initiating sessions and GPRS IP-CAN or P-CSCF.  c15: IF A.4/20 AND (A.3/4 OR A.3/9B OR A.3/11 OR A.3/13B) THEN m ELSE o – SIP specific event notification extensions and S-CSCF or IBCF (IMS-ALG) or E-CSCF or ISC gateway function (IMS-ALG).  c16: IF A.4/20 AND (A.3/1 OR A.3/2 OR A.3/9B OR A.3/12 OR A.3/13B OR A.3A/81) THEN m ELSE o - - SIP specific event notification extension and UE or P-CSCF or IBCF (IMS-ALG) or MSC Server enhanced for ICS or LRF or ISC gateway function (IMS-ALG).  c17: IF A.3/1 OR A.3/4 OR A.3A/81 THEN m ELSE n/a - - UE or S-CSCF or MSC Server enhanced for ICS.  c18: IF A.4/2B THEN m ELSE n/a - - initiating sessions.  c19: IF A.4/2B THEN o ELSE n/a - - initiating sessions.  c20: IF A.3/1 AND (A.3D/1 OR A.3D/4) THEN m ELSE n/a - - UE and (IMS AKA plus IPsec ESP or SIP digest with TLS).  c21: IF A.4/30 THEN o.4 ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP).  c22: IF A.4/30 AND (A.3/1 OR A.3/4 OR A.3A/81) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and S-CSCF or UE or MSC Server enhanced for ICS.  c23: IF A.4/30 AND (A.3/1 OR A.3A/81) THEN o ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and UE or MSC Server enhanced for ICS.  c24: IF A.4/30 AND (A.3/4 OR A.3A/81 OR A.3A/81A) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and S-CSCF or MSC Server enhanced for ICS or MSC server enhanced for SRVCC using SIP interface.  c25: IF A.4/30 AND (A.3A/81 OR A.3/4 OR A.3/6 OR A.3/7A OR A.3/7D OR A.3/9B OR A.3/13B OR A3A/84 OR A.3A/81A OR A.3A/81B) THEN m ELSE IF A.4/30 AND A.3/1 AND (A.3B/1OR A.3B/2 OR A.3B/3 OR A.3B/4 OR A.3B/5 OR A.3B/6 OR A.3A/7 OR A.3A/8 OR A.3B/11OR A.3B/12 OR A.3B/13 OR A.3B/14 OR A.3A/15 OR A.3B/41) THEN m ELSE IF A4/30 AND A.3/1 AND (A.3B/21 OR A.3B/22 OR A.3B/23 OR A.3B/24 OR A.3B/25 OR A.3B/26 OR A.3A/27 OR A.3A/28 OR A.3B/29 OR A.3B/30) THEN o ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP), MSC Server enhanced for ICS, S-CSCF, MGCF or AS acting as terminating UA or AS acting as third-party call controller or IBCF (IMS-ALG), ISC gateway function (IMS-ALG), UE, EATF, P-Access-Network-Info values or MSC server enhanced for SRVCC using SIP interface, MSC server enhanced for DRVCC using SIP interface.  c26: IF A.4/30 AND (A.3A/81 OR (A.3/4 AND A.4/2) OR A.3/6 OR A.3/7A OR A.3/7B or A.3/7D OR A.3/9B OR A.3/13B OR A3A/84 OR A.3A/89 OR A.3A/81A OR A.3A/81B) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) MSC Server enhanced for ICS, S-CSCF, registrar, MGCF, AS acting as a terminating UA, or AS acting as an originating UA, or AS acting as third-party call controller, IBCF (IMS-ALG), ISC gateway function (IMS-ALG), EATF, ATCF (UA), MSC server enhanced for SRVCC using SIP interface, MSC server enhanced for DRVCC using SIP interface.  c27: IF A.3/7D OR A.3/9D THEN o ELSE x - - AS performing 3rd party call control, IBCF (Privacy).  c29: IF A.4/40A OR A.4/40B OR A.4/40C OR A.4/40D OR A.4/40E OR A.4/40F THEN m ELSE n/a - - support of any directives within caller preferences for the session initiation protocol.  c30: IF A.3A/1 OR A.3A/2 THEN m ELSE IF A.3/1 OR A.3/11A OR A.3/2A THEN o ELSE n/a - - presence server, presence user agent, UE, AS, E-CSCF acting as UA, P-CSCF (IMS-ALG). | | | | | |
| c33: IF A.3/9B OR A.3/12 OR A.3/13B OR A.3A/81 OR A.3A/11 OR A.3A/12 OR A.4/44 OR A.3A/81A OR A.3A/81B THEN m ELSE o - - IBCF (IMS-ALG) or LRF or ISC gateway function (IMS-ALG) or MSC Server enhanced for ICS or conference focus or conference participant or the Session Inititation Protocol (SIP) "Replaces" header, MSC server enhanced for SRVCC using SIP interface, MSC server enhanced for DRVCC using SIP interface.  c34: IF A.4/44 OR A.4/45 OR A.3/9B OR A.3/13 THEN m ELSE n/a - - the Session Inititation Protocol (SIP) "Replaces" header or the Session Inititation Protocol (SIP) "Join" header or IBCF (IMS-ALG) or ISC gateway function (IMS-ALG).  c35: IF A.3/4 OR A.3/9B OR A.3/13B OR A.3A/82 OR A.3A/83 OR A.3A/21 OR A.3A/22 OR A3A/84 THEN m ELSE IF (A.3/1 OR A.3/6 OR A.3/7 OR A.3/8 OR A.3A/81 OR A.3A/81A OR A.3A/81B) THEN o ELSE n/a - - S-CSCF or IBCF (IMS-ALG) or ISC gateway function (IMS-ALG) functional entities or ICS user agent or SCC application server or CSI user agent or CSI application server, UE or MGCF or AS or MRFC functional entity or MSC Server enhanced for ICS or EATF or MSC server enhanced for SRVCC using SIP interface, MSC server enhanced for DRVCC using SIP interface.  c37 IF A.4/47 THEN o.3 ELSE n/a - - an extension to the session initiation protocol for request history information.  c38: IF A.4/2B AND (A.3A/11 OR A.3A/12 OR A.3/7D) THEN m ELSE IF A.4/2B THEN o ELSE n/a - - initiating sessions, conference focus, conference participant, AS performing 3rd party call control.  c39: IF A.3/1 THEN m ELSE IF A.3/7B OR A.3/7D OR A.3/9 THEN o ELSE n/a - - UE, AS acting as an originating UA, or AS acting as third-party call controller, IBCF.  c40 IF A.3/4 OR (A.3/1 AND NOT A.3C/1) OR A.3A/81 OR A.4/22 THEN m ELSE IF (A.3/7A OR A.3/7B OR A.3/7D) THEN o ELSE n/a - - S-CSCF, UE, UE performing the functions of an external attached network, MSC Server enhanced for ICS, notifier of event information, AS, AS acting as terminating UA, or redirect server, AS acting as originating UA, AS performing 3rd party call control.  c42: IF A.3/1 THEN n/a ELSE o - - UE.  c43: IF A.4/2B THEN o ELSE n/a - - initiating sessions.  c44: IF A.4/2C THEN m ELSE o - - initiating a session which require local and/or remote resource reservation.  c45: IF A.4/97 THEN m ELSE n/a - - multiple registrations.  c46 IF A.3/1 OR A.3/4 THEN o ELSE n/a - - UE, S-CSCF.  c47: IF A.4/27 THEN o ELSE n/a - - a messaging mechanism for the Session Initiation Protocol (SIP).  c48: IF A.3A/32 AND A.4/27 THEN m ELSE IF A.4/27 THEN o ELSE n/a - - messaging list server, a messaging mechanism for the Session Initiation Protocol (SIP).  c49: IF A.3/1 OR A.3/9B OR A.3/13B OR A.3A/81 OR A.3/11 OR A.3/12 OR A3A/84 THEN m ELSE o - - UE, IBCF (IMS-ALG), ISC gateway function (IMS-ALG), MSC Server enhanced for ICS, E-CSCF, LRF, EATF.  c50: IF A.3A/81 OR A.3A/81A OR A.3A/81B THEN n/a ELSE IF A.4/15 THEN o ELSE n/a - - MSC Server enhanced for ICS, MSC server enhanced for SRVCC using SIP interface, MSC server enhanced for DRVCC using SIP interface, the REFER method.  c51: IF A.4/2B THEN o ELSE n/a - - initiating a session.  c52: IF A.3A/11 AND A.4/2B THEN m ELSE IF A.4/2B THEN o ELSE n/a - - conference focus, initiating a session.  c53: IF A.3A/81 THEN n/a ELSE IF A.4/20 THEN o ELSE n/a - - MSC Server enhanced for ICS, SIP specific event notification.  c54: IF A.3/1 OR A.3/6 OR A.3/7A OR A.3/7D OR A.3/9 THEN o, ELSE n/a - - UE, MGCF, AS acting as originating UA, AS performing 3rd party call control, IBCF.  c55: IF A.4/67 THEN m ELSE n/a - - number portability parameters for the 'tel' URI.  c57: IF A.4/67 THEN m ELSE n/a - - number portability parameters for the 'tel' URI.  c58: IF A.3/9B OR A.3/13B OR A.3/6 OR A.3A/81 OR A.3A/81A OR A.3A/81B THEN m ELSE o - - IBCF (IMS-ALG), ISC gateway function (IMS-ALG), MGCF, MSC Server enhanced for ICS, MSC server enhanced for SRVCC using SIP interface, MSC server enhanced for DRVCC using SIP interface.  c59: IF A.3/4 THEN m ELSE IF (A.3/1 OR A.3/6 OR A.3/7A OR A.3/7B OR A.3/7D OR A.3/8) THEN o ELSE n/a - - S-CSCF, UE, MGCF, AS, AS acting as terminating UA, or redirect server, AS acting as originating UA, AS performing 3rd party call control, or MRFC.  c60: IF A.3/9B OR A.3/13B THEN m ELSE IF A.3/1 OR A.3/7A OR A.3/7B OR A.3/7D THEN o ELSE n/a - - IBCF (IMS-ALG), ISC gateway function (IMS-ALG), UE, AS acting as terminating UA, AS acting as originating UA, AS performing 3rd party call control.  c61: IF (A.3/1 OR A.3A/81 OR A.3/6 OR A.3/7A OR A.3/7B OR A.3/7D OR A.3/8 OR A.3/9B OR A.3/13 OR A3A/84 OR A.3A/81A OR A.3A/81B) THEN o ELSE n/a - - UE, MSC Server enhanced for ICS, MGCF, AS, AS acting as terminating UA, or redirect server, AS acting as originating UA, AS performing 3rd party call control, or MRFC or IBCF (IMS-ALG), ISC gateway function (IMS-ALG), EATF, MSC server enhanced for SRVCC using SIP interface, MSC server enhanced for DRVCC using SIP interface.  c62: IF A.3/1 THEN o ELSE n/a - - UE.  c68: IF A.3/2A OR A.3/9 OR A.4/69 OR A.3A/83 THEN m ELSE o - - P-CSCF (IMS-ALG), IBCF, extending the session initiation protocol Reason header for preemption events and Q.850 causes, SCC application server.  c69: IF A.4/70 THEN o ELSE n/a - - communications resource priority for the session initiation protocol.  c70: IF A.3/9B OR A.3/13B OR A.3A/102 OR A.3A/103 THEN m ELSE IF A.3/1 OR A.3/6 OR A.3/7 OR A.3/7A OR A.3/7B OR A.3/7D OR A.3A/81 OR A.3A/81A OR A.3A/81B THEN o ELSE n/a - - IBCF (IMS-ALG), ISC gateway function (IMS-ALG), MCPTT client, MCPTT server, UE, MGCF, AS, AS acting as terminating UA, or redirect server, AS acting as originating UA, AS performing 3rd party call control, MSC Server enhanced for ICS, MSC server enhanced for SRVCC using SIP interface, MSC server enhanced for DRVCC using SIP interface.  c72: IF A.4/70 THEN o ELSE n/a - - communications resource priority for the session initiation protocol | | | | | |
| c74: IF A.3/4 OR A.3/1 THEN o ELSE n/a. - - S-CSCF or UE.  c75: IF A.3/1 THEN o ELSE n/a. - - UE.  c76: IF A.4/75A OR A.4/75B THEN m ELSE n/a - - a relay within the framework for consent-based communications in SIP, a recipient within the framework for consent-based communications in SIP.  c77: IF A.4/59 OR A.4/61 OR A.4/62 OR A.4/63 THEN m ELSE o - - multiple-recipient MESSAGE requests in the session initiation protocol, referring to multiple resources in the session initiation protocol, conference establishment using request-contained lists in the session initiation protocol, subscriptions to request-contained resource lists in the session initiation protocol.  c78: IF (A.4/59 OR A.4/61 OR A.4/62 OR A.4/63) AND (A.3A/11 OR A.3A/31) THEN m ELSE o - - multiple-recipient MESSAGE requests in the session initiation protocol, referring to multiple resources in the session initiation protocol, conference establishment using request-contained lists in the session initiation protocol, subscriptions to request-contained resource lists in the session initiation protocol, conference focus, messaging application server.  c79: IF A.3/9B OR A.3/13B OR (A.3/1 AND (A.4/2B OR A.4/15 OR A.4/20 OR A.4/27)) THEN m ELSE IF A.3/6 OR A.3/7A OR A.3/7D THEN o ELSE n/a - - IBCF (IMS-ALG), ISC gateway function (IMS-ALG), UE, initiating a session, the REFER method, SIP specific event notification, a messaging mechanism for the Session Initiation Protocol (SIP), AS acting as terminating UA, or redirect server, AS performing 3rd party call control.  c80: IF A.4/2B OR A.4/15 OR A.4/20 OR A.4/27 THEN m ELSE n/a - - initiating a session, the REFER method, SIP specific event notification, a messaging mechanism for the Session Initiation Protocol (SIP).  c81: IF A.3/1 OR A.3/6 OR A.3/7A OR A.3/7B OR A.3/7D THEN o ELSE IF A.3/9B OR A.3/13B THEN m ELSE n/a - - UE, MGCF, AS acting as terminating UA, or redirect server, AS acting as originating UA, AS performing 3rd party call control, IBCF (IMS-ALG), ISC gateway function (IMS-ALG).  c82: IF A.3/6 OR A.3A/81 OR A.3A/81A OR A.3A/81B THEN m ELSE n/a - - MGCF, MSC server enhanced for ICS, MSC server enhanced for SRVCC using SIP interface, MSC server enhanced for DRVCC using SIP interface.  c85: IF A.3/1 OR A.3/6 OR A.3A/81 OR A.3A/81A OR A.3A/81B OR A.3/2 OR A.3/7B THEN m ELSE n/a - - UE, MGCF, MSC Server enhanced for ICS, MSC Server enhanced for SRVCC using SIP interface, MSC Server enhanced for DRVCC using SIP interface, P-CSCF, AS acting as originating UA.  c86: IF A.4/3 OR A.4/4 THEN m ELSE n/a - - client behaviour for INVITE requests, server behaviour for INVITE requests.  c87: IF A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C THEN m ELSE o - - IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling).  c88: IF A.3/1 OR A.3/2 THEN m ELSE o - - UE, P-CSCF.  c89: IF A.3/7A OR A.3/8 THEN o ELSE n/a - - AS performing 3rd party call control, MRFC.  c90: IF A.4/13 OR A.3A/53 OR A.3A/54 OR A.3A/91 OR A.3A/85 OR A.3A/86 THEN m ELSE o - - SIP INFO method and package framework, advice of charge application server, advice of charge UA client, malicious communication identification application server, in-dialog overlap signalling application server, in-dialog overlap signalling UA client.  c91: IF A.3A/61 OR A.3A/62 OR A.3A/63 OR A.3A/71 THEN m ELSE o - - SM-over-IP sender, SM-over-IP receiver, IP-SM-GW, IP-SM-GW.  c93: IF A.3/7B OR A.3/7D OR A3A/84 THEN o ELSE n/a - - AS acting as originating UA, AS performing 3rd party call control, EATF.  c94: IF A.3/4 OR A.3/7A OR A.3/7D THEN o ELSE n/a - - S-CSCF and AS acting as terminating UA or redirect server or AS performing 3rd party call control.  c96: IF A.4/30 THEN o ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.  c97: IF (A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C) AND A.4/30 THEN m ELSE IF (A.3/7D OR A.3/11 OR A.3C/1) AND A.4/30 THEN o ELSE n/a - - IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling), AS performing 3rd party call control, E-CSCF, UE performing the functions of an external attached network and extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.  c98: IF A.3/7D OR A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C OR A.3C/1 OR A3A/84 OR A.3A/89 THEN m ELSE n/a - - AS performing 3rd party call control, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling), UE performing the functions of an external attached network, EATF, ATCF (UA).  c99: IF A.4/15 AND (A.3/9B OR A.3/9C OR A.13/B OR A.13/C) THEN m ELSE IF A.4/15 THEN o ELSE n/a - - the REFER method, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling).  c100: IF A.3/6 OR A.3A/57 OR A.3A/58 OR A.3A/59 OR A.3A/60 OR A.3A/81 OR A.3A/81A OR A.3A/81B THEN m ELSE o - - MGCF, customized alerting tones application server, customized alerting tones UA client, customized ringing signal application server, customized ringing signal UA client, MSC server enhanced for ICS, MSC server enhanced for SRVCC using SIP interface, MSC server enhanced for DRVCC using SIP interface.  c101: IF A.3D/30 OR A.3D/20A OR A.3D/20B OR A.3D/20C OR A.3D/31 THEN m ELSE n/a - - end-to-access-edge media security using SDES, end-to-access-edge media security for MSRP using TLS and certificate fingerprints, end-to-access-edge media security for BFCP using TLS and certificate fingerprints, end-to-access-edge media security for UDPTL using DTLS and certificate fingerprints, end-to-access-edge media security for RTP media using DTLS-SRTP and certificate fingerprints.  c102: IF A.3A/11 OR A.3A/12 OR A.3/9 THEN m ELSE n/a - - conference focus, conference participant, IBCF.  c103: IF A.3/1 THEN o ELSE IF A.3/2 OR A.3/4 THEN m ELSE n/a - - UE, P-CSCF, S-CSCF.  c104: IF A.3/9B OR A.3/13B THEN m ELSE IF A.3/7A OR A.3/7B OR A.3/7D THEN o ELSE n/a - - IBCF (IMS-ALG), ISC gateway function (IMS-ALG), AS acting as terminating UA, AS acting as originating UA, AS performing 3rd party call control. | | | | | |
| c105: IF A.3/9B OR A.3/13B OR A.3A/82 OR A.3A/83 OR A.3A/87 OR A.3A/89 THEN m ELSE o - - IBCF (IMS-ALG), ISC gateway function (IMS-ALG), ICS user agent, SCC application server, Session continuity controller UE, ATCF (UA).  c106: IF A.3A/50A OR A.3A/83 OR A.3A/89 THEN m ELSE o - - Multimedia telephony application server, SCC application server, ATCF (UA).  c107: IF A.3C/1 OR A.4/2 THEN o ELSE n/a - - UE performing the functions of an external attached network, registrar.  c108: IF A.3/7 OR A.3/8 OR A.3/8A THEN o ELSE n/a - - AS, MRFC, MRB.  c109: IF A.4/76 THEN o ELSE n/a - - a mechanism for transporting user to user call control information in SIP.  c110: IF A.3/1 THEN m ELSE IF A.3/2 OR A.3/3 OR A.3/4 THEN o ELSE n/a - - UE, P-CSCF, I-CSCF, S-CSCF.  c111: IF A.3/1 OR A.3/2 THEN m ELSE n/a - - UE, P-CSCF.  c112: IF NOT (A.3/1 AND NOT A.3C/1) THEN o ELSE n/a - - not UE, UE performing the functions of an external attached network.  c113: IF A.4/104 THEN o.7 ELSE n/a - - SIP overload control.  c114: IF A.4/104 THEN IF A.3/4 OR A.3/7 OR A.3/10 THEN o.7 ELSE n/a - - SIP overload control, S-CSCF, AS, additional routeing functionality.  c115: IF A.3/6 OR A.3/9 OR A.3/7 THEN o ELSE n/a - - MGCF, IBCF, AS  c116: IF A.3/2A OR A.3/6 OR A.3/7 OR A.3/9 THEN o ELSE IF A.3/1 THEN x ELSE n/a - - P-CSCF (IMS-ALG), MGCF, AS, IBCF, UE.  c117 IF A.3/2 OR A.3/4 OR OR A.3/9 OR A.3A/81 OR A.3A/83 OR A.3A/89 OR A.3A/81A THEN o ELSE n/a - - P-CSCF, S-CSCF, IBCF, MSC server enhanced for ICS, SCC application server, ATCF (UA), MSC server enhanced for SRVCC using SIP interface.  c118: IF A.4/49 THEN o ELSE n/a - - session initiation protocol URIs for applications such as voicemail and interactive voice response (NOTE 3).  c119: IF A.3/2A OR A.3/9 THEN o ELSE n/a - - P-CSCF (IMS-ALG), IBCF.  c120: IF A.3/2A OR A.3/9 THEN o ELSE n/a - - P-CSCF (IMS-ALG), IBCF.  c121: IF A.4/15 THEN m ELSE n/a - - the REFER method.  c122: IF A.4/22 THEN m ELSE n/a - - act as a notifier.  c123: IF A.4/111 AND (A.3/7A OR A.3/7B OR A.3/9A OR A.3/9B OR A.3/13A OR A.3/13B) THEN m ELSE IF A.3/4 OR A.3/7 OR A.3A/102 THEN o ELSE n/a.-.-.the Relayed-Charge header field extension, AS acting as terminating UA, or redirect server, AS acting as originating UA, IBCF (THIG), IBCF (IMS-ALG), ISC gateway function (THIG), ISC gateway function (THIG), S-CSCF, AS, transit function.  c124: IF A.3/2A OR A.3/9B OR A.3/7 THEN o ELSE n/a - - P-CSCF (IMS-ALG), I-BCF (IMS-ALG), AS.  c125: IF (A.3/4 OR A.3/6 OR A.3/7A OR A.3/7D OR A.3/9B OR A.3/13B OR A.3A/84 OR A.3A/89 OR A.3/2A OR A.3/8 OR A.3/11A) THEN m ELSE IF A.3/1 AND (A.3B/11 OR A.3B/12 OR A.3B/13 OR A.3B/14 OR A.3B/15) AND (A.3B/1 OR A.3B/2 OR A.3B/3 OR A.3B/4 OR A.3B/5 OR A.3B/6 OR A.3B/7 OR A.3B/8 OR A.3B/9) THEN m ELSE n/a. - - S-CSCF, MGCF, AS acting as terminating UA, AS acting as third-party call controller, IBCF (IMS-ALG), ISC gateway function (IMS-ALG), EATF, ATCF acting as UA, P-CSCF (IMS-ALG), MRFC, E-CSCF acting as UA, UE.  c126: IF A.4/78 THEN o ELSE n/a - - the SIP P-Served-User private header for the 3GPP IM CN subsystem.  c127: IF A.4/78 THEN m ELSE n/a - - the SIP P-Served-User private header for the 3GPP IM CN subsystem.  c128: IF A.3/2A OR A.3/9B OR A.3/7 OR A.3A/103 THEN o ELSE n/a - - P-CSCF (IMS-ALG), IBCF (IMS-ALG), AS, MCPTT server.  c129 IF A.3/6 OR A.3/7 OR A.3/9 OR A.3A/81 OR A.3A/81A OR A.3A/81B THEN o ELSE n/a - - MGCF, AS, IBCF, MSC Server enhanced for ICS, MSC server enhanced for SRVCC using SIP interface, MSC server enhanced for DRVCC using SIP interface.  c130: IF A.3/1 OR A.3/7 THEN o ELSE n/a - - UE, AS,  c131: IF A.3/6 OR A.3A/81 OR A.3A/81A OR A.3A/81B THEN o ELSE n/a - - MGCF, MSC server enhanced for ICS, MSC server enhanced for SRVCC using SIP interface, MSC server enhanced for DRVCC using SIP interface.  c132: IF A.3/6 OR A.3/7 OR A.3/9 THEN o ELSE n/a - - MGCF, AS, IBCF.  c133: IF A.3/2 OR A.3/7 OR A.3/9 THEN o ELSE n/a - - P-CSCF, AS, IBCF.  c134 IF A.4/60 THEN o ELSE n/a - - the Geolocation header field  c135: IF A.3/1 OR A.3/2 OR A.3/7 OR A.3/9 THEN o ELSE n/a - - UE, P-CSCF, AS, IBCF.  c136: IF A.3/1 THEN o ELSE n/a - - UE.  o.1: At least one of these capabilities is supported.  o.2: At least one of these capabilities is supported.  o.3: At least one of these capabilities is supported.  o.4: At least one of these capabilities is supported.  o.5: At least one of these capabilities is supported.  o.6: It is mandatory to support at least one of these items.  o.7: At least one of these capabilities is supported. | | | | | |
| NOTE 1: An AS acting as a proxy may be outside the trust domain, and therefore not able to support the capability for that reason; in this case it is perfectly reasonable for the header to be passed on transparently, as specified in the PDU parts of the profile.  NOTE 2: If a UE is unable to become engaged in a service that potentially requires the ability to identify and interact with a specific UE even when multiple UEs share the same single Public User Identity then the UE support can be "o" instead of "m". Examples include telemetry applications, where point-to-point communication is desired between two users.  NOTE 3: AS performing a service number translation (eg. Freephone) | | | | | |

Prerequisite A.4/20 - - SIP specific event notification

Table A.4A: Supported event packages

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Item | Does the implementation support | Subscriber | | | Notifier | | |
| Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | reg event package? | [43] | c1 | c3 | [43] | c2 | c4 |
| 1A | reg event package extension for GRUUs? | [94] | c1 | c25 | [94] | c2 | c4 |
| 2 | refer package? | [36] 3 | c13 | c13 | [36] 3 | c13 | c13 |
| 3 | presence package? | [74] 6 | c1 | c5 | [74] 6 | c2 | c6 |
| 4 | eventlist with underlying presence package? | [75], [74] 6 | c1 | c7 | [75], [74] 6 | c2 | c8 |
| 5 | presence.winfo template-package? | [72] 4 | c1 | c9 | [72] 4 | c2 | c10 |
| 6 | xcap-diff package? | [77] 4 | c1 | c11 | [77] 4 | c2 | c12 |
| 7 | conference package? | [78] 3 | c1 | c21 | [78] 3 | c1 | c22 |
| 8 | message-summary package? | [65] | c1 | c23 | [65] 3 | c2 | c24 |
| 9 | poc-settings package? | [110] | c1 | c26 | [110] | c2 | c27 |
| 11 | dialog event package? | [171] | c1 | c14 | [171] | c2 | c15 |
| 12 | load-control package? | [201] | c29 | c30 | [201] | c29 | c31 |
| c1: IF A.4/23 THEN o ELSE n/a - - acting as the subscriber to event information.  c2: IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.  c3: IF A.3/1 OR A.3A/81 OR A.3/2 THEN m ELSE IF A.3/7 THEN o ELSE n/a - - UE, MSC Server enhanced for ICS, P-CSCF, AS.  c4: IF A.3/4 THEN m ELSE IF A.3C/1 THEN o ELSE n/a - - S-CSCF, UE performing the functions of an external attached network.  c5: IF A.3A/3 OR A.3A/4 THEN m ELSE IF A.4/23 OR A.3/12 THEN o ELSE n/a - - resource list server or watcher, acting as the subscriber to event information, LRF.  c6: IF A.3A/1 THEN m ELSE IF A.4/22 OR A.3/11A THEN o ELSE n/a - - presence server, acting as the notifier of event information, E-CSCF acting as UA.  c7: IF A.3A/4 THEN m ELSE IF A.4/23 THEN o ELSE n/a - - watcher, acting as the subscriber to event information.  c8: IF A.3A/3 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - resource list server, acting as the notifier of event information.  c9: IF A.3A/2 THEN m ELSE IF A.4/23 THEN o ELSE n/a - - presence user agent, acting as the subscriber to event information.  c10: IF A.3A/1 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - presence server, acting as the notifier of event information.  c11: IF A.3A/2 OR A.3A/4 OR A.3A/56 THEN o ELSE IF A.4/23 THEN o ELSE n/a - - presence user agent or watcher or Ut reference point XCAP client for supplementary services, acting as the subscriber to event information.  c12: IF A.3A/1 OR A.3A/3 OR A.3A/55 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - presence server or resource list server or Ut reference point XCAP server for supplementary services, acting as the notifier of event information.  c13: IF A.4/15 THEN m ELSE n/a - - the REFER method.  c14: IF A.3/12 OR A.3A/87 THEN m ELSE IF A.3/1 OR A.3/7B OR A.3/7D THEN o ELSE n/a - - LRF, session continuity controller UE, UE, AS acting as originating UA, AS performing 3rd party call control.  c15: IF A.3/11 OR A.3A/83 THEN m ELSE IF A.3/1 OR A.3/7A OR A.3/7D THEN o ELSE n/a - - E-CSCF, SCC application server, UE, AS acting as terminating UA, or redirect server, AS performing 3rd party call control.  c21: IF A.3A/12 THEN m ELSE IF A.4/23 THEN o ELSE n/a - - conference participant or acting as the subscriber to event information.  c22: IF A.3A/11 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - conference focus or acting as the notifier of event information.  c23: IF A.3A/52 THEN m ELSE (A.3/1 OR A.3/7A OR A.3/7B) AND A.4/23 THEN o ELSE n/a - - message waiting indication subscriber UA, UE, AS acting as terminating UA, or redirect server, AS acting as originating UA all as subscriber of event information.  c24: IF A.3A/52 THEN m ELSE (A.3/1 OR A.3/7A OR A.3/7B) AND A.4/22 THEN o ELSE n/a - - message waiting indication notifier UA, UE, AS acting as terminating UA, or redirect server, AS acting as originating UA all as notifier of event information.  c25: IF A.4A/1 THEN (IF A.3/1 AND A.4/53 THEN m ELSE o) ELSE n/a - - reg event package, UE, reg event package extension for GRUUs.  c26: IF (A.3/7B OR A.3/1) AND (A.4/23 OR A.4/41) THEN o ELSE n/a - - AS acting as originating UA, UE, acting as the subscriber to event information, an event state publication extension to the session initiation protocol.  c27: IF (A.4/22 OR A.4/41) AND A.3/1 THEN o ELSE n/a - - UE, acting as the notifier of event information, an event state publication extension to the session initiation protocol.  c28: IF A.3/1 OR A.3A/81 OR A.3/2 OR A.3/7B THEN m ELSE n/a - - UE, MSC Server enhanced for ICS, P-CSCF, AS acting as originating UA.  c29: IF A.4/104B THEN m ELSE n/a - - distribution of load filters.  c30: IF A.4/104B THEN IF A.3/4 OR A.3/7 OR A.3/9 THEN m ELSE n/a - - distribution of load filters. S-CSCF, IBCF, AS.  c31: IF A.4/104B THEN If A.3/7 THEN m ELSE n/a - - distribution of load filters, AS. | | | | | | | |

Prerequisite A.4/13 - - SIP INFO method and package framework.

Table A.4B: Supported info packages

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Item | Does the implementation support | Sender | | | Receiver | | |
| Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | DTMF info package? | 7.12.1 | n/a | c1 | 7.12.1 | n/a | c1 |
| 2 | g.3gpp.mid-call? | [8M] | n/a | c2 | [8M] | n/a | c3 |
| 3 | g.3gpp.ussd? | [8W] | n/a | c4 | [8W] | n/a | c4 |
| 4 | g.3gpp.current-location-discovery info package ? | subclause 7.12.2.1 | n/a | c5 | subclause 7.12.2.1 | n/a | c6 |
| 5 | EmergencyCallData.eCall.MSD Info-Package | [244] 14.9 | m | c7 | [244] 14.9 | m | c7 |
| c1: IF A.3/6 OR A.3A/57 OR A.3A/58 OR A.3A/59 OR A.3A/60 THEN m ELSE o - - MGCF, customized alerting tones application server, customized alerting tones UA client, customized ringing signal application server, customized ringing signal UA client.  c2: IF A.3A/83 THEN o ELSE n/a - - SCC application server.  c3: IF A.3A/81 OR A.3A/81B THEN o ELSE n/a - - MSC server enhanced for ICS, MSC server enhanced for DRVCC using SIP interface.  c4: IF A.3A/92 OR A.3A/93 THEN m ELSE n/a - - USSI UE, USSI AS.  c5: IF A.3/11A OR A.3/2A THEN o ELSE n/a - - E-CSCF acting as UA, P-CSCF (IMS-ALG).  c6: IF (A.3/1 AND (A.3B/11 OR A.3B/12 OR A.3B/13 OR A.3B/14 OR A.3B/15)) OR A.3/2A THEN o ELSE n/a - - UE, IEEE-802.11, IEEE-802.11a, IEEE-802.11b, IEEE-802.11g, IEEE-802.11n, IEEE-802.11ac, P-CSCF (IMS-ALG).  c7: IF (A.3/1 AND A.4/120) THEN m ELSE n/a - - UE, Next-Generation Pan-European eCall emergency service. | | | | | | | |

Table A.4C: Supported media control packages

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Item | Does the implementation support | Sender | | | Receiver | | |
| Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | msc-ivr/1.0 | [147] |  | c1 | [147] |  | c2 |
| 2 | msc-mixer/1.0 | [148] |  | c1 | [148] |  | c2 |
| 3 | mrb-publish/1.0 | [192] |  | c3 | [192] |  | c4 |
| c1: IF A.3/7D THEN o ELSE n/a - - AS performing 3rd party call control.  c2: IF A.3/8 THEN o ELSE n/a - - MRFC.  c3: IF A.3/8 THEN o ELSE n/a - - MRFC.  c4: IF A.3/8A THEN o ELSE n/a - - MRB. | | | | | | | |

\*\*\* Next Change \*\*\*

### A.2.2.2 Major capabilities

Table A.162: Major capabilities

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item | Does the implementation support | Reference | RFC status | Profile status |
|  | **Capabilities within main protocol** |  |  |  |
| 3 | initiate session release? | [26] 16 | x | c27 |
| 4 | stateless proxy behaviour? | [26] 16.11 | o.1 | c29 |
| 5 | stateful proxy behaviour? | [26] 16.2 | o.1 | c28 |
| 6 | forking of initial requests? | [26] 16.1 | c1 | c31 |
| 7 | support of indication of TLS connections in the Record-Route header on the upstream side? | [26] 16.7 | o | n/a |
| 8 | support of indication TLS connections in the Record-Route header on the downstream side? | [26] 16.7 | o | n/a |
| 8A | authentication between UA and proxy? | [26] 20.28, 22.3, [287] | o | c85 |
| 9 | insertion of date in requests and responses? | [26] 20.17 | o | o |
| 10 | suppression or modification of alerting information data? | [26] 20.4 | o | o |
| 11 | reading the contents of the Require header before proxying the request or response? | [26] 20.32 | o | o |
| 12 | adding or modifying the contents of the Require header before proxying the REGISTER request or response | [26] 20.32 | o | m |
| 13 | adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER? | [26] 20.32 | o | o |
| 14 | being able to insert itself in the subsequent transactions in a dialog (record-routing)? | [26] 16.6 | o | c2 |
| 15 | the requirement to be able to use separate URIs in the upstream direction and downstream direction when record routeing? | [26] 16.7 | c3 | c3 |
| 16 | reading the contents of the Supported header before proxying the response? | [26] 20.37 | o | o |
| 17 | reading the contents of the Unsupported header before proxying the 420 response to a REGISTER? | [26] 20.40 | o | m |
| 18 | reading the contents of the Unsupported header before proxying the 420 response to a method other than REGISTER? | [26] 20.40 | o | o |
| 19 | the inclusion of the Error-Info header in 3xx - 6xx responses? | [26] 20.18 | o | o |
| 19A | reading the contents of the Organization header before proxying the request or response? | [26] 20.25 | o | o |
| 19B | adding or concatenating the Organization header before proxying the request or response? | [26] 20.25 | o | o |
| 19C | reading the contents of the Call-Info header before proxying the request or response? | [26] 20.9 | o | o |
| 19D | adding or concatenating the Call-Info header before proxying the request or response? | [26] 20.9 | o | o |
| 19E | delete Contact headers from 3xx responses prior to relaying the response? | [26] 20 | o | o |
| 19F | proxy reading the contents of a body or including a body in a request or response? | [26] | o | c88 |
| 19G | proxy modifying the content of a body | 3GPP TS 24.237 [8M] | n/a | c103 |
|  | **Extensions** |  |  |  |
| 20 | SIP INFO method and package framework? | [25] | o | o |
| 20A | legacy INFO usage? | [25] 2, 3 | o | o |
| 21 | reliability of provisional responses in SIP? | [27] | o | i |
| 22 | the REFER method? | [36] | o | o |
| 22A | clarifications for the use of REFER with RFC6665? | [231] | c113 | c113 |
| 22B | explicit subscriptions for the REFER method? | [232] | o | o |
| 23 | integration of resource management and SIP? | [30] [64] | o | i |
| 24 | the SIP UPDATE method? | [29] | c4 | i |
| 26 | SIP extensions for media authorization? | [31] | o | c7 |
| 27 | SIP specific event notification | [28] | o | i |
| 28 | a clarification on the use of GRUUs in the SIP event notification framework? | [232] | n/a | n/a |
| 29 | Session Initiation Protocol Extension Header Field for Registering Non-Adjacent Contacts | [35] | o | c6 |
| 30 | private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks | [34] | o | m |
| 30A | act as first entity within the trust domain for asserted identity? | [34] | c5 | c9 |
| 30B | act as entity within trust network that can route outside the trust network? | [34] | c5 | c9 |
| 30C | act as entity passing on identity transparently independent of trust domain? | [34] | c5 | c96 |
| 31 | a privacy mechanism for the Session Initiation Protocol (SIP) | [33] | o | m |
| 31A | request of privacy by the inclusion of a Privacy header | [33] | n/a | n/a |
| 31B | application of privacy based on the received Privacy header | [33] | c10 | c12 |
| 31C | passing on of the Privacy header transparently | [33] | c10 | c13 |
| 31D | application of the privacy option "header" such that those headers which cannot be completely expunged of identifying information without the assistance of intermediaries are obscured? | [33] 5.1 | x | x |
| 31E | application of the privacy option "session" such that anonymization for the session(s) initiated by this message occurs? | [33] 5.2 | n/a | n/a |
| 31F | application of the privacy option "user" such that user level privacy functions are provided by the network? | [33] 5.3 | n/a | n/a |
| 31G | application of the privacy option "id" such that privacy of the network asserted identity is provided by the network? | [34] 7 | c11 | c12 |
| 31H | application of the privacy option "history" such that privacy of the History-Info header is provided by the network? | [66] 7.2 | c34 | c34 |
| 32 | Session Initiation Protocol Extension Header Field for Service Route Discovery During Registration | [38] | o | c30 |
| 33 | a messaging mechanism for the Session Initiation Protocol (SIP) | [50] | o | m |
| 34 | Compressing the Session Initiation Protocol | [55] | o | c7 |
| 35 | private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP)? | [52] | o | m |
| 36 | the P-Associated-URI header extension? | [52] 4.1, [52A] 4 | c14 | c15 |
| 37 | the P-Called-Party-ID header extension? | [52] 4.2, [52A] 4` | c14 | c16 |
| 38 | the P-Visited-Network-ID header extension? | [52] 4.3, [52A] 4, [52B] 3 | c14 | c17 |
| 39 | reading, or deleting the P-Visited-Network-ID header before proxying the request or response? | [52] 4.3 | c18 | n/a |
| 41 | the P-Access-Network-Info header extension? | [52] 4.4, [52A] 4, [234] 2 | c14 | c19 |
| 42 | act as first entity within the trust domain for access network information? | [52] 4.4 | c20 | c21 |
| 43 | act as subsequent entity within trust network for access network information that can route outside the trust network? | [52] 4.4 | c20 | c22 |
| 44 | the P-Charging-Function-Addresses header extension? | [52] 4.5, [52A] 4 | c14 | m |
| 44A | adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response? | [52] 4.6 | c25 | c26 |
| 45 | the P-Charging-Vector header extension? | [52] 4.6, [52A] 4 | c14 | m |
| 46 | adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response? | [52] 4.6 | c23 | c24 |
| 47 | security mechanism agreement for the session initiation protocol? | [48] | o | c7 |
| 47A | mediasec header field parameter for marking security mechanisms related to media? | Subclause 7.2A.7 | n/a | c99 |
| 48 | the Reason header field for the session initiation protocol | [34A] | o | c78 |
| 48A | carrying Q.850 codes in reason header fields in SIP (Session Initiation Protocol) responses? | [130] | o | o |
| 48B | the location parameter for the SIP Reason header field? | [255] | o | o |
| 49 | an extension to the session initiation protocol for symmetric response routeing | [56A] | o | m |
| 50 | caller preferences for the session initiation protocol? | [56B] | c33 | c33 |
| 50A | the proxy-directive within caller-preferences? | [56B] 9.1 | o.4 | o.4 |
| 50B | the cancel-directive within caller-preferences? | [56B] 9.1 | o.4 | o.4 |
| 50C | the fork-directive within caller-preferences? | [56B] 9.1 | o.4 | c32 |
| 50D | the recurse-directive within caller-preferences? | [56B] 9.1 | o.4 | o.4 |
| 50E | the parallel-directive within caller-preferences? | [56B] 9.1 | o.4 | c32 |
| 50F | the queue-directive within caller-preferences? | [56B] 9.1 | o.4 | o.4 |
| 51 | an event state publication extension to the session initiation protocol? | [70] | o | m |
| 52 | SIP session timer? | [58] | o | o |
| 53 | the SIP Referred-By mechanism? | [59] | o | o |
| 54 | the Session Inititation Protocol (SIP) "Replaces" header? | [60] | o | o |
| 55 | the Session Inititation Protocol (SIP) "Join" header? | [61] | o | o |
| 56 | the callee capabilities? | [62] | o | o |
| 57 | an extension to the session initiation protocol for request history information? | [66] | o | o |
| 57A | application of the "mp" optional header field parameter? | [66] | o | o |
| 57B | application of the "rc" optional header field parameter? | [66] | o | o |
| 57C | application of the "np" optional header field parameter? | [66] | o | o |
| 58 | Rejecting anonymous requests in the session initiation protocol? | [67] | o | o |
| 59 | session initiation protocol URIs for applications such as voicemail and interactive voice response | [68] | o | o |
| 59A | Session Initiation Protocol (SIP) cause URI parameter for service number translation? | [230] | c111 | c111 |
| 60 | the P-User-Database private header extension? | [82] | o | c95 |
| 61 | Session initiation protocol's non-INVITE transactions? | [84] | m | m |
| 62 | a uniform resource name for services | [69] | n/a | c35 |
| 63 | obtaining and using GRUUs in the Session Initiation Protocol (SIP) | [93] | o | c36 |
|  |  |  |  |  |
| 65 | the Stream Control Transmission Protocol (SCTP) as a Transport for the Session Initiation Protocol (SIP)? | [96] | o | o (note2) |
| 66 | the SIP P-Profile-Key private header extension? | [97] | o | c41 |
| 66A | making the first query to the database in order to populate the P-Profile-Key header? | [97] | c38 | c39 |
| 66B | using the information in the P-Profile-Key header? | [97] | c38 | c40 |
| 67 | managing client initiated connections in SIP? | [92] 11 | o | c42 |
| 68 | indicating support for interactive connectivity establishment in SIP? | [102] | o | o |
| 69 | multiple-recipient MESSAGE requests in the session initiation protocol | [104] | n/a | n/a |
| 70 | SIP location conveyance? | [89] | o | c94 |
| 70A | addition or modification of location in a SIP method? | [89] | c44 | c45 |
| 70B | passes on locations in SIP method without modification? | [89] | c44 | c46 |
| 71 | referring to multiple resources in the session initiation protocol? | [105] | n/a | n/a |
| 72 | conference establishment using request-contained lists in the session initiation protocol? | [106] | n/a | n/a |
| 73 | subscriptions to request-contained resource lists in the session initiation protocol? | [107] | n/a | n/a |
| 74 | dialstring parameter for the session initiation protocol uniform resource identifier? | [103] | o | n/a |
| 75 | the P-Answer-State header extension to the session initiation protocol for the open mobile alliance push to talk over cellular? | [111] | o | c60 |
| 76 | the SIP P-Early-Media private header extension for authorization of early media? | [109] 8 | o | c51 |
| 77 | number portability parameters for the 'tel' URI? | [112] | o | c47 |
| 77A | assert or process carrier indication? | [112] | o | c48 |
| 77B | local number portability? | [112] | o | c50 |
|  |  |  |  |  |
| 79 | extending the session initiation protocol Reason header for preemption events | [115] | c79 | c79 |
| 80 | communications resource priority for the session initiation protocol? | [116] | o | c80 |
| 80A | inclusion of MESSAGE, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol? | [116] 4.2 | c82 | c82 |
| 80B | inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol? | [116] 4.2 | c82 | c82 |
| 81 | addressing an amplification vulnerability in session initiation protocol forking proxies? | [117] | c52 | c52 |
| 82 | the remote application identification of applying signalling compression to SIP | [79] 9.1 | o | c7 |
| 83 | a session initiation protocol media feature tag for MIME application subtypes? | [120] | o | c53 |
| 84 | SIP extension for the identification of services? | [121] | o | c54 |
| 84A | act as authentication entity within the trust domain for asserted service? | [121] | c55 | c56 |
| 85 | a framework for consent-based communications in SIP? | [125] | o | m |
| 86 | a mechanism for transporting user-to-user call control information in SIP? | [126] | o | c84 |
| 87 | the SIP P-Private-Network-Indication private-header (P-Header)? | [134] | o | o |
| 88 | the SIP P-Served-User private header in the 3GG IM CN subsystem? | [133] 6 | o | o |
| 89 | the SIP P-Served-User header extension for Originating CDIV session case? | [239] 4 | c126 | c126 |
| 90 | marking SIP messages to be logged? | [140] | o | m |
| 91 | the 199 (Early Dialog Terminated) response code | [142] | o | c90 |
| 92 | message body handling in SIP? | [150] | o | c89 |
| 93 | indication of support for keep-alive? | [143] | o | c51 | |
| 94 | SIP Interface to VoiceXML Media Services? | [145] | o | c91 |
| 95 | common presence and instant messaging (CPIM): message format? | [151] | o | o |
| 96 | instant message disposition notification? | [157] | o | o |
| 97 | requesting answering modes for SIP? | [158] | o | o |
| 97A | adding, deleting or reading the Answer-Mode header or Priv-Answer-Mode before proxying the request or response? | [158] | o | c92 |
| 99 | the early session disposition type for SIP? | [74B] | i | i |
|  |  |  |  |  |
| 101 | The Session-ID header? | [162] | o | o |
| 102 | correct transaction handling for 2xx responses to Session Initiation Protocol INVITE requests? | [163] | m | m |
| 103 | addressing Record-Route issues in the Session Initiation Protocol (SIP)? | [164] | o | o |
| 104 | essential correction for IPv6 ABNF and URI comparison in RFC3261? | [165] | m | m |
| 105 | suppression of session initiation protocol REFER method implicit subscription? | [173] | o | c100 |
| 106 | Alert-Info URNs for the Session Initiation Protocol? | [175] | o | o |
| 107 | multiple registrations? | Subclause 3.1 | n/a | c101 |
| 108 | the SIP P-Refused-URI-List private-header? | [183] | o | c102 |
| 109 | request authorization through dialog Identification in the session initiation protocol? | [184] | o | o |
| 110 | indication of features supported by proxy? | [190] | o | c104 |
| 111 | registration of bulk number contacts? | [191] | o | c105 |
| 112 | media control channel framework? | [146] | n/a | n/a |
| 113 | S-CSCF restoration procedures? | Subclause 4.14 | n/a | n/a |
| 114 | SIP overload control? | [198] | o | o |
| 114A | feedback control? | [199] | c106 | c106 |
| 114B | distribution of load filters? | [201] | n/a | n/a |
| 115 | handling of a 380 (Alternative service) response? | Subclause 5.2.10 | n/a | n/a |
| 116 | indication of adjacent network in the Via "received-realm" header field parameter? | [208] | o | c107 |
| 117 | PSAP callback indicator? | [209] | o | c108 |
| 118 | SIP URI parameter to indicate traffic leg? | [225] | o | c109 |
| 119 | PCF or PCRF based P-CSCF restoration? | Subclause 4.14.2 | n/a | c110 |
| 120 | UDM/HSS or HSS based P-CSCF restoration? | Subclause 4.14.2 | n/a | c112 |
| 121 | the Relayed-Charge header field extension? | Subclause 7.2.12 | n/a | c114 |
| 122 | resource sharing? | Subclause 4.15 | n/a | c115 |
| 123 | the Cellular-Network-Info header extension? | Subclause 7.2.15 | n/a | c116 |
| 124 | the Priority-Share header field extension? | Subclause 7.2.16 | n/a | c127 |
| 125 | the Response-Source header field extension? | Subclause 7.2.17 | n/a | o |
| 126 | authenticated identity management in the Session Initiation Protocol? | [252] | o | c128 |
| 127 | a SIP response code for unwanted calls extension? | [254] | o | o |
| 128 | the Attestation-Info header field extension? | Subclause 7.2.18 | n/a | o |
| 129 | the Origination-Id header field extension? | Subclause 7.2.19 | n/a | o |
| 130 | Dynamic services interactions? | Subclause 4.18 | n/a | c128 |
| 131 | the Additional-Identity header field extension? | Subclause 7.2.20 | n/a | o |
| 132 | RLOS? | Subclause 4.19 | n/a | c129 |
| 133 | the Priority-Verstat header field extension? | Subclause 7.2.21 | n/a | c82 |
| c1: IF A.162/5 THEN o ELSE n/a - - stateful proxy behaviour.  c2: IF A.3/2 OR A.3/9A OR A.3/4 OR A.3/13A OR A.3A/88 THEN m ELSE o - - P-CSCF, IBCF (THIG), S-CSCF, ISC gateway function (THIG), ATCF (proxy).  c3: IF (A.162/7 AND NOT A.162/8) OR (NOT A.162/7 AND A.162/8) THEN m ELSE IF A.162/14 THEN o ELSE n/a - - TLS interworking with non-TLS else proxy insertion.  c4: IF A.162/23 THEN m ELSE o - - integration of resource management and SIP.  c5: IF A.162/30 THEN o ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.  c6: IF A.3/2 OR A.3/9A OR A.3A/88 THEN m ELSE n/a - - P-CSCF, IBCF (THIG), ATFC (proxy).  c7: IF A.3/2 AND (A.3D/1 OR A.3D/4) THEN m ELSE n/a - - P-CSCF and (IMS AKA plus IPsec ESP or SIP digest with TLS).  c9: IF (A.3/2 OR A.3/4 OR A.3/9A OR A.3/13A) AND A.162/30 THEN m ELSE IF A.3/7C AND A.162/30 THEN o ELSE n/a - - P-CSCF or S-CSCF or IBCF (THIG) or ISC gateway function (THIG) or AS acting as proxy and extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks (NOTE 1).  c10: IF A.162/31 THEN o.2 ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  c11: IF A.162/31B THEN o ELSE x - - application of privacy based on the received Privacy header.  c12: IF A.162/31 AND A.3/4 THEN m ELSE IF A.3/11 THEN o ELSE n/a - - S-CSCF, E-CSCF.  c13: IF A.162/31 AND (A.3/2 OR A.3/3 OR A.3/7C OR A.3/9A OR A.3/13A OR A.3A/88) THEN m ELSE n/a - - P-CSCF, I-CSCF, AS acting as a SIP proxy or IBCF (THIG), ISC gateway function (THIG), ATCF (proxy).  c14: IF A.162/35 THEN o.3 ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP).  c15: IF A.162/35 AND (A.3/2 OR A.3/3 OR A.3/9A OR A.3/13A) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and P-CSCF or I-CSCF or IBCF (THIG) or ISC gateway function (THIG).  c16: IF A.162/35 AND (A.3/2 OR A.3/3 OR A.3/4 OR A.3/9A OR A.3/13A) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and P-CSCF or I-CSCF or S-CSCF or IBCF (THIG) or ISC gateway function (THIG).  c17: IF A.162/35 AND (A.3/2 OR A.3/3 OR A.3/9A OR A.3/13A) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and P-CSCF or I-CSCF or IBCF (THIG) or ISC gateway function (THIG).  c18: IF A.162/38 THEN o ELSE n/a - - the P-Visited-Network-ID header extension.  c19: IF A.162/35 AND (A.3/2 OR A.3.3 OR A.3/4 OR A.3/7 THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and P-CSCF, I-CSCF, S-CSCF, AS acting as a proxy.  c20: IF A.162/41 THEN o ELSE n/a - - the P-Access-Network-Info header extension.  c21: IF A.162/41 AND A.3/2 THEN m ELSE n/a - - the P-Access-Network-Info header extension and P-CSCF.  c22: IF A.162/41 AND A.3/4 THEN m ELSE n/a - - the P-Access-Network-Info header extension and S-CSCF.  c23: IF A.162/45 THEN o ELSE n/a - - the P-Charging-Vector header extension.  c24: IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.  c25: IF A.162/44 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.  c26: IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function Addresses header extension.  c27: IF A.3/2 OR A.3/4 THEN m ELSE x - - P-CSCF or S-CSCF.  c28: IF A.3/2 OR A.3/3 OR A.3/4 THEN m ELSE o.8 - - P-CSCF or I-CSCF or S-CSCF.  c29: IF A.3/2 OR A.3/4 THEN n/a ELSE IF A.3/3 THEN o ELSE o.8 - - P-CSCF or S-CSCF or I-CSCF.  c30: IF A.3/2 o ELSE i - - P-CSCF.  c31: IF A.3/4 THEN m ELSE x - - S-CSCF.  c32: IF A.3/4 THEN m ELSE o.4 - - S-CSCF.  c33: IF A.162/50A OR A.162/50B OR A.162/50C OR A.162/50D OR A.162/50E OR A.162/50F THEN m ELSE n/a - - support of any directives within caller preferences for the session initiation protocol.  c34: IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.  c35: IF A.3/2 OR A.3/11 THEN m ELSE IF A.3/7C OR A.3/9 OR A.3/13A THEN o ELSE n/a - - P-CSCF, E-CSCF, AS acting as proxy, IBCF, ISC gateway function (THIG). | | | | |
| c36: IF A.3/4 THEN m ELSE n/a - - S-CSCF.  c38: IF A.162/66 THEN o ELSE n/a - - the SIP P-Profile-Key private header.  c39: IF A.162/66 AND (A.3/3 OR A.3/9A) THEN m ELSE n/a - - the SIP P-Profile-Key private header, I-CSCF or IBCF (THIG).  c40: IF A.162/66 AND A.3/4 THEN m ELSE n/a - - the SIP P-Profile-Key private header, S-CSCF.  c41: IF A.3/3 OR A.3/4 OR A.3/9A THEN o ELSE n/a - - I-CSCF or S-CSCF or IBCF (THIG).  c42: IF A.162/107 THEN m ELSE n/a - - multiple registrations.  c44: IF A.162/70 THEN o.5 ELSE n/a - - SIP location conveyance.  c45: IF A.3/11 THEN m ELSE IF A.162/70 AND A.3/7C THEN o.6 ELSE n/a - - E-CSCF, SIP location conveyance, AS acting as a SIP proxy.  c46: IF A.162/70 AND A.3/2 OR A.3/3 OR A.3/5 OR A.3/10 OR A.3A/88 THEN m ELSE IF A.162/70 AND A.3/7C THEN o.6 ELSE n/a - - SIP location conveyance, P-CSCF, I-CSCF, S-CSCF, BGCF, additional routeing functionality, ATCF (proxy).  c47: IF A.3/3 OR A.3/4 OR A.3/5 OR A.3/7C THEN o ELSE n/a - - I-CSCF, S-CSCF, BGCF, AS acting as a SIP proxy.  c48: IF A.162/77 THEN m ELSE n/a - - number portability parameters for the 'tel' URI.  c50: IF A.162/77 THEN m ELSE n/a - - number portability parameters for the 'tel' URI.  c51: IF A.3/2 THEN m ELSE o - - P-CSCF.  c52: IF A.162/6 THEN m ELSE o - - forking of initial requests.  c53: IF A.3/4 THEN m ELSE n/a - - S-CSCF.  c54: IF A.3/3 OR A.3/4 OR A.3/7 OR A.3/2 OR A.3/9A OR A.3/13A THEN m ELSE n/a - - I-CSCF, S-CSCF, BGCF, P-CSCF. IBCF (THIG), ISC gateway function (THIG).  c55: IF A.162/84 THEN o ELSE n/a - - SIP extension for the identification of services.  c56: IF A.3/4 AND A.162/84 THEN m ELSE n/a - - S-CSCF and SIP extension for the identification of services.  c60: IF A.3/2 OR A.3/3 OR A.3/4 THEN o ELSE n/a - - P-CSCF, I-CSCF, S-CSCF.  c78: IF A.3/2 OR A.3/4 OR A.3/9 OR A.162/79 OR A.162/3 THEN m ELSE o - - P-CSCF, S-CSCF, IBCF, extending the session initiation protocol Reason header for preemption events, initiate session release.  c79: IF A.162/80 THEN o ELSE n/a - - communications resource priority for the session initiation protocol.  c80: IF A.3/2 OR A.3/3 OR A.3/4 OR A.3/5 OR A.3/7C OR A.3/9A OR A.3/10 OR A.3/13A THEN o ELSE n/a - - P-CSCF, I-CSCF, S-CSCF, BGCF, AS acting as proxy, IBCF (THIG), additional routeing functionality, ISC gateway function (THIG).  c82: IF A.162/80 THEN o ELSE n/a - - communications resource priority for the session initiation protocol.  c84: A.3/2 OR A.3/3 OR A.3/4 OR A.3/5 OR A.3/7C OR A.3/9A OR A.3/10 OR A.3/11 OR A.3/13A THEN o ELSE n/a - - P-CSCF, I-CSCF, S-CSCF, BGCF, AS acting as proxy, IBCF (THIG), additional routeing functionality, E-CSCF, ISC gateway function (THIG).  c85: IF A.3/2 OR A.3/3 OR A.3/4 THEN o ELSE x - - P-CSCF, I-CSCF, S-CSCF.  c88: IF A.3/2 OR A.3/4 OR A.3/7 OR A.3/7C OR A.3/9C OR A.3/11 OR A.3/13C OR A.3A/88 THEN m ELSE o - - P-CSCF, S-CSCF, AS, AS acting as a SIP proxy, IBCF (Screening of SIP signalling), E-CSCF, ISC gateway function (Screening of SIP signalling), ATCF (proxy).  c89: IF A.162/19F THEN m ELSE n/a - - proxy reading the contents of a body or including a body in a request or response.  c90: IF A.3/4 THEN m ELSE i - - S-CSCF.  c91: IF A.3/4 THEN o ELSE n/a - - S-CSCF.  c92: IF A.162/92 THEN o ELSE n/a - - requesting answering modes for SIP.  c94: IF A.3/11 THEN m ELSE o - - E-CSCF.  c95: IF A.3/3 OR A.3/4 OR A.3/7C THEN o ELSE n/a - - I-CSCF, S-CSCF, AS acting as a SIP proxy.  c96: IF A.3/2 OR A.3/11 OR A.3A/88 THEN m ELSE n/a - - P-CSCF, E-CSCF, ATCF (proxy).  c99: IF A.3/2A AND (A.3D/30 OR A.3D/20A OR A.3D/20B OR A.3D/20C OR A.3D/31) THEN m ELSE n/a - - P-CSCF (IMS-ALG) and end-to-access-edge media security using SDES, end-to-access-edge media security for MSRP using TLS and certificate fingerprints, end-to-access-edge media security for BFCP using TLS and certificate fingerprints, end-to-access-edge media security for UDPTL using DTLS and certificate fingerprints, end-to-access-edge media security for RTP media using DTLS-SRTP and certificate fingerprints.  c100: IF A.4/22 THEN o ELSE n/a - - the REFER method.  c101: IF A.3/2 OR A.3/4 THEN m ELSE n/a - - P-CSCF, S-CSCF. | | | | |
| c102: IF A.3/9B THEN m ELSE IF A.3/7A OR A.3/7B OR A.3/7D THEN o ELSE n/a - - IBCF (IMS-ALG), AS acting as terminating UA, AS acting as originating UA, AS performing 3rd party call control.  c103: IF A.3A/88 THEN m ELSE n/a - - ATCF (proxy).  c104: IF A.3/2 OR A.3A/50A OR A.3A/83 OR A.3A/88 THEN m ELSE o - - P-CSCF, Multimedia telephony application server, SCC application server, ATCF (proxy).  c105: IF A.3/2 OR A.3/3 OR A.3/9 THEN o ELSE n/a - - P-CSCF, I-CSCF, IBCF.  c106: IF A.162/114 THEN o.9 ELSE n/a - - SIP overload control.  c107: IF A.162/115 THEN o.9 ELSE n/a - - indication of adjacent network in the Via "received-realm" header field parameter.  c108: IF A.3/2 OR A.3/3 OR A.3/4 OR A.3/7 OR A.3/9 THEN o ELSE n/a - - P-CSCF, I-CSCF, S-CSCF, AS, IBCF.  c109: IF A.3/2 OR A.3/4 OR A.3/5 OR A.3/9 OR A.3/10 OR A.3A/83 OR A.3A/88 OR A.3/3 THEN o ELSE n/a - - P-CSCF, S-CSCF, BGCF, IBCF, Additional routeing functionality, SCC application server, ATCF (proxy), I-CSCF.  c110: IF A.3/2 OR A.3/4 OR A.3/9 THEN o ELSE n/a - - P-CSCF, S-CSCF, IBCF.  c111: IF A.162/59 THEN o ELSE n/a - - session initiation protocol URIs for applications such as voicemail and interactive voice response (NOTE 3).  c112: IF A.3/2 OR A.3/4 OR A.3/9 THEN o ELSE n/a - - P-CSCF, S-CSCF, IBCF.  c113: IF A.162/22 THEN m ELSE n/a - - the REFER method.  c114: IF A.3/4 OR A.3/7 OR A.3A/102 THEN o ELSE n/a.-.-.S-CSCF, AS, transit function.  c115: IF A.3/2 OR A.3/7C OR A.3/9 THEN o ELSE n/a - - P-CSCF, AS acting as a SIP proxy, IBCF.  c116: IF A.3/2 OR A.3.3 OR A.3/4 OR A.3/7C OR A.3/9 OR A.3/11B OR A.3A/88 OR A.3/5 THEN m ELSE n/a - - P-CSCF, I-CSCF, S-CSCF, AS acting as a proxy, IBCF, E-CSCF acting as a SIP Proxy, ATCF (proxy), BGCF.  c126: IF A.162/88 THEN o ELSE n/a - - the SIP P-Served-User private header for the 3GPP IM CN subsystem.  c127: IF A.3/2 OR A.3/7C OR A.3/9 THEN o ELSE n/a - - P-CSCF, AS acting as a SIP proxy, IBCF.  c128: IF A.3/7 OR A.3/9 THEN o ELSE n/a - - AS, IBCF.  c129: IF A.3/2 OR A.3/4 THEN o ELSE n/a - - P-CSCF, S-CSCF.  o.1: It is mandatory to support at least one of these items.  o.2: It is mandatory to support at least one of these items.  o.3: It is mandatory to support at least one of these items.  o.4 At least one of these capabilities is supported.  o.5: It is mandatory to support exactly one of these items.  o.6: It is mandatory to support exactly one of these items.  o.7: It is mandatory to support at least one of these items.  o.8 It is mandatory to support at least one of these items.  o.9: At least one of these capabilities is supported. | | | | |
| NOTE 1: An AS acting as a proxy may be outside the trust domain, and therefore not able to support the capability for that reason; in this case it is perfectly reasonable for the header to be passed on transparently, as specified in the PDU parts of the profile.  NOTE 2: Not applicable over Gm reference point (UE – P-CSCF).  NOTE 3: AS performing a service number translation (e.g. Freephone) | | | | |

\*\*\* Next Change \*\*\*

### A.3.2.1 Major capabilities

Table A.317: Major capabilities

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item | Does the implementation support | Reference | RFC status | Profile status |
|  | **Capabilities within main protocol** |  |  |  |
|  |  |  |  |  |
|  | **Extensions** |  |  |  |
| 22 | integration of resource management and SIP? | [30] [64] | o | c14 |
| 23 | grouping of media lines? | [53] | c3 | c3 |
| 24 | mapping of media streams to resource reservation flows? | [54] | o | c1 |
| 25 | SDP bandwidth modifiers for RTCP bandwidth? | [56] | o | o (NOTE 1) |
| 26 | TCP-based media transport in the session description protocol? | [83] | o | c2 |
| 27 | interactive connectivity establishment? | [289], [290] | o | c4 |
| 28 | session description protocol format for binary floor control protocol streams? | [108] | o | o |
| 29 | extended RTP profile for real-time transport control protocol (RTCP)-based feedback (RTP/AVPF)? | [135] | o | c5 |
| 30 | SDP capability negotiation? | [137] | o | c6 |
| 31 | Session Description Protocol (SDP) extension for setting up audio media streams over circuit-switched bearers in the Public Switched Telephone Network (PSTN)? | [155] | o | c7 |
| 32 | miscellaneous capabilities negotiation in the Session Description Protocol (SDP)? | [156] | o | c7 |
| 33 | transport independent bandwidth modifier for the Session Description Protocol? | [152] | o | c8 |
| 34 | Secure Real-time Transport Protocol (SRTP)? | [169] | o | c15 |
| 35 | MIKEY-TICKET? | [170] | o | c10 |
| 36 | SDES? | [168] | o | c9 |
| 37 | end-to-access-edge media security using SDES? | 7.5.2 | n/a | c16 |
| 37A | end-to-access-edge media security for MSRP using TLS and certificate fingerprints? | 7.5.2 | n/a | c22 |
| 37B | end-to-access-edge media security for BFCP using TLS and certificate fingerprints? | 7.5.2 | n/a | c23 |
| 37C | end-to-access-edge media security for UDPTL using DTLS and certificate fingerprints? | 7.5.2 | n/a | c24 |
| 37D | end-to-access-edge media security for RTP media using DTLS-SRTP and certificate fingerprints? | 7.5.2 | n/a | c40 |
| 38 | SDP media capabilities negotiation? | [172] | o | c12 |
| 39 | Transcoding Services Invocation in the Session Initiation Protocol (SIP) Using Third Party Call Control (3pcc)? | [166] | o | c13 |
| 40 | Message Session Relay Protocol? | [178] | o | c17 |
| 40A | Connection establishment for media anchoring for the message session relay protocol? | [214] | o | c26 |
| 41 | a SDP offer/answer mechanism to enable file transfer? | [185] | o | o |
| 42 | optimal media routeing | [11D] | n/a | c18 |
| 43 | ECN for RTP over UDP | [188] | o | c19 |
| 44 | T.38 FAX? | [202] | n/a | c20 |
| 45 | support for reduced-size RTCP? | [204] | o | o |
| 46 | RTCP extended reports? | [205] | o | o |
| 47 | maximum receive SDU size? | [9B] | o | o |
| 48 | the SDP content attribute? | [206] | o | c21 |
| 49 | a general mechanism for RTP header extensions? | [210] | o | o |
| 50 | negotiation of generic image attributes in the session description protocol (SDP)? | [211] | o | o |
| 51 | connection-oriented media transport over the TLS protocol in the SDP? | [241] | o | c25 |
| 52 | UDPTL over DTLS? | [217] | o | c27 |
| 53 | telepresence? | [7G] | o | o |
| 54 | SCTP over DTLS? | [219] | o | c28 |
| 55 | DTLS-SRTP? | [222], [223] | o | c41 |
| 56 | STUN Usage for Consent Freshness? | [224] | o | c29 |
| 57 | Alternate Connectivity (ALTC) Attribute? | [228] | o | c30 |
| 58 | 3GPP MTSI RTCP-APP adaptation? | [9B] | n/a | o |
| 59 | 3GPP MTSI Pre-defined Region-of-Interest (ROI)? | [9B] | n/a | o |
| 60 | 3GPP MTSI Arbitrary Region-of-Interest (ROI)? | [9B] | n/a | o |
| 61 | multiplexing RTP data and control packets on a single port | [237], [237A] | o | o |
| 61A | Exclusive RTP and RTCP multiplexed on one port (a=rtcp-mux-only)? | [246] | o | c34 |
| 62 | SDP-based data channel negotiation? | [238] | o | c31 |
| 63 | Media plane optimization for WebRTC? | [8Z] | n/a | c32 |
| 64 | Enhanced bandwidth negotiation mechanism? | [9B] | n/a | o |
| 65 | an SDP offer/answer mechanism to negotiate DTLS protected media? | [240] | o | c33 |
| 66 | Using simulcast in SDP and RTP sessions? | [249] | o | c35 |
| 67 | RTP payload format restrictions? | [250] | o | c36 |
| 68 | Compact Concurrent Codec Negotiation and Capabilities? | [9B] | n/a | c35 |
| 69 | 3GPP MTSI Delay Budget Information (DBI)? | [9B] | n/a | c37 |
| 70 | Access Network Bitrate Recommendation (ANBR)? | [9B] | n/a | c38 |
| 71 | Framework for Live Uplink Streaming (FLUS)? | [276] | n/a | c39 |
| 72 | 3GPP MTSI client using data channels? | [9B] | n/a | c39 |
| c1: IF A.3/1 THEN m ELSE n/a - - UE role.  c2: IF A.3/9B AND A.3/13B THEN m ELSE IF A.3/1 OR A.3/2A OR A.3/6 OR A.3/7 THEN o ELSE n/a - - IBCF (IMS-ALG), ISC gateway function (IMS-ALG), UE, P-CSCF (IMS-ALG), MGCF, AS.  c3: IF A.317/24 OR A.317/53 THEN m ELSE o - - mapping of media streams to resource reservation flows, telepresence.  c4: IF A.3/9B OR A.3/13B THEN m ELSE IF A.3/1 OR A.3/6 THEN o ELSE n/a - - IBCF (IMS-ALG), application gateway function (IMS-ALG), UE, MGCF.  c5: IF A.3A/50 OR A.3A/50A OR A.3/6 OR A.3/9B OR A.3A/89 OR A.3A/11 OR A.3A/12 THEN m ELSE o - - multimedia telephony service participant, multimedia telephony service application server, MGCF, IBCF (IMS-ALG), ATCF (UA), conference focus, conference participant.  c6: IF A.3A/50 OR A.3A/50A OR A.3/6 OR A.3/9B OR A.3/13B OR A.3A/89 THEN m ELSE o - - multimedia telephony service participant, multimedia telephony service application server, MGCF, IBCF (IMS-ALG), application gateway function (IMS-ALG), ATCF (UA).  c7: IF A.3A/82 OR A.3A/83 THEN m ELSE o - - ICS user agent, SCC application server.  c8: IF A.317/25 AND (A.3/1 OR A.3/6 OR A.3A/89) THEN o ELSE n/a - - SDP bandwidth modifiers for RTCP bandwidth, UE, MGCF, ATCF (UA).  c9: IF A.3D/30 OR A.3D/20 THEN m ELSE n/a - - end-to-access-edge media security using SDES, end-to-end media security using SDES.  c10: IF A.3D/21 OR A.3D/22 THEN m ELSE n/a - - end-to-end media security using KMS, end-to-end media security for MSRP using TLS and KMS.  c12: IF A.3A/82 OR A.3A/83 THEN m ELSE o - - ICS user agent, SCC application server.  c13: IF IF A.3/7D OR A.3/8 THEN o else n/a - - AS performing 3rd party call control or MRFC.  c14: IF A.4/2C THEN m ELSE o - - initiating a session which require local and/or remote resource reservation.  c15: IF A.3D/20 OR A.3D/21 OR A.3D/30 THEN m ELSE n/a - - end-to-end media security using SDES, end-to-end media security using KMS, end-to-access-edge media security using SDES.  c16: If A.3D/30 THEN m ELSE n/a - - end-to-access-edge media security using SDES.  c17: IF A.3A/33B OR A.3A/34 THEN m ELSE IF A.3A/8 OR A.3A/9 OR A.3/2A THEN o ELSE n/a - - session-mode messaging participant, session-mode messaging intermediate node, IBCF, MRFC, P-CSCF (IMS-ALG).  c18: IF A.3/2A OR A.3/6 OR A.3/7 OR A.3/9B OR A.3A/89 OR A.3/13B THEN o ELSE n/a - - P-CSCF (IMS-ALG), MGCF, AS, IBCF (IMS-ALG), ATCF (UA), application gateway function (IMS-ALG).  c19: IF A.3/2A OR A.3/6 OR A.3/8 OR A.3/9B OR A.3A/81 OR A.3A/89 OR A.3/13B OR A.3A/81A OR A.3A/81B THEN o ELSE n/a - - P-CSCF (IMS-ALG), MGCF, MRFC, IBCF (IMS-ALG), MSC Server enhanced for ICS, ATCF (UA), application gateway function (IMS-ALG), MSC server enhanced for SRVCC using SIP interface, MSC server enhanced for DRVCC using SIP interface.  c20: IF A.3/1 OR A.3/6 THEN o ELSE n/a - - UE, MGCF.  c21: IF A.3A/57 OR A.3A/58 OR A.3A/59 OR A.3A/60 OR A.3/2A OR A.3/9B OR A.3A/11 OR A.3A/12 THEN m ELSE o - - Customized alerting tones application server, Customized alerting tones UA client, Customized ringing signal application server, Customized ringing signal UA client, P-CSCF (IMS-ALG), IBCF (IMS-ALG), conference focus, conference participant.  c22: If A.3D/20A THEN m ELSE n/a - - end-to-access-edge media security for MSRP using TLS and certificate fingerprints.  c23: If A.3D/20B THEN m ELSE n/a - - end-to-access-edge media security for BFCP using TLS and certificate fingerprints.  c24: If A.3D/20C THEN m ELSE n/a - - end-to-access-edge media security for UDPTL using DTLS and certificate fingerprints.  c25: IF (A.317/37A AND A.317/40) OR (A.317/37B AND A.317/28) OR (A.317/37C AND A.317/52) OR (A.317/37D AND A.317/55) THEN m ELSE o - - end-to-access-edge media security for MSRP using TLS and certificate fingerprints, message session relay protocol, end-to-access-edge media security for BFCP using TLS and certificate fingerprints, session description protocol format for binary floor control protocol streams, end-to-access-edge media security for UDPTL using DTLS and certificate fingerprints, UDPTL over DTLS, end-to-access-edge media security for RTP media using DTLS-SRTP and certificate fingerprints, DTLS-SRTP.  c26: IF A.317/40 THEN m ELSE n/a - - message session relay protocol.  c27: IF A.317/37C THEN m ELSE o - - end-to-access-edge media security for UDPTL using DTLS and certificate fingerprints.  c28: IF (A.3/1 AND A.317/53) OR A.3/14 OR A.3A/95 THEN m ELSE o - - UE, telepresence, Gm based WIC, eP-CSCF.  c29: IF A.3/14 OR A.3A/95 THEN m ELSE o - - Gm based WIC, eP-CSCF.  c30: IF A.3A/81 OR A.3/9B OR A.3/2A THEN o ELSE n/a - - UE performing the functions of an external attached network, IBCF (IMS-ALG), P-CSCF (IMS-ALG).  c31: IF A.3/14 OR A.3A/95 THEN o ELSE n/a - - Gm based WIC, eP-CSCF.  c32: IF A.3A/95 OR A.3/9B THEN o ELSE n/a - - eP-CSCF, IMS-ALG.  c33: IF A.317/52 OR A.317/54 OR A.317/55 THEN m ELSE n/a - - UDPTL over DTLS, SCTP over DTLS, DTLS-SRTP.  c34: IF A.3/14 OR A.3A/95 THEN m ELSE n/a - - Gm based WIC, eP-CSCF.  c35: IF A.3A/11 OR A.3A/12 THEN o ELSE n/a - - conference focus, conference participant.  c36: IF A.317/66 AND (A.3A/11 OR A.3A/12) THEN o ELSE n/a - - Using simulcast in SDP and RTP sessions, conference focus, conference participant.  c37: IF A.3/1 OR A.3/2A OR A.3/8 OR A.3/9B THEN o ELSE n/a - - UE, P-CSCF (IMS-ALG), MRFC, IBCF (IMS-ALG).  c38: IF A.3/1 THEN o ELSE n/a - - UE.  c39: IF A.3/1 OR A.3/2 THEN o ELSE n/a - - UE, P-CSCF.  c40: IF A.3D/31 THEN m ELSE n/a - - end-to-access-edge media security for RTP media using DTLS-SRTP and certificate fingerprints.  c41: IF A.3D/31 THEN m ELSE o - - end-to-access-edge media security for RTP media using DTLS-SRTP and certificate fingerprints. | | | | |
| NOTE 1: For "video" and "audio" media types that utilise RTP/RTCP, if the RTCP bandwidth level for the session is different than the default RTCP bandwidth as specified in RFC 3556 [56], then, it shall be specified. For other media types, it may be specified. | | | | |

\*\*\* Next Change \*\*\*

### A.3.2.2 SDP types

Table A.318: SDP types

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Item | Type | Sending | | | Receiving | | |
| Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
|  | **Session level description** | | | | | | |
| 1 | v= (protocol version) | [39] 5.1 | m | m | [39] 5.1 | m | m |
| 2 | o= (owner/creator and session identifier) | [39] 5.2 | m | m | [39] 5.2 | m | m |
| 3 | s= (session name) | [39] 5.3 | m | m | [39] 5.3 | m | m |
| 4 | i= (session information) | [39] 5.4 | o | c2 | [39] 5.4 | m | c3 |
| 5 | u= (URI of description) | [39] 5.5 | o | c4 | [39] 5.5 | o | n/a |
| 6 | e= (email address) | [39] 5.6 | o | c4 | [39] 5.6 | o | n/a |
| 7 | p= (phone number) | [39] 5.6 | o | c4 | [39] 5.6 | o | n/a |
| 8 | c= (connection information) | [39] 5.7 | c5 | c5 | [39] 5.7 | m | m |
| 9 | b= (bandwidth information) | [39] 5.8 | o | o | [39] 5.8 | m | m |
|  | **Time description (one or more per description)** | | | | | | |
| 10 | t= (time the session is active) | [39] 5.9 | m | m | [39] 5.9 | m | m |
| 11 | r= (zero or more repeat times) | [39] 5.10 | o | c4 | [39] 5.10 | o | n/a |
|  | **Session level description (continued)** | | | | | | |
| 12 | z= (time zone adjustments) | [39] 5.11 | o | n/a | [39] 5.11 | o | n/a |
| 13 | k= (encryption key) | [39] 5.12 | x | x | [39] 5.12 | n/a | n/a |
| 14 | a= (zero or more session attribute lines) | [39] 5.13 | o | o | [39] 5.13 | m | m |
|  | **Media description (zero or more per description)** | | | | | | |
| 15 | m= (media name and transport address) | [39] 5.14 | m | m | [39] 5.14 | m | m |
| 16 | i= (media title) | [39] 5.4 | o | c2 | [39] 5.4 | o | c3 |
| 17 | c= (connection information) | [39] 5.7 | c1 | c1 | [39] 5.7 | m | m |
| 18 | b= (bandwidth information) | [39] 5.8 | o | o | [39] 5.8 | m | m |
| 19 | k= (encryption key) | [39] 5.12 | x | x | [39] 5.12 | n/a | n/a |
| 20 | a= (zero or more media attribute lines) | [39] 5.13 | o | o | [39] 5.13 | m | m |
| c1: IF (A.318/15 AND NOT A.318/8) THEN m ELSE IF (A.318/15 AND A.318/8) THEN o ELSE n/a - - "c=" contained in session level description and SDP contains media descriptions.  c2: IF A.3/6 THEN x ELSE o - - MGCF.  c3: IF A.3/6 THEN n/a ELSE m - - MGCF.  c4: IF A.3/6 THEN x ELSE n/a - - MGCF.  c5: IF A.318/17 THEN o ELSE m - - "c=" contained in all media description. | | | | | | | |

Prerequisite A.318/14 OR A.318/20 - - a= (zero or more session/media attribute lines)

Table A.319: zero or more session / media attribute lines (a=)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Item | Field | Sending | | | Receiving | | |
| Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | category (a=cat) | [39] 6 | c8 | c8 | [39] 6 | c9 | c9 |
| 2 | keywords (a=keywds) | [39] 6 | c8 | c8 | [39] 6 | c9 | c9 |
| 3 | name and version of tool (a=tool) | [39] 6 | c8 | c8 | [39] 6 | c9 | c9 |
| 4 | packet time (a=ptime) | [39] 6 | c10 | c10 | [39] 6 | c11 | c11 |
| 5 | maximum packet time (a=maxptime) | [39] 6 (NOTE 1) | c10 | c10 | [39] 6 (NOTE 1) | c11 | c11 |
| 6 | receive-only mode (a=recvonly) | [39] 6 | o | o | [39] 6 | m | m |
| 7 | send and receive mode (a=sendrecv) | [39] 6 | o | o | [39] 6 | m | m |
| 8 | send-only mode (a=sendonly) | [39] 6 | o | o | [39] 6 | m | m |
| 8A | Inactive mode (a=inactive) | [39] 6 | o | o | [39] 6 | m | m |
| 9 | whiteboard orientation (a=orient) | [39] 6 | c10 | c10 | [39] 6 | c11 | c11 |
| 10 | conference type (a=type) | [39] 6 | c8 | c8 | [39] 6 | c9 | c9 |
| 11 | character set (a=charset) | [39] 6 | c8 | c8 | [39] 6 | c9 | c9 |
| 12 | language tag (a=sdplang) | [39] 6 | o | o | [39] 6 | m | m |
| 13 | language tag (a=lang) | [39] 6 | o | o | [39] 6 | m | m |
| 14 | frame rate (a=framerate) | [39] 6 | c10 | c10 | [39] 6 | c11 | c11 |
| 15 | quality (a=quality) | [39] 6 | c10 | c10 | [39] 6 | c11 | c11 |
| 16 | format specific parameters (a=fmtp) | [39] 6 | c10 | c10 | [39] 6 | c11 | c11 |
| 17 | rtpmap attribute (a=rtpmap) | [39] 6 | c10 | c10 | [39] 6 | c11 | c11 |
| 18 | current-status attribute (a=curr) | [30] 5 | c1 | c1 | [30] 5 | c2 | c2 |
| 19 | desired-status attribute (a=des) | [30] 5 | c1 | c1 | [30] 5 | c2 | c2 |
| 20 | confirm-status attribute (a=conf) | [30] 5 | c1 | c1 | [30] 5 | c2 | c2 |
| 21 | media stream identification attribute (a=mid) | [53] 3 | c3 | c3 | [53] 3 | c4 | c4 |
| 22 | group attribute (a=group) | [53] 4 | c5 | c5 | [53] 3 | c6 | c6 |
| 23 | setup attribute (a=setup) | [83] 4 | c7 | c45 | [83] 4 | c7 | c45 |
| 24 | connection attribute (a=connection) | [83] 5 | c7 | c7 | [83] 5 | c7 | c7 |
| 24A | DTLS association ID attribute (a=tls-id) | [240] 4 | c62 | c62 | [240] 4 | c62 | c62 |
| 25 | IP addresses (a=candidate) | [290] | c12 | c12 | [290] | c13 | c13 |
| 26 | floor control server determination (a=floorctrl) | [108] 4 | c14 | c14 | [108] 4 | c14 | c14 |
| 27 | conference id (a=confid) | [108] 5 | c14 | c14 | [108] 5 | c14 | c14 |
| 28 | user id (a=userid) | [108] 5 | c14 | c14 | [108] 5 | c14 | c14 |
| 29 | association between streams and floors (a=floorid) | [108] 6 | c14 | c14 | [108] 6 | c14 | c14 |
| 30 | RTCP feedback capability attribute (a=rtcp-fb) | [135] 4.2 | c15 | c15 | [135] 4.2 | c15 | c15 |
| 31 | extension of the rtcp-fb attribute (a=rtcp-fb) | [136] 7.1, [188] 6.2, [251] 9 | c15 | c15 | [136] 7.1, [251] 9 | c15 | c15 |
| 32 | supported capability negotiation extensions (a=csup) | [137] 3.3.1 | c16 | c16 | [137] 3.3.1 | c16 | c16 |
| 33 | required capability negotiation extensions (a=creq) | [137] 3.3.2 | c16 | c16 | [137] 3.3.2 | c16 | c16 |
| 34 | attribute capability (a=acap) | [137] 3.4.1 | c16 | c16 | [137] 3.4.1 | c16 | c16 |
| 35 | transport protocol capability (a=tcap) | [137] 3.4.2 | c16 | c16 | [137] 3.4.2 | c16 | c16 |
| 36 | potential configuration (a=pcfg) | [137] 3.5.1  [172] 3.3.6 | c16 | c16 | [137] 3.5.1  [172] 3.3.6 | c16 | c16 |
| 37 | actual configuration (a=acfg) | [137] 3.5.2 | c16 | c16 | [137] 3.5.2 | c16 | c16 |
| 38 | connection data capability (a=ccap) | [156] 3.1 | c17 | c17 | [156] 3.1 | c18 | c18 |
| 39 | maximum packet rate (a=maxprate) | [152] 6.3 | c19 | c19 | [152] 6.3 | c19 | c19 |
| 40 | crypto attribute (a=crypto) | [168] | c20 | c20 | [168] | c20 | c20 |
| 41 | key management attribute (a=key-mgmt) | [167] | c21 | c21 | [167] | c21 | c21 |
| 42 | 3GPP\_e2ae-security-indicator (a=3ge2ae) | 7.5.2 | c22 | c22 | 7.5.2 | c22 | c22 |
| 43 | media capability (a=rmcap) | [172] 3.3.1 | c23 | c23 | [172] 3.3.1 | c23 | c23 |
| 43A | media capability (a=omcap) | [172] 3.3.1 | c23 | c23 | [172] 3.3.1 | c23 | c23 |
| 44 | media format capability (a=mfcap) | [172] 3.3.2 | c23 | c23 | [172] 3.3.2 | c23 | c23 |
| 45 | media-specific capability (a=mscap) | [172] 3.3.3 | c23 | c23 | [172] 3.3.3 | c23 | c23 |
| 46 | latent configuration (a=lcfg) | [172] 3.3.5 | c44 | c44 | [172] 3.3.5 | c44 | c44 |
| 47 | session capability (a=sescap) | [172] 3.3.8 | c24 | c24 | [172] 3.3.8 | c24 | c24 |
| 48 | msrp path (a=path) | [178] | c25 | c25 | [178] | c25 | c25 |
| 49 | file selector (a=file-selector) | [185] 6 | c27 | c27 | [185] 6 | c28 | c28 |
| 50 | file transfer identifier (a= file-transfer-id) | [185] 6 | c26 | c26 | [185] 6 | c28 | c28 |
| 51 | file disposition (a=file-disposition) | [185] 6 | c26 | c26 | [185] 6 | c28 | c28 |
| 52 | file date (a=file-date) | [185] 6 | c26 | c26 | [185] 6 | c28 | c28 |
| 53 | file icon (a=file-icon | [185] 6 | c26 | c26 | [185] 6 | c28 | c28 |
| 54 | file range (a=file-range) | [185] 6 | c26 | c26 | [185] 6 | c28 | c28 |
| 55 | optimal media routeing visited realm (a=visited-realm) | 7.5.3 | c29 | c29 | 7.5.3 | c29 | c29 |
| 56 | optimal media routeing secondary realm (a=secondary-realm) | 7.5.3 | c29 | c29 | 7.5.3 | c29 | c29 |
| 57 | optimal media routeing media level checksum (a=omr-m-cksum) | 7.5.3 | c29 | c29 | 7.5.3 | c29 | c29 |
| 58 | optimal media routeing session level checksum (a=omr-s-cksum) | 7.5.3 | c29 | c29 | 7.5.3 | c29 | c29 |
| 59 | optimal media routeing codecs (a=omr-codecs) | 7.5.3 | c29 | c29 | 7.5.3 | c29 | c29 |
| 60 | optimal media routeing media attributes (a=omr-m-att) | 7.5.3 | c29 | c29 | 7.5.3 | c29 | c29 |
| 61 | optimal media routeing session attributes (a=omr-s-att) | 7.5.3 | c29 | c29 | 7.5.3 | c29 | c29 |
| 62 | optimal media routeing media bandwidth (a=omr-m-bw) | 7.5.3 | c29 | c29 | 7.5.3 | c29 | c29 |
| 63 | optimal media routeing session bandwidth (a=omr-s-bw) | 7.5.3 | c29 | c29 | 7.5.3 | c29 | c29 |
| 64 | ecn-attribute (a=ecn-capable-rtp) | [188] | c30 | c30 | [188] | c30 | c30 |
| 65 | T38 FAX Protocol version (a=T38FaxVersion) | [202] | n/a | c31 | [202] | n/a | c31 |
| 66 | T38 FAX Maximum Bit Rate (a=T38MaxBitRate) | [202] | n/a | c31 | [202] | n/a | c31 |
| 67 | T38 FAX Rate Management (a=T38FaxRateManagement) | [202] | n/a | c31 | [202] | n/a | c31 |
| 68 | T38 FAX Maximum Buffer Size (a=T38FaxMaxBuffer) | [202] | n/a | c31 | [202] | n/a | c31 |
| 69 | T38 FAX Maximum Datagram Size (a=T38FaxMaxDatagram) | [202] | n/a | c31 | [202] | n/a | c31 |
| 70 | T38 FAX maximum IFP frame size (a=T38FaxMaxIFP) | [202] | n/a | c32 | [202] | n/a | c32 |
| 71 | T38 FAX UDP Error Correction Scheme (a=T38FaxUdpEC) | [202] | n/a | c32 | [202] | n/a | c32 |
| 72 | T38 FAX UDP Error Correction Depth (a=T38FaxUdpECDepth) | [202] | n/a | c32 | [202] | n/a | c32 |
| 73 | T38 FAX UDP FEC Maximum Span (a=T38FaxUdpFECMaxSpan) | [202] | n/a | c32 | [202] | n/a | c32 |
| 74 | T38 FAX Modem Type (a=T38ModemType) | [202] | n/a | c32 | [202] | n/a | c32 |
| 75 | T38 FAX Vendor Info  (a=T38VendorInfo) | [202] | n/a | c32 | [202] | n/a | c32 |
| 76 | reduced-size RTCP (a=rtcp-rsize) | [204] | c33 | c33 | [204] | c34 | c34 |
| 77 | RTP control protocol extended report parameters (a=rtcp-xr) | [205] | c35 | c35 | [205] | c36 | c36 |
| 78 | maximum receive SDU size (a=3gpp\_MaxRecvSDUSize) | [9B] | c37 | c37 | [9B] | c38 | c38 |
| 79 | content (a=content) | [206] | c39 | c39 | [206] | c39 | c39 |
| 80 | generic header extension map definition (a=extmap) | [210] | c40 | c40 | [210] | c41 | c41 |
| 81 | image attribute (a=imageattr) | [211] | c42 | c42 | [211] | c43 | c43 |
| 82 | fingerprint (a=fingerprint) | [241] | c46 | c46 | [241] | c46 | c46 |
| 83 | msrp-cema (a=msrp-cema) | [214] | c47 | c47 | [214] | c47 | c47 |
| 84 | sctp-port (a=sctp-port) | [219] | c48 | c48 | [219] | c48 | c48 |
| 84A | max-message-size (a=max-message-size) | [219] | c68 | c68 | [219] | c48 | c48 |
| 85 | CS correlation (a=cs-correlation) | [155] 5.2.3.1 | c49 | c49 | [155] 5.2.3.1 | c49 | c49 |
| 86 | Alternate Connectivity (ALTC) Attribute (a=altc) | [228] | o | c50 | [228] | o | c50 |
| 87 | 3GPP MTSI RTCP-APP adaptation (a=3gpp\_mtsi\_app\_adapt) | [9B] | n/a | c51 | [9B] | n/a | c52 |
| 88 | 3GPP MTSI Pre-defined Region-of-Interest (ROI)  (a=predefined\_ROI) | [9B] | n/a | c53 | [9B] | n/a | c54 |
| 89 | RTP and RTCP multiplexed on one port (a=rtcp-mux) | [237], [237A] | c55 | c55 | [237], [237A] | c55 | c55 |
| 90 | data channel mapping (a=dcmap) | [238] | c56 | c56 | [238] | c56 | c56 |
| 91 | data channel subprotocol specific attributes (a=dcsa) | [238] | c55 | c56 | [238] | c56 | c56 |
| 92 | Media plane optimization for WebRTC Contact (a= tra-contact) | 7.5.4 | c57 | c57 | 7.5.4 | c57 | c57 |
| 93 | Media plane optimization for WebRTC m-line (a= tra-m-line) | 7.5.4 | c58 | c58 | 7.5.4 | c58 | c58 |
| 94 | Media plane optimization for WebRTC attribute (a= tra-att) | 7.5.4 | c57 | c57 | 7.5.4 | c57 | c57 |
| 95 | Media plane optimization for WebRTC bandwidth (a= tra-bw) | 7.5.4 | c57 | c57 | 7.5.4 | c57 | c57 |
| 96 | Media plane optimization for WebRTC SCTP-association (a= tra-SCTP-association) | 7.5.4 | c58 | c58 | 7.5.4 | c58 | c58 |
| 97 | Media plane optimization for WebRTC media line number (a= tra-media-line-number) | 7.5.4 | c59 | c59 | 7.5.4 | c59 | c59 |
| 98 | Enhanced bandwidth negotiation mechanism (a=bw-info) | [9B] | n/a | c60 | [9B] | n/a | c61 |
| 99 | Exclusive RTP and RTCP multiplexed on one port (a=rtcp-mux-only) | [246] | c63 | c63 | [246] | c63 | c63 |
| 100 | Simulcast stream description (a=simulcast) | [249] 6.1 | c64 | c64 | [249] 6.1 | c64 | c64 |
| 101 | Restriction identifier (a=rid) | [250] 10 | c65 | c65 | [250] 10 | c66 | c66 |
| 102 | 3GPP compact concurrent codec capabilities (a=ccc-list) | [9B] | n/a | c67 | [9B] | n/a | c67 |
| 103 | Delay Budget Information (DBI) RTCP feedback type (a=rtcp-fb:\* 3gpp-delay-budget) | [9B] 6.2.8 | n/a | c69 | [9B] 6.2.8 | n/a | c69 |
| 104 | ANBR Support attribute (a=anbr) | [9B] | n/a | c70 | [9B] | n/a | c70 |
| 105 | Label attribute (a=label) | [277] 4 | o | c71 | [277] 4 | o | c71 |
| 106 | 3GPP QoS hint attribute (a=3gpp-qos-hint) | [9B] 6.2.7.4 | n/a | c71 | [9B] 6.2.7.4 | n/a | c71 |
| c1: IF A.317/22 AND A.318/20 THEN o ELSE n/a - - integration of resource management and SIP, media level attribute name "a=".  c2: IF A.317/22 AND A.318/20 THEN m ELSE n/a - - integration of resource management and SIP, media level attribute name "a=".  c3: IF A.317/23 AND A.318/20 THEN o ELSE n/a - - grouping of media lines, media level attribute name "a=".  c4: IF A.317/23 AND A.318/20 THEN m ELSE n/a - - grouping of media lines, media level attribute name "a=".  c5: IF A.317/23 AND A.318/14 THEN o ELSE n/a - - grouping of media lines, session level attribute name "a=".  c6: IF A.317/23 AND A.318/14 THEN m ELSE n/a - - grouping of media lines, session level attribute name "a=".  c7: IF A.317/26 AND A.318/20 THEN m ELSE n/a - - TCP-based media transport in the session description protocol, media level attribute name "a=".  c8: IF A.318/14 THEN o ELSE x - - session level attribute name "a=".  c9: IF A.318/14 THEN m ELSE n/a - - session level attribute name "a=".  c10: IF A.318/20 THEN o ELSE x - - media level attribute name "a=".  c11: IF A.318/20 THEN m ELSE n/a - - media level attribute name "a=".  c12: IF A.317/27 AND A.318/20 THEN o ELSE n/a - - candidate IP addresses, media level attribute name "a=".  c13: IF A.317/27 AND A.318/20 THEN m ELSE n/a - - candidate IP addresses, media level attribute name "a=".  c14: IF A.317/28 AND A.318/20 THEN m ELSE n/a - - session description protocol format for binary floor control protocol streams, media level attribute name "a=".  c15: IF (A.317/29 AND A.318/20) THEN m ELSE n/a - - extended RTP profile for real-time transport control protocol (RTCP)-based feedback (RTP/AVPF), media level attribute name "a=".  c16: IF A.317/30 AND A.318/20 THEN m ELSE n/a - - SDP capability negotiation, media level attribute name "a=".  c17: IF A.317/32 AND A.318/20 THEN o ELSE n/a - - miscellaneous capabilities negotiation in the Session Description Protocol (SDP), media level attribute name "a=".  c18: IF A.317/32 AND A.318/20 THEN m ELSE n/a - - miscellaneous capabilities negotiation in the Session Description Protocol (SDP), media level attribute name "a=".  c19: IF A.317/33 AND (A.318/14 OR A.318/20) THEN o ELSE n/a - - bandwidth modifier packet rate parameter, media or session level attribute name "a=".  c20: IF A.317/34 AND A.317/36 AND A.318/20 THEN m ELSE n/a - - Secure Real-time Transport Protocol, media plane security using SDES, media level attribute name "a=".  c21: IF ((A.317/34 AND A.3D/21) OR A.3D/22) AND A.317/35 AND A.318/20 THEN m ELSE n/a - - Secure Real-time Transport Protocol, end-to-end media security using KMS, end-to-end media security for MSRP using TLS and KMS, MIKEY-TICKET, media level attribute name "a=".  c22: IF (A.317/37 OR A.317/37A OR A.317/37B OR A.317/37C OR A.317/37D) AND A.318/20 THEN m ELSE n/a - - end-to-access edge media security using SDES, end-to-access-edge media security for MSRP using TLS and certificate fingerprints, end-to-access-edge media security for BFCP using TLS and certificate fingerprints, end-to-access-edge media security for UDPTL using DTLS and certificate fingerprints, end-to-access-edge media security for RTP media using DTLS-SRTP and certificate fingerprints, media level attribute name "a=".  c23: IF A.317/38 THEN m ELSE n/a - - SDP media capabilities negotiation.  c24: IF A.317/38 AND A.318/14 THEN m ELSE n/a - - SDP media capabilities negotiation, session level attribute name "a=".  c25: IF A.317/40 AND A.318/20 THEN m ELSE n/a - - message session relay protocol, media level attribute name "a=".  c26: IF A.317/41 AND A.318/20 THEN o ELSE n/a - - a SDP offer/answer mechanism to enable file transfer, media level attribute name "a=".  c27: IF A.317/41 AND A.318/20 AND (A.3A/31 OR A.3A/33) THEN m ELSE IF A.317/41 AND A.318/20 AND NOT (A.3A/31 OR A.3A/33) THEN o ELSE n/a - - a SDP offer/answer mechanism to enable file transfer, media level attribute name "a=", messaging application server, messaging participant.  c28: IF A.317/41 AND A.318/20 THEN m ELSE n/a - - a SDP offer/answer mechanism to enable file transfer, media level attribute name "a=".  c29: IF A.317/42 AND A.318/20 THEN o ELSE n/a - - optimal media routeing, media level attribute name "a=".  c30: IF A.317/43 THEN m ELSE n/a - - ECN for RTP over UDP, media level attribute name "a=".  c31: IF A.317/44 AND A.318/20 THEN m ELSE n/a - - T.38 FAX, media level attribute name "a=".  c32: IF A.317/44 AND A.318/20 THEN o ELSE n/a - - T.38 FAX, media level attribute name "a=".  c33: IF A.317/45 AND A.318/20 THEN o ELSE n/a - - support for reduced-size RTCP, media level attribute name "a=".  c34: IF A.317/45 AND A.318/20 THEN m ELSE n/a - - support for reduced-size RTCP, media level attribute name "a=".  c35: IF A.317/46 AND A.318/20 AND A.318/14 THEN o ELSE n/a - - RTCP extended reports, media level attribute name "a=", session level attribute name "a=".  c36: IF A.317/46 AND A.318/20 AND A.318/14 THEN m ELSE n/a - - RTCP extended reports, media level attribute name "a=", session level attribute name "a=".  c37: IF A.317/47 AND A.318/20 AND A.318/14 THEN o ELSE n/a - - maximum receive SDU size, media level attribute name "a=", session level attribute name "a=".  c38: IF A.317/47 AND A.318/20 AND A.318/14 THEN m ELSE n/a - - maximum receive SDU size, media level attribute name "a=", session level attribute name "a=".  c39: IF A.317/48 AND A.318/20 THEN m ELSE n/a - - the SDP content attribute, media level attribute name "a=".  c40: IF A.317/49 AND A.318/20 AND A.318/14 THEN o ELSE n/a - - a general mechanism for RTP header extensions, media level attribute name "a=", session level attribute name "a=". | | | | | | | |
| c41: IF A.317/49 AND A.318/20 AND A.318/14 THEN m ELSE n/a - - a general mechanism for RTP header extensions, media level attribute name "a=", session level attribute name "a=".  c42: IF A.317/50 AND A.318/20 THEN o ELSE n/a - - negotiation of generic image attributes in the session description protocol (SDP), media level attribute name "a=".  c43: IF A.317/50 AND A.318/20 THEN m ELSE n/a - - negotiation of generic image attributes in the session description protocol (SDP), media level attribute name "a=".  c44: IF A.317/38 AND A.318/20 THEN m ELSE n/a - - SDP media capabilities negotiation, media level attribute name "a=".  c45: IF (A.317/26 OR A.317/52) AND A.318/20 THEN m ELSE n/a - - TCP-based media transport in the session description protocol, UDPTL over DTLS, media level attribute name "a=".  c46: IF (A.317/51 OR A.317/55) AND A.318/20 AND A.318/14 THEN m ELSE n/a - - connection-oriented media transport over the TLS protocol in the SDP, DTLS-SRTP, media level attribute name "a=", session level attribute name "a=".  c47: IF A.317/40A AND A.318/20 THEN m ELSE n/a - - connection establishment for media anchoring for the message session relay protocol, media level attribute name "a=".  c48: IF A.317/54 AND A.318/20 THEN m ELSE n/a - - SCTP over DTLS, media level attribute name "a=".  c49: IF A.317/31 AND A.318/20 THEN m ELSE n/a - - Session Description Protocol (SDP) extension for setting up audio media streams over circuit-switched bearers in the Public Switched Telephone Network (PSTN) and SIP, media level attribute name "a=".  c50: IF A.317/57 AND A.318/20 THEN o ELSE n/a - - Alternate Connectivity (ALTC) Attribute, media level attribute name "a="  c51: IF A.317/58 AND A.318/20 THEN o ELSE n/a - - 3GPP MTSI RTCP-APP adaptation, media level attribute name "a=".  c52: IF A.317/58 AND A.318/20 THEN m ELSE n/a - - 3GPP MTSI RTCP-APP adaptation, media level attribute name "a=".  c53: IF A.317/59 AND A.318/20 THEN o ELSE n/a - - 3GPP MTSI Pre-defined Region-of-Interest (ROI), media level attribute name "a=".  c54: IF A.317/59 AND A.318/20 THEN m ELSE n/a - - 3GPP MTSI Pre-defined Region-of-Interest (ROI), media level attribute name "a=".  c55: IF A.317/61 AND A.318/20 THEN m ELSE n/a - - multiplexing RTP data and control packets on a single port, media level attribute name "a=".  c56: IF A.317/62 AND A.318/20 THEN m ELSE n/a - - SDP-based data channel negotiation, media level attribute name "a=".  c57: IF A.317/63 AND (A.318/14 OR A.318/20) THEN o ELSE n/a - -, Media plane optimization for WebRTC session or media level attribute name "a=".  c58: IF A.317/63 AND A.318/20 THEN o ELSE n/a - -, Media plane optimization for WebRTC media level attribute name "a=".  c59: IF A.317/63 AND A.318/14 THEN o ELSE n/a - -, Media plane optimization for WebRTC session level attribute name "a=".  c60: IF A.317/64 AND A.318/20 THEN o ELSE n/a - - Enhanced bandwidth negotiation mechanism, media level attribute name "a=".  c61: IF A.317/64 AND A.318/20 THEN m ELSE n/a - - Enhanced bandwidth negotiation mechanism, media level attribute name "a=".  c62: IF (A.317/52 OR A.317/54 OR A.317/55) AND A.318/20 THEN m ELSE n/a - - UDPTL over DTLS, SCTP over DTLS, DTLS-SRTP, media level attribute name "a=".  c63: IF A.317/61A AND A.318/20 THEN m ELSE n/a - - Exclusive RTP and RTCP multiplexed on one port (a=rtcp-mux-only), media level attribute name "a=".  c64: IF A.317/66 AND A.318/20 THEN m ELSE n/a - - Using simulcast in SDP and RTP sessions, media level attribute name "a=".  c65: IF A.317/67 AND A.318/20 THEN o ELSE n/a - - RTP payload format restrictions, media level attribute name "a=".  c66: IF A.317/67 AND A.318/20 THEN m ELSE n/a - - RTP payload format restrictions, media level attribute name "a=".  c67: IF A.317/68 AND A.318/14 THEN o ELSE n/a - - Compact Concurrent Codec Negotiation and Capabilities, session level attribute name "a=".  c68: IF A.317/54 AND A.318/20 THEN o ELSE n/a - - SCTP over DTLS, media level attribute name "a=".  c69: IF A.317/69 AND A.318/20 THEN m ELSE n/a - - Delay Budget Information (DBI), media level attribute name "a=".  c70: IF A.317/70 AND A.318/20 THEN m ELSE n/a - - Access Network Bitrate Recommendation (ANBR), media level attribute name "a=".  c71: IF (A.317/71 OR A.317/72) AND A.318/20 THEN o ELSE n/a - - Framework for Live Uplink Streaming (FLUS), 3GPP MTSI client using data channels, media level attribute name "a=". | | | | | | | |
| NOTE 1: Further specification of the usage of this attribute is defined by specifications relating to individual codecs. | | | | | | | |

Prerequisite A.319/80 - - a= generic header extension map definition (a=extmap)

Table A.319A: RTP header extensions

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Item | Field | Sending | | | Receiving | | |
| Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | coordination of video orientation (urn:3gpp:video-orientation) | [9B] | n/a | o | [9B] | n/a | o |
| 2 | higher granularity coordination of video orientation (urn:3gpp:video-orientation:6) | [9B] | n/a | c1 | [9B] | n/a | c1 |
| 3 | video region-of-interest predefined-roi-sent (urn:3gpp: predefined-roi-sent) | [9B] | n/a | c2 | [9B] | n/a | c2 |
| 4 | video region-of-interest arbitrary-roi-sent (urn:3gpp:roi-sent) | [9B] | n/a | c3 | [9B] | n/a | c3 |
| c1: IF A.319A/1 THEN o ELSE n/a - - coordination of video orientation.  c2: IF A.317/59 THEN o ELSE n/a - - 3GPP MTSI Pre-defined Region-of-Interest (ROI).  c3: IF A.317/60 THEN o ELSE n/a - - 3GPP MTSI Arbitrary Region-of-Interest (ROI). | | | | | | | |

\*\*\* Next Change \*\*\*

### A.3.3.1 Major capabilities

Table A.328: Major capabilities

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item | Does the implementation support | Reference | RFC status | Profile status |
|  | **Capabilities within main protocol** |  |  |  |
| 0A | application of session policy? | 6.2, 6.3 | x | c2 |
|  | **Extensions** |  |  |  |
| 1 | integration of resource management and SIP? | [30] [64] | o | n/a |
| 2 | grouping of media lines? | [53] | c3 | x |
| 3 | mapping of media streams to resource reservation flows? | [54] | o | x |
| 4 | SDP bandwidth modifiers for RTCP bandwidth? | [56] | o | c1 |
| 5 | TCP-based media transport in the session description protocol? | [83] | o | c11 |
| 6 | interactive connectivity establishment? | [289], [290] | o | c4 |
| 7 | session description protocol format for binary floor control protocol streams? | [108] | o | o |
| 8 | extended RTP profile for real-time transport control protocol (RTCP)-based feedback (RTP/AVPF)? | [135] | o | c5 |
| 9 | SDP capability negotiation? | [137] | o | c9 |
| 10 | Session Description Protocol (SDP) extension for setting up audio media streams over circuit-switched bearers in the Public Switched Telephone Network (PSTN)? | [155] | o | c6 |
| 11 | miscellaneous capabilities negotiation in the Session Description Protocol (SDP)? | [156] | o | c6 |
| 14 | Secure Real-time Transport Protocol (SRTP)? | [169] | o | o |
| 15 | MIKEY-TICKET? | [170] | o | o |
| 16 | SDES? | [168] | o | o |
| 17 | end-to-access edge media security using SDES? | 7.5.2 | n/a | n/a |
| 17A | end-to-access-edge media security for MSRP using TLS and certificate fingerprints? | 7.5.2 | n/a | n/a |
| 17B | end-to-access-edge media security for BFCP using TLS and certificate fingerprints? | 7.5.2 | n/a | n/a |
| 17C | end-to-access-edge media security for UDPTL using DTLS and certificate fingerprints? | 7.5.2 | n/a | n/a |
| 17D | end-to-access-edge media security for RTP media using DTLS-SRTP and certificate fingerprints? | 7.5.2 | n/a | n/a |
| 18 | SDP media capabilities negotiation? | [172] | o | c8 |
| 19 | Transcoding Services Invocation in the Session Initiation Protocol (SIP) Using Third Party Call Control (3pcc)? | [166] | m | i |
| 20 | Message Session Relay Protocol? | [178] | o | o |
| 20A | Connection establishment for media anchoring for the message session relay protocol? | [214] | o | c12 |
| 21 | a SDP offer/answer mechanism to enable file transfer? | [185] | o | o |
| 22 | optimal media routeing? | [11D] | n/a | o |
| 23 | ECN for RTP over UDP? | [188] | o | c10 |
| 24 | T.38 FAX? | [202] | n/a | o |
| 25 | support for reduced-size RTCP? | [204] | o | o |
| 26 | RTCP extended reports? | [205] | o | o |
| 27 | maximum receive SDU size? | [9B] | o | o |
| 28 | the SDP content attribute | [206] | o | o |
| 29 | a general mechanism for RTP header extensions? | [210] | o | o |
| 30 | negotiation of generic image attributes in the session description protocol (SDP)? | [211] | o | o |
| 31 | connection-oriented media transport over the TLS protocol in the SDP? | [241] | o | o |
| 32 | UDPTL over DTLS? | [217] | o | o |
| 33 | telepresence? | [7G] | o | o |
| 34 | SCTP over DTLS? | [219] | o | o |
| 35 | DTLS-SRTP? | [222], [223] | o | o |
| 36 | STUN Usage for Consent Freshness? | [224] | o | o |
| 38 | 3GPP MTSI RTCP-APP adaptation? | [9B] | n/a | o |
| 39 | 3GPP MTSI Pre-defined Region of Interest (ROI)? | [9B] | n/a | o |
| 40 | 3GPP MTSI Arbitrary Region-of-Interest (ROI)? | [9B] | n/a | o |
| 41 | multiplexing RTP data and control packets on a single port | [237], [237A] | o | o |
| 42 | Media plane optimization for WebRTC | 7.5.4 | n/a | o |
| 43 | Enhanced bandwidth negotiation mechanism | [9B] | n/a | o |
| 45 | an SDP offer/answer mechanism to negotiate DTLS protected media? | [240] | o | c13 |
| 46 | Using simulcast in SDP and RTP sessions? | [249] | o | o |
| 47 | RTP payload format restrictions? | [250] | o | o |
| 48 | Compact Concurrent Codec Negotiation and Capabilities? | [9B] | n/a | o |
| 49 | 3GPP MTSI Delay Budget Information (DBI)? | [9B] | n/a | c14 |
| 50 | Access Network Bitrate Recommendation (ANBR)? | [9B] | n/a | c15 |
| 51 | Framework for Live Uplink Streaming (FLUS)? | [276] | n/a | c15 |
| 52 | 3GPP MTSI client using data channels? | [9B] | n/a | c15 |
| c1: IF A.3/2 OR A.3A/88 THEN m ELSE n/a - - P-CSCF, ATCF (proxy).  c2: IF A.3/2 OR A.3/4 THEN o ELSE x – P-CSCF, S-CSCF.  c3: IF A.328/3 THEN m ELSE o - - mapping of media streams to resource reservation flows.  c4: IF A.3/2 OR A.3/4 THEN m ELSE n/a - - P-CSCF, S-CSCF.  c5: IF (A.3A/50A AND A.3/7C) OR A.3/2 OR A.3/4 OR A.3A/88 THEN m ELSE n/a - - multimedia telephony service application server as AS acting as a SIP proxy, P-CSCF, S-CSCF, ATCF (proxy).  c6: IF (A.3A/83 AND A.3/7C) OR A.3/4 THEN m ELSE IF A.3A/88 THEN i ELSE n/a - - SCC application server, AS acting as a SIP proxy, S-CSCF, ATCF (proxy).  c7: IF A.328/18 THEN m ELSE o - - SDP media capabilities negotiation.  c8: IF A.3/2 OR A.3/4 THEN m ELSE IF A.3A/88 THEN i ELSE o - - P-CSCF, S-CSCF, ATCF (proxy).  c9: IF (A.3A/50A AND A.3/7C) OR A.3/2 OR A.3/4 OR A.328/18 OR A.3A/88 THEN m ELSE n/a - - multimedia telephony service application server as AS acting as a SIP proxy, P-CSCF, S-CSCF, SDP media capabilities negotiation, ATCF (proxy).  c10: IF A.3A/88 THEN o ELSE i - - ATCF (proxy).  c11: IF A.3/2 OR A.3/4 OR A.3A/88 THEN m ELSE n/a - - P-CSCF, S-CSCF, ATCF (proxy).  c12: IF A.328/20 THEN m ELSE n/a - - message session relay protocol.  c13: IF A.328/32 OR A.328/34 OR A.328/35 THEN m ELSE n/a - - UDPTL over DTLS, SCTP over DTLS, DTLS-SRTP.  c14: IF A.3/2 OR A.3/4 THEN o ELSE n/a - - P-CSCF, S-CSCF.  c15: If A.3/2 THEN o ELSE n/a - - P-CSCF. | | | | |

\*\*\* End of Changes \*\*\*