**3GPP TSG-CT WG1 Meeting #123-eC1-202xxx**

**Electronic meeting, 16-24 April 2020 was C1-202551**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **24.379** | **CR** | **0556** | **rev** | **1** | **Current version:** | **16.4.0** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

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

|  |
| --- |
|  |
| ***Title:***  | Authorisation validation for first-to-answer call origination requesting user using pre-established session |
|  |  |
| ***Source to WG:*** | Samsung |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | MCProtoc16 |  | ***Date:*** | 2020-03-19 |
|  |  |  |  |  |
| ***Category:*** | **F**  |  | ***Release:*** | Rel-16 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)Rel-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | In subclause 11.1.1.2.2.1 of pre-established session case, user authorisation to originate the first-to-answer call is missing and same validation exist in case of on demand session. |
|  |  |
| ***Summary of change:*** | New step 2) has been included in subclause 11.1.1.2.2.1 client originating procedure for first-to-answer call based on pre-established session. |
|  |  |
| ***Consequences if not approved:*** | Handling at client can avoid the request being rejected from server and in-consistence procedure across the sections. |
|  |  |
| ***Clauses affected:*** | 11.1.1.2.2.1 |
|  |  |
|  | **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 \* \* \* \* \* \* \*

###### 11.1.1.2.2.1 Client originating procedures

Upon receiving a request from an MCPTT user to establish an MCPTT private call within a pre-established session the MCPTT client shall generate a SIP REFER request outside a dialog in accordance with the procedures specified in 3GPP TS 24.229 [4], IETF RFC 4488 [22] and IETF RFC 3515 [25] as updated by IETF RFC 6665 [26] and IETF RFC 7647 [27], with the clarifications given below.

If the user requested the private call to be a first-to-answer call, if the <allow-request-first-to-answer-call> element of the <ruleset> element is not present in the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) or is set to a value of "false", the MCPTT client shall inform the MCPTT user and shall exit this procedure.

If the MCPTT user is initiating a private call and an end-to-end security context needs to be established the MCPTT client:

1) if necessary, shall instruct the key management client to request keying material from the key management server as described in 3GPP TS 33.180 [78];

2) shall use the keying material to generate a PCK as described in 3GPP TS 33.180 [78];

3) shall use the PCK to generate a PCK-ID with the four most significant bits set to "0001" to indicate that the purpose of the PCK is to protect private call communications and with the remaining twenty eight bits being randomly generated as described in 3GPP TS 33.180 [78];

4) shall encrypt the PCK to a UID associated to the MCPTT client using the MCPTT ID and KMS URI of the invited user as determined by the procedures of subclause 6.2.8.3.9 and a time related parameter as described in 3GPP TS 33.180 [78];

5) shall generate a MIKEY-SAKKE I\_MESSAGE using the encapsulated PCK and PCK-ID as specified in 3GPP TS 33.180 [78];

6) shall add the MCPTT ID of the originating MCPTT to the initiator field (IDRi) of the I\_MESSAGE as described in 3GPP TS 33.180 [78]; and

7) shall sign the MIKEY-SAKKE I\_MESSAGE using the originating MCPTT user's signing key provided in the keying material together with a time related parameter, and add this to the MIKEY-SAKKE payload, as described in 3GPP TS 33.180 [78].

The MCPTT client populates the SIP REFER request as follows:

1) shall include the Request-URI set to the public service identity identifying the pre-established session on the MCPTT server serving the MCPTT user;

2) shall include the Refer-Sub header field with value "false" according to rules and procedures of IETF RFC 4488 [22];

3) shall include the Supported header field with value "norefersub" according to rules and procedures of IETF RFC 4488 [22];

4) shall include the option tag "multiple-refer" in the Require header field;

5) may include a P-Preferred-Identity header field in the SIP REFER request containing a public user identity as specified in 3GPP TS 24.229 [4];

6) shall include a P-Preferred-Service header field set to the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcptt" (coded as specified in 3GPP TS 24.229 [4]), according to IETF RFC 6050 [9];

7) shall set the Refer-To header field of the SIP REFER request as specified in IETF RFC 3515 [25] with a Content-ID ("cid") Uniform Resource Locator (URL) as specified in IETF RFC 2392 [62] that points to an application/resource-lists MIME body as specified in IETF RFC 5366 [20], and with the Content-ID header field set to this "cid" URL;

8) for the initiation of a private call, shall include in the application/resource-lists MIME body a single <entry> element containing a "uri" attribute set to the MCPTT ID of the called user, extended with the following URI header fields:

NOTE 1: Characters that are not formatted as ASCII characters are escaped in the following parameters in the headers portion of the SIP URI.

a) if force of automatic commencement mode at the invited MCPTT client is requested by the MCPTT user, shall include a Priv-Answer-Mode header field with the value "Auto" according to the rules and procedures of IETF RFC 5373 [18];

b) if force of automatic commencement mode at the invited MCPTT client is not requested by the MCPTT user and:

i) if automatic commencement mode at the invited MCPTT client is requested by the MCPTT user, shall include an Answer-Mode header field with the value "Automatic" according to rules and procedures of IETF RFC 5373 [18]; and

ii) if manual commencement mode at the invited MCPTT client is requested by the MCPTT user, shall include an Answer-Mode header field with the value "Manual" according to rules and procedures of IETF RFC 5373 [18]; and

c) shall include in an hname "body" parameter:

i) if the SDP parameters of the pre-established session do not contain a media-level section of a media-floor control entity or if end-to-end security is required for the private call, an application/sdp MIME body containing the SDP parameters of the pre-established session according to 3GPP TS 24.229 [4] with the clarifications given in subclause 6.2.1. If implicit floor control is required and the pre-established session was not established with an implicit floor request, then the application/sdp MIME body shall contain an implicit floor request as specified in subclause 6.4; and

ii) an application/vnd.3gpp.mcptt-info MIME body:

A) with the <session-type> element set to "private"; and

B) if the MCPTT client needs to include an active functional alias in the SIP REFER request, with the <functional-alias-URI> set to the URI of the used functional alias;

NOTE 2: The MCPTT client learns the functional aliases that are activated for an MCPTT ID from procedures specified in subclause 9A.2.1.3.

9) for an initiation of a first-to-answer call, shall include in the application/resource-lists MIME body an <entry> element for each of the targeted MCPTT users, with each <entry> element containing a "uri" attribute set to the MCPTT ID of the targeted user, extended with hname "body" parameter in the headers portion of the SIP URI containing:

NOTE 3: Characters that are not formatted as ASCII characters are escaped in the following parameters in the headers portion of the SIP URI.

a) if the SDP parameters of the pre-established session do not contain a media-level section of a media-floor control entity, an application/sdp MIME body containing the SDP parameters of the pre-established session according to 3GPP TS 24.229 [4] with the clarification given in subclause 6.2.1. If implicit floor control is required and the pre-established session was not established with an implicit floor request, then the application/sdp MIME body shall contain an implicit floor request as specified in subclause 6.4; and

b) an application/vnd.3gpp.mcptt-info MIME body with the <session-type> element set to "first-to-answer";

10) if the MCPTT user has requested the origination of an MCPTT emergency private call or is originating an MCPTT private call and the MCPTT emergency state is already set, the MCPTT client:

a) if this is an authorised request for an MCPTT emergency private call as determined by the procedures of subclause 6.2.8.3.1.1, shall comply with the procedures in subclause 6.2.8.3.2; and

b) if this is an unauthorised request for an MCPTT emergency private call as determined in step a) above, should indicate to the MCPTT user that they are not authorised to initiate an MCPTT emergency private call;

11) if the MCPTT emergency private priority state for this call is set to "MEPP 2: in-progress", the MCPTT client shall comply with the procedures in subclause 6.2.8.3.3;

12) shall include a Target-Dialog header field as specified in IETF RFC 4538 [23] identifying the pre-established session; and

13) if:

a) implicit floor control is required;

b) the pre-established session was not established with an implicit floor request; and

c) location information has not yet been included in the SIP REFER request;

 then shall include an application/vnd.3gpp.mcptt-location-info+xml MIME body with a <Report> element included in the <location-info> root element.

The MCPTT client shall send the SIP REFER request towards the MCPTT server according to 3GPP TS 24.229 [4].

Upon receiving a final SIP 2xx response to the SIP REFER request the MCPTT client shall interact with media plane as specified in 3GPP TS 24.380 [5].

On receiving a SIP 4xx response, SIP 5xx response or a SIP 6xx response to the SIP REFER request for an MCPTT emergency private call:

1) if the MCPTT emergency private call state is set to "MEPC 2: emergency-pc-requested", the MCPTT client shall perform the actions specified in subclause 6.2.8.3.5; and

2) shall skip the remaining steps.

Upon receipt of a SIP re-INVITE request within the pre-established session targeted by the sent SIP REFER request, the MCPTT client:

1) if the sent SIP REFER request was a request to originate a first-to-answer call:

a) if the received SIP re-INVITE request contains an SDP offer including an a=key-mgmt attribute field with a "mikey" attribute value containing a MIKEY-SAKKE I\_MESSAGE:

i) shall extract the MCPTT ID of the sender of the SIP 200 (OK) response from the initiator field (IDRi) of the I\_MESSAGE as described in 3GPP TS 33.180 [78];

ii) shall convert the MCPTT ID to a UID as described in 3GPP TS 33.180 [78];

iii) shall use the UID to validate the signature of the MIKEY-SAKKE I\_MESSAGE as described in 3GPP TS 33.180 [78];

iv) if authentication verification of the MIKEY-SAKKE I\_MESSAGE fails:

A) shall set the MCPTT emergency private call state to "MEPC 1: emergency-pc-capable";

B) if the MCPTT emergency private priority state of the private call is "MEPP 3: confirm-pending" shall set the MCPTT emergency private priority state of the private call to "MEPP 1: no-emergency";

C) if the sent SIP request for an MCPTT emergency private call contained an application/vnd.3gpp.mcptt-info+xml MIME body with an <alert-ind> element set to a value of "true", shall set the MCPTT private emergency alert state to "MPEA 1: no-alert"; and

D) shall release the session as specified in the procedures of subclause 11.1.3.1.2.1 with the following clarifications:

I) shall include in the SIP BYE request an application/vnd.3gpp.mcptt-info+xml MIME body containing a <release-reason> element set to a value of "authentication of the MIKEY-SAKE I\_MESSAGE failed"; and

II) shall skip the remaining steps in the present subclause; and

v) if the signature of the MIKEY-SAKKE I\_MESSAGE was successfully validated:

A) shall extract and decrypt the encapsulated PCK using the originating user's (KMS provisioned) UID key as described in 3GPP TS 33.180 [78]; and

B) shall extract the PCK-ID, from the payload as specified in 3GPP TS 33.180 [78];

NOTE 4: With the PCK successfully shared between the originating MCPTT client and the terminating MCPTT client, both clients are able to use SRTP/SRTCP to create an end-to-end secure session.

2) if the sent SIP REFER request was a request for an MCPTT emergency private call:

a) if the MCPTT emergency private call state is set to "MEPC 2: emergency-pc-requested" or "MEPC 3: emergency-pc-granted":

i) shall set the MCPTT emergency private priority state of the call to "MEPP 2: in-progress" if it was not already set;

ii) shall set the MCPTT emergency private call state to "MEPC 3: emergency-pc-granted"; and

iii) if the MCPTT private emergency alert state is set to "MPEA 2: emergency-alert-confirm-pending" and:

A) if the SIP re-INVITE request contains an <alert-ind> element set to a value of "true" or does not contain an <alert-ind> element, shall set the MCPTT private emergency alert state to " MPEA 3: emergency-alert-initiated "; or

B) if the SIP re-INVITE request contains an <alert-ind> element set to a value of "false", shall set the MCPTT private emergency alert state to "MPEA 1: no-alert ";

3) shall check if a Resource-Priority header field is included in the incoming SIP re-INVITE request and may perform further actions outside the scope of this specification to act upon an included Resource-Priority header field as specified in 3GPP TS 24.229 [4];

4) shall accept the SIP re-INVITE request and generate a SIP 200 (OK) response according to rules and procedures of 3GPP TS 24.229 [4];

5) shall include an SDP answer in the SIP 200 (OK) response to the SDP offer in the incoming SIP re-INVITE request according to 3GPP TS 24.229 [4], based upon the parameters already negotiated for the pre-established session; and

6) shall send the SIP 200 (OK) response towards the participating MCPTT function according to rules and procedures of 3GPP TS 24.229 [4].

On call release by interaction with the media plane as specified in subclause 9.2.2 of 3GPP TS 24.380 [5] if the sent SIP REFER request was a request for an MCPTT emergency private call, the MCPTT client shall perform the procedures specified in subclause 6.2.8.1.18.

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