**3GPP TSG-CT WG1 Meeting #133-e *draft1 rev1* C1-216632**

**E-meeting, 11-19 Novembe 2021**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.379** | **CR** | **0760** | **rev** | **1** | **Current version:** | **17.4.0** |  |
|  | | | | | | | | |
| *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:*** | Interconnect – MCPTT Gateway server procedures | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Airbus | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | MCSMI\_CT | | | | |  | ***Date:*** | | | 04/11/2021 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | As specified in TS 23.280, when MCPTT systems in different trust domains are interconnected, MCPTT gateway servers are inserted in the path between the controlling and participating functions that are in the different domains.  This is done transparently to the involved participating and controlling functions.  One role of the MCPTT gateway server is to provide topology hiding.  Another role of the MCPTT Gateway server is to apply local policies such as control, configuration, sensitive data exposure. That role is implementation dependent. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Reference new clauses from clause 5.5.1  Add new warning texts  Add a clause in the common procedures to specify MCPTT gateway server behavior.  Use primary/partner based on the system where the message was originated | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Interconnection os MCPTT systems from different trust domains would not be possible | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.4.2, 5.5.1, 6.X (new), 6.X.1 (new), 6.X.2 (new), 6.X.3 (new), 6.X.4 (new) | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\*\*\* Next change \*\*\*

### 4.4.2 Warning texts

The text string included in a Warning header field consists of an explanatory text preceded by a 3-digit text code, according to the following format in Table 4.4.2-1.

Table 4.4.2-1 ABNF for the Warning text

warn-text =/ DQUOTE mcptt-warn-code SP mcptt-warn-text DQUOTE

mcptt-warn-code = DIGIT DIGIT DIGIT

mcptt-warn-text = \*( qdtext | quoted-pair )

Table 4.4.2-2 defines the warning texts that are defined for the Warning header field when a Warning header field is included in a response to a SIP INVITE request as specified in clause 4.4.1.

Table 4.4.2-2: Warning texts defined for the Warning header field

|  |  |  |
| --- | --- | --- |
| Code | Explanatory text | Description |
| 100 | function not allowed due to <detailed reason> | The function is not allowed to this user.  The <detailed reason> will be either "group definition", "access policy", "local policy", "user authorisation" or "pre-established session not supported", or can be a free text string. |
| 101 | service authorisation failed | The service authorisation of the MCPTT ID against the IMPU failed at the MCPTT server. |
| 102 | too many simultaneous affiliations | The MCPTT user already has N2 maximum number of simultaneous affiliations (see <MaxAffiliationsN2> element of user profile configuration document). |
| 103 | maximum simultaneous MCPTT group calls reached | The number of maximum simultaneous MCPTT group calls supported for the MCPTT user has been exceeded. |
| 104 | isfocus not assigned | A controlling MCPTT function has not been assigned to the MCPTT session. |
| 105 | subscription not allowed in a broadcast group call | Subscription to the conference event package rejected during a group call initiated as a broadcast group call. |
| 106 | user not authorised to join chat group | The MCPTT user is not authorised to join this chat group. |
| 107 | user not authorised to make private calls | The MCPTT user is not authorised to make private calls. |
| 108 | user not authorised to make chat group calls | The MCPTT user is not authorised to make chat group calls. |
| 109 | user not authorised to make prearranged group calls | The MCPTT user is not authorised to make group calls to a prearranged group. |
| 110 | user declined the call invitation | The MCPTT user declined to accept the call. |
| 111 | group call proceeded without all required group members | The required members of the group did not respond within the acknowledged call time, but the call still went ahead. |
| 112 | group call abandoned due to required group members not part of the group session | The group call was abandoned, as the required members of the group did not respond within the acknowledged call time. |
| 113 | group document does not exist | The group document requested from the group management server does not exist. |
| 114 | unable to retrieve group document | The group document exists on the group management server but the MCPTT server was unable to retrieve it. |
| 115 | group is disabled | The group has the <disabled> element set to "true" in the group management server. |
| 116 | user is not part of the MCPTT group | The group exists on the group management server but the requesting user is not part of this group. |
| 117 | the group identity indicated in the request is a prearranged group | The group id that is indicated in the request is for a prearranged group, but did not match the request from the MCPTT user. |
| 118 | the group identity indicated in the request is a chat group | The group id that is indicated in the request is for a chat group, but did not match the request from the MCPTT user. |
| 119 | user is not authorised to initiate the group call | The MCPTT user identified by the MCPTT ID is not authorised to initiate the group call. |
| 120 | user is not affiliated to this group | The MCPTT user is not affiliated to the group. |
| 121 | user is not authorised to join the group call | The MCPTT user identified by the MCPTT ID is not authorised to join the group call. |
| 122 | too many participants | The group call has reached its maximum number of participants. |
| 123 | MCPTT session already exists | Inform the MCPTT user that the group call is currently ongoing. |
| 124 | maximum number of private calls reached | The maximum number of private calls allowed at the MCPTT server for the MCPTT user has been reached. |
| 125 | user not authorised to make private call with automatic commencement | The MCPTT user is not authorised to make a private call with automatic commencement. |
| 126 | user not authorised to make private call with manual commencement | The MCPTT user is not authorised to make a private call with manual commencement. |
| 127 | user not authorised to be called in private call | The called MCPTT user is not allowed to be part of a private call. |
| 128 | isfocus already assigned | The MCPTT server owning an MCPTT group received a SIP INVITE request destined to the MCPTT group from another MCPTT server already assigned as the controlling MCPTT function and the MCPTT server owning the MCPTT group does not support mutual aid or supports trusted mutual aid but does not authorise trusted mutual aid. |
| 136 | authentication of the MIKEY-SAKKE I\_MESSAGE failed | The MCPTT client's application of the procedures of 3GPP TS 33.180 [78] to authenticate the received I\_MESSAGE fails. |
| 137 | the indicated group call does not exist | The participating MCPTT function cannot find an ongoing group session associated with the received MCPTT session identity. |
| 138 | subscription of conference events not allowed | The controlling MCPTT function could not allow the MCPTT user to subscribe to the conference event package. |
| 139 | integrity protection check failed | The integrity protection of an XML MIME body failed. |
| 140 | unable to decrypt XML content | The XML content cannot be decrypted. |
| 141 | user unknown to the participating function | The participating function is unable to associate the public user identity with an MCPTT ID. |
| 142 | unable to determine the controlling function | The participating function is unable to determine the controlling function for the group call or private call. |
| 143 | not authorised to force auto answer | The calling user is not authorised to force auto answer on the called user. |
| 144 | user not authorised to call this particular user | The calling user is not authorised to call this particular called user. |
| 145 | unable to determine called party | The participating function was unable to determine the called party from the information received in the SIP request. |
| 146 | T-PF unable to determine the service settings for the called user | The service settings have not been uploaded by the terminating client to the terminating participating server. |
| 147 | user is authorized to initiate a temporary group call | The non-controlling MCPTT function has authorized a request from the controlling MCPTT function to authorize a user to initiate an temporary group session. |
| 148 | group is regrouped | The group hosted by a non-controlling function is part of a temporary group session as the result of the group regroup function. |
| 149 | SIP-INFO request pending | The MCPTT client needs to wait for a SIP-INFO request with specific content, before taking further action. |
| 150 | invalid combinations of data received in MIME body | The MCPTT client included invalid combinations of data in the SIP request. |
| 151 | user not authorised to make a private call call-back request | The MCPTT user is not authorised to make a private call call-back request. |
| 152 | user not authorised to make a private call call-back cancel request | The MCPTT user is not authorised to make a private call call-back cancel request. |
| 153 | user not authorised to call any of the users requested in the first-to-answer call | All users that were invited in the first-to-answer call cannot be involved in a private call with the inviting user. |
| 154 | user not authorised to make ambient listening call | The MCPTT user is not authorised to make an ambient listening call. |
| 155 | user not authorised to change user's selected group | The MCPTT user is not authorised to change the selected group of the targeted user. |
| 156 | user not authorised to originate a first-to-answer call | The MCPTT user is not authorised to make a first-to-answer call. |
| 157 | user not authorised to request a remotely initiated group call | The MCPTT user is not authorised to request a remotely initiated group call. |
| 158 | user not authorised to request a remotely initiated private call | The MCPTT user is not authorised to request a remotely initiated private call. |
| 159 | user not authorised to be called by this originating user | The called user is not authorised to receive a call by this originating user. |
| 160 | user not authorised to request creation of a regroup | The user is not authorised to request creation of a regroup. |
| 161 | user not authorised to request removal of a regroup | The user is not authorised to request removal of a regroup. |
| 162 | group call abandoned due to required group members not affiliated | The group call was abandoned as the required number of affiliated group members is not met or some required members are not affiliated. |
| 163 | the group identity indicated in the request does not exist | The server determines that the group identity indicates a user or group regroup based on a preconfigured group that does not exist. |
| 164 | maximum number of service authorizations reached | The number of maximum simultaneous service authorizations for the MCPTT user has been reached. |
| 165 | group ID for regroup already in use | The group ID proposed by the client for the user/group regroup based on a preconfigured group is already in use. |
| 166 | constituent group is in an emergency call state | The proposed constituent group cannot be added to the temporary group because there is a call on the constituent group that is in an emergency state. |
| 167 | call is not allowed on the preconfigured group | Calls are not allowed on this group that is administratively designated for preconfigured group use only. |
| 168 | alert is not allowed on the preconfigured group | Alerts are not allowed on this group that is administratively designated for preconfigured group use only. |
| 169 | user is not authorised to remove regroup in an emergency state | The MCPTT user is not authorised to remove a regroup that is in an in-progress emergency state. |
| 170 | user not authorised to make a private call transfer request | The MCPTT user is not authorised to make a private call transfer request. |
| 171 | functional alias not allowed to call this particular functional alias | The calling user is not authorised to call this particular functional alias by using this activated functional alias |
| 172 | functional alias not allowed to be called from this functional alias | The called functional alias is not authorised to receive a call from the originating user using this particular Functional Alias |
| 173 | user not authorised to make a private call forwarding request | The MCPTT user is not authorized to use MCPTT private call forwarding |
| 174 | maximum number of allowed forwardings exceeded | The maximum number of allowed call forwardings has been exceeded |
| 175 | call is forwarded | The MCPTT private call that is requested to be established is released, and a new MCPTT private call is originated to the target of the call forwarding |
| 1xx | service not authorized with the partner system | The MCPTT service is not authorized between the primary and the partner system and is rejected in the primary system |
| 1yy | Service is not authorized by the partner system | The MCPTT service is not authorized between the primary and the partner system and is rejected by the partner system |

\*\*\* Next change \*\*\*

### 5.5.1 General

To allow interconnection between MCPTT system in different trust domains, MC Gateway Servers can be optionally added on the path between controlling and participating MCPTT functions.

An MCPTT gateway server acts as a SIP and HTTP proxy for signalling with a partner MCPTT system in a different trust domain.

An MCPTT gateway server acts as an application and security gateway with a partner MCPTT system in a different trust domain.

An MCPTT gateway server provides topology hiding to the partner MCPTT system in a different trust domain.

An MCPTT gateway server enforces local policies and local security.

An MCPTT gateway server can be an exit point from its MCPTT system to a partner MCPTT system in a different trust domain, an entry point to its MCPTT system from a partner MCPTT system in a different trust domain, or both.

An MCPTT gateway server is transparent to MCPTT controlling and participating servers. When required for interconnection, MC gateway servers URIs are known and used by MCPTT servers in place of the PSIs of the interconnected MCPTT server. The MCPTT server does not need to know if it finally addresses directly an MCPTT controlling function or an intermediate MCPTT gateway server.

To be compliant with the procedures in the present document, an MCPTT gateway server shall:

- support the MC gateway server procedures defined in 3GPP TS 23.280 [82] and 3GPP TS 23.379 [3]; and

- support the MC gateway server procedures defined in 3GPP TS 33.180 [78];

- implement the procedures specified in clause 6.X

To be compliant with the procedures for confidentiality protection in the present document, the MCPTT gateway server shall implement the procedures specified in clause 6.6.2, acting on behalf of the MCPTT server when sending or receiving confidentiality protected content to or from an MCPTT server in another trust domain.

To be compliant with the procedures for integrity protection of XML MIME bodies in the present document, the MCPTT gateway server shall implement the procedures specified in clause 6.6.3, acting on behalf of the MCPTT server when sending or receiving integrity protected content to or from an MCPTT server in another trust domain.

\*\*\* Next change \*\*\*

## 6.X Procedures at the MCPTT gateway

### 6.X.1 General

As described in clause 5.5, the MCPTT gateway servers are inserted in the path between MCPTT functions that reside in MCPTT systems from different trust domains.

This clause specifies the behavior of an MCPTT gateway server that acts as an exit point from a primary MCPTT system or as an entry point in a partner MCPTT system

Local policies enforcement covers a wide variety of actions that are left to implementation. An example of local policies enforcement is given in clause 6.X.4.

### 6.X.2 MCPTT gateway server acting as an exit point from a primary MCPTT system

When acting as an exit point from a primary MCPTT system to a partner MCPTT system, the MCPTT gateway server receives SIP requests and SIP responses intended for the controlling, non-controlling or participating function in the partner MCPTT system.

When receiving an outgoing SIP message, the MCPTT gateway server acting as an exit point:

1) shall identify the MCPTT system identity of the partner MCPTT system from the Request-URI of the outgoing SIP messages or other information elements from the outgoing SIP message;

2) may enforce local policy, and. if local policy enforcement results in rejecting a SIP request (e.g. not having a mutual aid relationship), the MCPTT gateway shall reject the request by sending back a SIP 403 (Forbidden) response including a warning text "1xx service not authorized with the partner system", and the MCPTT gateway server shall not continue with the rest of the steps;

3) shall replace in the outgoing SIP message any addressing information linked to the primary MCPTT system topology with its own addressing information. This includes;

a) the P-Asserted-Identity header field shall be set to the MCPTT gateway server's own URI; and

b) the Request-URI shall be set to the public service identity of the targeted function in the partner MCPTT system, or to the URI of the MCPTT gateway server that acts as an entry point in the partner MCPTT system; and

NOTE: How the MCPTT gateway server distinguishes SIP requests and SIP responses and determines the public service identity of the targeted MCPTT function in the partner MCPTT system or the URI of the MCPTT gateway server in the partner MCPTT system is out of the scope of the present document.

4) shall forward the outgoing SIP message according to 3GPP TS 24.229 [4]

### 6.X.3 MCPTT gateway server acting as an entry point in a partner MCPTT system

When acting as an entry point in a partner MCPTT system from a primary MCPTT system, the MCPTT gateway receives SIP requests and SIP responses intended for the controlling, non-controlling or participating function in the partner MCPTT system.

When receiving an incoming SIP message, the MCPTT gateway server acting as an entry point:

1) shall identify the MCPTT system identity of the primary MCPTT system from the P-Asserted-Identity header field of the incoming SIP messages;

2) may enforce local policy, and. if local policy enforcement results in rejecting a SIP request (e.g. not having a mutual aid relationship), the MCPTT gateway shall reject the request by sending back a SIP 403 (Forbidden) response including a warning text "1yy service not authorized by the partner system", and the MCPTT gateway server shall not continue with the rest of the steps;

3) shall replace in the incoming SIP message its own addressing information with the addressing information of the targeted MCPTT function in the partner MCPTT system:

a) the Request-URI shall be set to the public service identity of the targeted MCPTT function in the partner MCPTT system; and

NOTE: How the MCPTT gateway server distinguishes SIP requests and SIP responses and determines the public service identity of the targeted MCPTT function in the partner MCPTT system is out of the scope of the present document.

4) shall forward the incoming SIP message according to 3GPP TS 24.229 [4]

### 6.X.4 Local policies enforcement

Below is one example of local policy enforcement that can be handled by an MCPTT gateway server.

If an MCPTT gateway server acting as an exit point receives a SIP request or a SIP response that contains sensitive information that cannot be exposed to the targeted partner system based on local policies but does not prevent the service from being delivered (e.g. a functional alias), the MCPTT gateway server can remove that information from the outgoing SIP message before forwarding it.

\*\*\* End of change \*\*\*