The Standards People

Observations Plugtests

Presented by: **Saurav Arora & Fidel Liberal**

For: **3GPP WGs**

© ETSI

Observation 1: Ambiguity in mcptt-request-uri in notification entry/exit group area

Description - An inconsistency has been identified in subclause ~~6.3.3.1.22~~ => 6.3.2.4.2 in 3GPP TS 24.379 regarding the value of REQUEST URI being MCPTT ID of the user <mcptt-request-uri> being the group ID (i.e. in 6.3.2.4.1 the MCPTT ID is used for the equivalent functionality)

ANALYSIS: STILL MISSING/DISMISSED? in 24379-h31
REQUEST URI should be set to user public identity and not MCPTT ID
in the Participating -> terminating client interface
according to 6.3.2.2.11 and consequently
<mcptt-request-uri> should be set to MCPTT ID and not group ID
Draft CR C1-20XXXX_e_CR_Rel-15_TS24.379_Request-URI
and <mcptt-request-uri> in SIP messages for entry in geo areas.docx

6.3.2.4.2 Generating a SIP MESSAGE request for notification of entry into or exit from a group geographic area

This clause describes the procedures for generating a SIP MESSAGE request to notify an MCPTT client that it has entered a pre-defined group geographic area or exited from a pre-defined group geographic area requiring affiliation to or de-affiliation from a group. The procedure is initiated by the participating MCPTT function when the participating MCPTT function determines that the MCPTT client has entered a pre-defined group geographic area or exited from a pre-defined group geographic area.

The participating MCPTT function:

1) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [4] and IETF RFC 3428 [33];
2) shall include an Accept-Contact header field containing the g.3gpp.mcptt media feature tag along with the "require" and "explicit" header field parameters according to IETF RFC 3841 [6];
3) shall include an Accept-Contact header field with the media feature tag g.3gpp.icsi-ref with the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt" along with parameters "require" and "explicit" according to IETF RFC 3841 [6];
4) shall set the Request-URI to the MCPTT ID of the public user identity of the targeted MCPTT user;
5) shall include a P-Asserted-Identity header field set to the public service identity of the participating MCPTT function;
6) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcptt" (coded as specified in 3GPP TS 24.229 [4]), in a P-Asserted-Service-Id header field according to IETF RFC 6050 [9];
7) shall include an application/vnd.3gpp.mcptt-info+xml MIME body with the <mcpttinfo> element containing the <mcptt-Params> element with the <mcptt-request-uri> element set to the value of the MCPTT ID of the targeted MCPTT user;
8) shall include in the application/vnd.3gpp.mcptt-info+xml MIME body an <mcpttinfo> element containing the <mcptt-Params> element with

Release 17 106 3GPP TS 24.379 V17.3.1 (2021-06)

a) an <mcptt-request-uri> element set to the group identity of the group for which a pre-defined group geographic area has been entered or exited;

© ETSI

Observation 2: Need to affiliate to a MCPTT group upon entering a pre-defined geographic group area.

Description – 3GPP TS 24.379 subclause ~~6.3.3.1.22~~ => 6.3.2.4.2 states that "request to notify an MCPTT client that it has entered a pre-defined group geographic area or exited from a pre-defined group geographic area requiring affiliation to or de-affiliation from a group". However, in subclause 12.1.1.4 only the de-affiliation is mentioned during step 2b) iii) shall execute the procedure in subclause 9.2.1.2 to de-affiliate from the group indicated by the participating MCPTT function." but not the affiliation process (that should be in the counterpart 2a and would be needed for geofencing-like operations).

Solution could be to explicitly state the need for affiliation but including equivalent reference in the subclause 2a) iii)

ANALYSIS: FIXED in 24379-h31 for Rel17

Side NOTE: Ambient Listening reference has been also removed

3GPP TS 24.229 [4].

12.1.1.4 MCPTT client receives notification of entry into or exit from a group geographic area

Upon receipt of a "SIP MESSAGE request for notification of entry into or exit from a group geographic area", the MCPTT client;

1) shall send a SIP 200 (OK) to the participating MCPTT function that sent the SIP MESSAGE request; and

2) if the <group-geo-area-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body is:

a) set to "true":

i) may display to the MCPTT user an indication that a group geographic area has been entered; and

ii) shall execute the procedure in clause 9.2.1.2 to affiliate to the group indicated by the participating MCPTT function; or

b) set to "false":

i) may display to the MCPTT user an indication that a group geographic area has been exited; and

ii) shall execute the procedure in clause 9.2.1.2 to de-affiliate from the group indicated by the participating MCPTT function.

12.1.1.5 MCPTT group in-progress emergency group state cancel

Upon receiving a request from an MCPTT user to cancel the in-progress emergency condition on a prearranged MCPTT group on which there is no call ongoing, the MCPTT client shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [4] and IETF RFC 3428 [33] with the clarifications given below.

Release 17 472 3GPP TS 24.379 V17.3.1 (2021-06)

© ETSI

Observation 3: Ambiguity regarding the use of MCPTT user ID vs. MCPTT client ID in functional alias related pidf formatting

Description- Subclauses 9A.2 and 9A.3 (coding) in 3GPP 24.379 mismatch in terms of the id to be included in the tuple element of the PIDF (fixed in Release 16 to the MCPTT Client ID and not the User ID) in the for per-user informatior and the id in the per-functional one (fixed in Release 16 to the MCPTT ID and not the FA). The behaviour of the Participating server regarding the client ID is not properly described even in Rel16 and such fixes have not been portec to 15.8.0.

ANALYSIS: FIXED in 24379-h31 for Rel17
NOT BACKPORTED TO 24379-fb0

Solution

2) contains an "entity" attribute of the <presence> element set to the MCPTT ID of the MCPTT user;

3) contains one <tuple> child element according to IETF RFC 3863 [52] per <presence> element;

4) can contain a <p-id-fa> child element defined in the XML schema defined in table 9A.3.1.2-1, of the <presence> element set to an identifier of a SIP PUBLISH request;

5) contains an "id" attribute of the <tuple> element set to the MCPTT ~~user~~client ID;

6) contains one <status> child element of each <tuple> element;

7) contains one <functionalAlias> child element defined in the XML schema defined in table 9A.3.1.2-1, of the <status> element, for each functional alias in which the MCPTT user is interested;

8) contains a "functionalAliasID" attribute of each <fucntionalAlias> element set to the functional alias ID of the functional alias in which the MCPTT user is interested;;

9) can contain a "status" attribute of each <functionalAliasID> element indicating the activation status of functional alias for the MCPTT user; and

10) can contain an "expires" attribute of each <functionalAlias> element indicating expiration of activation of the functional alias for the MCPTT user.

The application/pidf+xml MIME body indicating per-functional alias status information is constructed according to IETF RFC 3856 [51] and:

1) contains the <presence> root element according to IETF RFC 3863 [52];

2) contains an "entity" attribute of the <presence> element set to the functional alias ID of the functional alias;

3) contains one <tuple> child element according to IETF RFC 3863 [52] of the <presence> element;

4) can contain a <p-id-fa> child element defined in the XML schema defined in table 9A.3.1.2-1, of the <presence> element set to an identifier of a SIP PUBLISH request;

5) contains an "id" attribute of the <tuple> element set to the ~~functional alias~~MCPTT ID;

6) contains one <status> child element of each <tuple> element;

7) contains one <functionalAlias> child element defined in the XML schema defined in table 9A.3.1.2-1, of the <status> element, for each MCPTT ID for which functional alias information is provided;

8) contains one "user" attribute defined in the XML schema defined in table 9A.3.1.2-2, of the <functionalAlias> element set to the MCPTT ~~user~~client ID; and

9) can contain an "expires" attribute defined in the XML schema defined in table 9A.3.1.2-2, of the <functionalAlias> element indicating expiration of activation of the functional alias for the MCPTT user.

© ETSI

Observation 4: FA activation refresh operation

Description - In Subclause 9A.2.1.1 in 3GPP TS 24.379 the use of SIP PUBLISH mechanism to refresh the interest on a FA is defined. The TS however only defines the use of full SIP PUBLISH for activation (with mcptt-info and pidf+xml bodies) while the refresh mechanism in IETF RFC 3903 makes use of empty body PUBLISH with SIP-if-match: previously received ETAG.

Solution – Clarification needed from CT1.

ANALYSIS: OUTDATED
Addressed initially in 17.3.2_C1-21305 C1-213589
TO be checked by plugtests participants and eventually
to be merged with Observation 31?

© ETSI

Observation 5:Determination of the FAs activated for another user (1/2)

Description - From the Subclause 9A.2.1.3 in 3GPP TS 24.379 the mcptt-request-uri in the SUBSCRIBE can be either the own one of another user's. Later, it states:

"3) if the Request-URI of the SIP SUBSCRIBE request contains the public service identity identifying the terminating participating MCPTT function serving the MCPTT user, shall identify the originating MCPTT ID in the <mcptt-calling-user-id> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP SUBSCRIBE request;"

That would mean that "somehow" the terminating participating MCPTT functions receives a SUBSCRIBE with the mcptt-calling-user-id fulfilled. It looks like it would be the originating participating (serving the initial user) the one including such information and forwarding it (but it's not explicitly specified in step 2 of the Subclause).

© ETSI

Observation 5 (2/2)

During the plugtest the equivalent approach to the that covered in test case "[AFFIL/DET/02]: subscription to the affiliation status of other user" was agreed.

In fact step 4 in 9A.2.2.2.4 Receiving subscription to functional alias status procedure would look like an error since it refers to the change of status, not to determination.

"4) if the originating MCPTT ID is different than the served MCPTT ID and the originating MCPTT ID is not authorized to modify functional alias status of the served MCPTT ID, shall send a SIP 403 (Forbidden) response and shall not continue with the rest of the steps; and"

Solution – The originating will check the mapping between PAI and mpctt-id, include it as <mpctt-calling-user-id> and route it to the terminating.

ANALYSIS: FIXED in 24379-h31 for Rel17 out of C1-211151

NOTE: FORMAT ERROR -header X- in Rel15

- a sending functional alias status change towards MCPTT server owning the functional procedure;
- a functional alias status determination from MCPTT server owning the functional alias procedure; and

24.379	0690	2	17.1.0	Rel-17	Determination of the FAs activated by another user	C1-211484	agreed	CP-210105	approved	17.2.0
24.379	0690	1	17.1.0	Rel-17	Determination of the FAs activated by another user	C1-211153	revised			
24.379	0690	-	17.1.0	Rel-17	Determination of the FAs activated by another user	C1-211131	revised			
24.379	0689	2	16.7.0	Rel-16	Determination of the FAs activated by another user	C1-211483	agreed	CP-210105	approved	16.8.0
24.379	0689	1	16.7.0	Rel-16	Determination of the FAs activated by another user	C1-211152	revised			
24.379	0689	-	16.7.0	Rel-16	Determination of the FAs activated by another user	C1-211129	revised			
24.379	0688	2	15.9.0	Rel-15	Determination of the FAs activated by another user	C1-211482	agreed	CP-210105	approved	15.10.0

- a forwarding subscription to functional alias status towards another MCPTT server procedure, which is used to identify the status of functional aliases activated by a target user who is served by another MCPTT server.9A.2.2.2.2 Stored information

Observation 6: Inclusion of status attribute of the <functionalAlias>

Description - According to 3GPP TS 24.379 Subclause 9A.2.1.2 the client "shall not include the "status" attribute and the "expires" attribute in the <functionalAlias> element".

However, in the participating part, Subclause 9A.2.2.2.6 only states that "The MCPTT server shall not include the "expires" attribute in the <functionalAlias> element". Although later the controlling has no specific logic to process such attribute the reference to include status has been removed.

Solution - We have included the status parameter in the PUBLISH from PAS=>CAS.

Clarification would be required from the relevant WG.

ANALYSIS: No change identified, dismissed? Little to no relevance…

© ETSI

Observation 7: Missing privateCallList -and probably others- element in MCVideo user profile

Description - Although Subclause 6.2.8.3.9 in 3GPP TS 24 281 states that "…shall search for the <entry> element of the <PrivateCallURI> element of the <PrivateCallList> element entry of the <Common> element of the MCVideo user profile document (see the MCVideo user profile document in 3GPP TS 24.484 [50]) containing the identified MCVideo ID;…" there is no privateCallList in the MCVideo user profile XSD in 3GPP TS 24 484 even in latest Release 16.

Solution - Agree with the counterpart in p2p basis (MCVideo client provider) whether this components needs to be added to the MCVideo UE profile.

Fixing in the XSD (or the text).

ANALYSIS: FIXED
due to MAJOR REFACTORING OF XSDs

Release 17 59 3GPP TS 24.484 V17.2.0 (2021-06)

1) shall include an "XUI-URI" attribute;
2) may include a <Name> element;
3) shall include one <Status> element;
4) shall include a "user-profile-index" attribute;
5) may include any other attribute for the purposes of extensibility;
6) may include one <ProfileName> element;
7) may include a <Pre-selected-indication> element;
8) shall include one <Common> element, which:
   a) shall have an "index" attribute;
   b) shall include one <UserAlias> element containing one or more <alias-entry> elements;
   c) shall include one <MCPTTUserID> element that contains a <uri-entry> element;
   d) shall include one <PrivateCall> element. The <PrivateCall> element contains:
      i) a <PrivateCallList> element that contains one or more of the following:

© ETSI

Observation 8:(Non)mandatory download and HTTP in MCData (1/2)

Observation : In 10.2.1.1 in 3GPP TS 24 282 the following procedure for the MCData Client wrt. mandatory download is defined:

1) shall follow the procedures in subclause 11.1 for transmission control; and

2) if the procedures in subclause 11.1 are successful:

a) if requiring to send data without mandatory download, shall follow the procedures in subclause 10.2.4; and

b) if requiring to send data with mandatory download, shall follow the the procedures in subclause 10.2.5.

© ETSI

Observation 8:(Non)mandatory download and HTTP in MCData (2/2)

Where 10.2.4 refers to the use of SIP MESSAGE and H

However, even in 6.2.2.2 Generating an FD Message f
download at the recipient side, shall include a Manda
set to the value of "MANDATORY DOWNLOAD";"

Furthermore, the Controlling could decide to include
the payload upon checking 11.2 conditions, resulting
the MANDATORY DOWNLOAD ie set.

Solution - We assume that a FD request using HTTP a
mandatory download i.e. FD signalling payload regard
Removal of 10.2.1.1 reference to the use of HTTP/MS
clarification.

ANALYSIS: FIXED C1-213070=>C1-213596=>CP-211157

10 File Distribution (FD)

10.1 General

The group administrator can disable the FD service on a MCData group by setting the <mcdata-allow-file-distribution> element under the <list-service> element, in the group document, to "false".

If the <mcdata-allow-file-distribution> element under the <list-service> element, in the group document, is set to "false" for a MCData group:

- an MCData client should not use the procedures in the subclauses of the parent subclause for FD to the said MCData group.
- a terminating MCData controlling function should reject the request for FD to the said MCData group.

10.2 On-network FD

10.2.1 General

10.2.1.1 Sending an FD message

When the MCData user wishes to send:

- a one-to-one standalone File Distribution (FD) message to another MCData user; or
- a group standalone File Distribution (FD) message to a pre-configured group;

the MCData client:

1) shall follow the procedures in subclause 11.1 for transmission control; and
2) if the procedures in subclause 11.1 are successful:
   a) if the MCData client decides to use HTTP, shall follow the procedures in subclause 10.2.4; and
   b) if the MCData client decides to use the media plane, shall follow the the procedures in subclause 10.2.5.

© ETSI

Observation 9: Value of Accept-Contact for the request of a list of deferred group communications

Description - Subclause 11.3 in 3GPP TS 24 282 refers to 6.2.4.1 for building the initial SIP message for requesting the list of deferred group S messages, SDS disposition notification and FD m FD MSF discovery messages are listed.

Therefore, the type of Accept-Contact for this re

Solution - FD is assumed.

ANALYSIS: Still missing, solution straightforward, included in the draft CR

* * * * * * FIRST CHANGE * * * * * * *

6.2.4.1 Generating a SIP MESSAGE request towards the originating participating MCData function

This subclause is referenced from other procedures.

In a SIP MESSAGE request, the MCData client:

1) when sending SDS messages or SDS disposition notifications:

   a) shall include an Accept-Contact header field containing the g.3gpp.mcdata.sds media feature tag along with the "require" and "explicit" header field parameters according to IETF RFC 3841 [8];

   b) shall include an Accept-Contact header field with the media feature tag g.3gpp.icsi-ref containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" along with the "require" and "explicit" header field parameters according to IETF RFC 3841 [8]; and

   c) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.sds" (coded as specified in 3GPP TS 24.229 [5]), in a P-Preferred-Service header field according to IETF RFC 6050 [7] in the SIP MESSAGE request;

2) when sending FD messages, FD disposition notifications ~~or~~, FD media storage function discovery or access a list of deferred group communications messages:

   a) shall include an Accept-Contact header field containing the g.3gpp.mcdata.fd media feature tag along with the "require" and "explicit" header field parameters according to IETF RFC 3841 [8];

   b) shall include an Accept-Contact header field with the media feature tag g.3gpp.icsi-ref containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" along with the "require" and "explicit" header field parameters according to IETF RFC 3841 [8]; and

   c) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcdata.fd" (coded as specified in 3GPP TS 24.229 [5]), in a P-Preferred-Service header field according to IETF RFC 6050 [7] in the SIP MESSAGE request;

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

4) shall set the Request-URI to the public service identity identifying the participating MCData function serving the MCData user.

* * * * * * * END CHANGES * * * * * * *

© ETSI

Observation 10: Role of controlling and participating in the deferred group communications list retrieval

Description - Subclause 11.3.3 in 3GPP TS 24 282 describes the behaviour of the participating MCData function upon receiving a request to access the list of deferred group communications. However, it looks like the role of the controlling is missing while the participating mentions forwarding messages back/from the controlling.

Upon receipt of a "SIP MESSAGE request for the list of deferred group communications", the participating MCData function:

1) shall generate a SIP 200 (OK) response according to 3GPP TS 24.229 [5];
2) shall send SIP 200 (OK) response towards MCData server according to 3GPP TS 24.229 [5]; and
3) shall follow the procedure described in subclause 11.3.3.2 to send response.

While no other mention to the role of the controlling can be extrapolated.

Solution - A role for the controlling and participating could be drafted in the TS.

ANALYSIS: Still missing, and overall sequence diagram unclear (see red-marked above)

© ETSI

Observation 11:Gaps in regrouping mechanism

Description - Ambiguous statement regarding the need for affiliation to the super group in A.1.3 in 3GPP TS 24.379. The following precondition is stated: "1) the temporary group mcptt-group-A-B is already created and all members are affiliated to the group".

However, the mcptt-group-A-B has only other (sub)groups as members. Furthermore, even in that case untrusted model is considered so that any mechanism for affiliation to the supergroup by users would be anyway troublesome.

Solution – To remove reference to affiliation

ANALYSIS: DISMISSED? Mcpttt-group-T reference in Annex A has not been fixed

© ETSI

Observation 12: Unsolicited notify (or updates to new - unsubscribed before- documents)

Description - From Subclause 5.7.3 in 3GPP TS 33 180 there are two possible options considered for the associated possible subscription to group document:

“When users are added to a new or existing group they may be implicitly affiliated to that group” in which case “the user is automatically subscribed to group configuration updates from the GMS”. The user shall be authorised for group management services to the GMS before the GMS provides the associated group management records and the GMK. Once the user is authorised, the GMS sends the group management record as well as the GMK to the UE.

"When the user configuration record indicates the user has been added to a new or existing group but is required to explicitly affiliate to the group", the user shall be authorised for group management services to the GMS followed by a subscription to group updates from the GMS. The user shall be authorised for group management services and the subscription shall be validated before the GMS provides group management records and the GMK. Once the user is authorised and the subscription processed by the GMS, the GMS sends the group management record and the GMK to the UE.

In the first case, how the NOTIFY will be processed by the MCPTT Client without prior subscription and no Access Token to be used for Authorisation is unclear.licited notify (or updates to new - unsubscribed before- documents)

Solution - NA

From: Tim Woodward <tim.woodward@motorolasolutions.com>
Sent: Tuesday, May 4, 2021 10:53 AM
To: William Janky <William.Janky@firstnet.gov>
Cc: Fidel Liberal <fidel.liberal@ehu.eus>; Michael Dolan <Michael.Dolan@Firstnet.gov>; Jeffrey Cichonski <jeffrey.cichonski@nist.gov>; Saurav Arora <Saurav.Arora@etsi.org>
Subject: Re: Unsolicited Notify (Observ. 12)

I'll generate a CR to correct the text in 33.180 regarding automatic subscription. As far as releases, how far back do we think we need to go?

© ETSI

Observation 12: Unsolicited notify (or updates to new -

33180-h30.pdf

'Security Gateway' bit in the 'Status' field of the GMK's key parameters (see clause E.6.9).

Should an MC client receive a GMK with the 'Security Gateway' bit set, the initiating MC client shall warn the MC user that an MC Security Gateway is in use during the group's comunications.

5.7.3 Group member GMK management

In some situations, the membership of a group may be modified whereby an MC user may be added to or removed from an MCX group. Users are alerted to these changes by a user profile update from the CMS for which they are subscribed. The updated user configuration profile indicates the group ID to which the group membership change is associated.

When users are added to a new or existing group they may be implicitly affiliated to that group in which case the user is automatically subscribed to group configuration updates from the GMS. The user shall be authorised for group management services to the GMS before the GMS provides the associated group management records and the GMK. Once the user is authorised, the GMS sends the group management record as well as the GMK to the UE. The user may join in on the group communication immediately after receiving the group update and GMK.

When the user configuration record indicates the user has been added to a new or existing group but is required to explicitly affiliate to the group, the user shall be authorised for group management services to the GMS followed by a subscription to group updates from the GMS. The user shall be authorised for group management services and the subscription shall be validated before the GMS provides group management records and the GMK. Once the user is authorised and the subscription processed by the GMS, the GMS sends the group management record and the GMK to the UE. The user may then join in on the group communication immediately after receiving the group update and GMK.

When a user is removed from a group, the UE receives a user profile update from the CMS indicating the user is no longer a member of the specified group ID(s). Upon receiving the user profile update, ending of any group communication(s) associated with that group, and if the GMK associated with the group ID is not associated with another group that the user remains a member, the UE shall immediately and securely delete the GMK associated with that group ID. If the group ID is associated to more than one service (i.e. MCPTT, MCData and/or MCVideo) then upon the ending of any group communication(s) associated with that group ID, and if the GMKs associated with that group ID is not associated with another group that the user remains a member, the GMKs associated with that group ID shall be immediately and securely deleted.

When a user is removed from the group, the Group Management Server may choose to update the GMK associated with the group ID (depending on the security profile of the group).

5.8 Key management from MC server to MC client (Key download)

33180-f50.pdf

Should an MC client receive a GMK with the 'Security Gateway' bit set, the initiating MC client shall warn the MC user that an MC Security Gateway is in use during the group's comunications.

5.7.3 Group member GMK management

In some situations, the membership of a group may be modified whereby an MC user may be added to or removed from an MCX group. Users are alerted to these changes by a user profile update from the CMS for which they are subscribed. The updated user configuration profile indicates the group ID to which the group membership change is associated.

When users are added to a new or existing group they may be implicitly affiliated to that group in which case the user is automatically subscribed to group configuration updates from the GMS. The user shall be authorised for group management services to the GMS before the GMS provides the associated group management records and the GMK. Once the user is authorised, the GMS sends the group management record as well as the GMK to the UE. The user may join in on the group communication immediately after receiving the group update and GMK.

When the user configuration record indicates the user has been added to a new or existing group but is required to explicitly affiliate to the group, the user shall be authorised for group management services to the GMS followed by a subscription to group updates from the GMS. The user shall be authorised for group management services and the subscription shall be validated before the GMS provides group management records and the GMK. Once the user is authorised and the subscription processed by the GMS, the GMS sends the group management record and the GMK to the UE. The user may then join in on the group communication immediately after receiving the group update and GMK.

When a user is removed from a group, the UE receives a user profile update from the CMS indicating the user is no longer a member of the specified group ID(s). Upon receiving the user profile update, ending of any group communication(s) associated with that group, and if the GMK associated with the group ID is not associated with another group that the user remains a member, the UE shall immediately and securely delete the GMK associated with that group ID. If the group ID is associated to more than one service (i.e. MCPTT, MCData and/or MCVideo) then

3GPP

Release 15 61 3GPP TS 33.180 V15.5.0 (2019-06)

upon the ending of any group communication(s) associated with that group ID, and if the GMKs associated with that group ID is not associated with another group that the user remains a member, the GMKs associated with that group ID shall be immediately and securely deleted.

When a user is removed from the group, the Group Management Server may choose to update the GMK associated with the group ID (depending on the security profile of the group).

ANALYSIS: Apparently no CR at least to 5.7.3….

© ETSI

Observation 13: Bindings between group membership information in CMS (user profile) and GMS (groups)

Description - Similarly to the previous observation, the sequence diagram of the procedures triggered by the addition of a user to a group -check IoP-4 for more information- or creation of new groups is not clear . More precisely, who keeps the consistency of the membership information distributed between the CMS and GMS is lacking. Furthermore, there's no reference to collections in GMS (which would allow subscription to any/all groups).

Solution - We have assumed there is no mechanism to subscribe to all groups in place since groups information in the GMS is global and not in User tree.

We have assumed the dispatcher/OAM is responsible for synching the information by firstly putting the updated group document to the GMS and later updating the User profile accordingly.

ANALYSIS: no action point/feedback?

© ETSI

Observation 14: Same SUBSCRIBE for functional alias and group affiliation

Description- Functional Alias determination specified in 3GPP TS 24.379 does not apparently provide an explicit mechanism to distinguish from the server pers
related one. In a participating and/or controlli
what type of SUBSCRIPTION has to be handlec

Was it the intention of the writer to combine t

Solution - Functional Alias subscription shall h
(in order to avoid possible XML validation issu

```
<mcptt-Params>
  <mcptt-request-uri type="Normal">
    <mcpttURI>sip:MCPTT_ID@ims.mnc001.m
  </mcptt-request-uri>
  '''<anyExt>'''
    '''<request-type>functional-alias-subscriptic
  '''</anyExt>'''
</mcptt-Params>
```

Release 17 **204** **3GPP TS 24.379 V17.3.1 (2021-06)**

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

9A.2.1.3 Functional alias status determination procedure

NOTE 1: The MCPTT UE also uses this procedure to determine which functional alias have been successfully activated for the MCPTT ID.

In order to discover functional aliases:

1) which which are activated for the MCPTT user; or

2) which another MCPTT user has activated;

the MCPTT client shall generate an initial SIP SUBSCRIBE request according to 3GPP TS 24.229 [4], IETF RFC 3856 [51], and IETF RFC 6665 [26].

In the SIP SUBSCRIBE request, the MCPTT client:

1) shall set the Request-URI to the public service identity identifying the originating participating MCPTT function serving the MCPTT user;

2) shall include an application/vnd.3gpp.mcptt-info+xml MIME body. In the application/vnd.3gpp.mcptt-info+xml MIME body, the MCPTT client shall include:

   a) the <mcptt-request-uri> element set to the MCPTT ID of the targeted MCPTT user; and

   b) the <request-type> element in the <anyExt> element of the <mcptt-Params> element of the <mcpttinfo> element set to the value "functional-alias-status-determination";

ANALYSIS: FIXED

© ETSI

Observation 16: Clarification of chat group behaviour in s2s signaling

Description - How roles are assigned and sequence diagram in the controlling vs non-controlling interfacing for chat group call is unclear in TS 24379

Solution- NA

ANALYSIS: no action point/feedback?

© ETSI

Observation 17: Drawbacks of using binary encoding for MCData Payloads transport in SIP MIME bodies

Description – As defined in 3GPP TS 24 282, the SIP SDS signaling payload message and Data Payload message are in binary format, but IETF SIP is a text-based protocol, and IETF has defined several encodings for MIME body like base64 that would make parsing probably easier for general purpose SIP stacks.

However, it seems clear that the 3GPP core specs mandate binary format and there are RFCs i.e. https://tools.ietf.org/html/rfc5621#section-3.2 (not specific of multipart but the "capability to handle binary data") and others that suggest using binary format in SIP would be possible (even convenient) according to sip standards.

Solution- NA

ANALYSIS: DISMISSED? I'd expect so

© ETSI

Observation 18: SDPs in private calls without floor control using pre-established sessions

Description – 3GPP TS 24.379 does not clearly state how full duplex (without floor control) private calls are performed over pre-established sessions. Current references onl DP me Plu ise 7.2 ent sol es wh

Sol

Wolfgang Seka Re: MCX - undeclared XML elements 79 KB 20/7/21, 11:55

Sent: Tuesday, August 3, 2021 9:55 AM
To: Michael Dolan <Michael.Dolan@Firstnet.gov>; 'Olivier Genoud' <Olivier.Genoud@etsi.org>
Cc: 'Francois Piroard' <fpiroairbus@gmail.com>; stoyan.baev@partner.samsung.com; 'Francois Piroard' <francois.piroard@airbus.com>; 'Timothy Woodward' <tim.woodward@motorolasolutions.com>; 'Kit Kilgour' <Kit.Kilgour@sepura.com>; sapan.shah@samsung.com; 'MOHAJERI, SHAHRAM' <sm7084@att.com>; 'VANK, ALEX' <av389j@att.com>; 'Wells, Derek' <Derek.Wells@l3harris.com>; 'Lazaros Gkatzikis' <lazaros.gkatzikis@nokia.com>; 'Rohit Nerlikar' <rohit.nerlikar@motorolasolutions.com>; 'Sivasubramaniam Ramanan' <Sivasubramaniam.Ramanan@homeoffice.gov.uk>; 'Estrella Basurto Domínguez' <estrella.basurto@nemergent-solutions.com>; 'Fidel Liberal' <fidel.liberal@ehu.eus>; 'Wolfgang Seka' <wolfgang.mcc160@gmail.com>; 'Dom Lazara' <dom.lazara@motorolasolutions.com>; 'Andoni Diaz de Cerio' <andoni.diazdecerio@nemergent-solutions.com>; 'Mikel Ramos' <mikel.ramos@ehu.eus>; stoyan.baev@imraff.com; 'Olaf Bergengruen' <olaf.bergengruen@adare.de>; 'Sudipto Biswas' <sudipto.biswas@motorolasolutions.com>; 'Piali Nath' <Piali.Nath[illegible]>; 'Rabindranath Das' <rabindranath.das@motorolasolutions.com>; 'Waltraud Bestelmeyer' <bestelmeyer-consulting@best-test.eu>; 'Dhiman Ghosh' <dhiman.ghosh@motorolasolutions.com>; David E. Cypher <david.cypher@nist.gov>; 'Harish Negalaguli' <harish.negalaguli@motorolasolutions.com>; 'Arunprasath Ramamoorthy' <arun.prasath@samsung.com>
Subject: RE: R5-213055: Issues with pre-established session establishment

mailto:stoyan.baev@imraff.com

Adding Arun to this email thread

Dear Mike, Olivier and All,

I think we need to allow some more discussion before reaching to the conclusion. The issue is not limited to only to a private call but for group call too.
So we should find a solution to mitigate the problem and also maintains the backward compatibility.

Regards,
Kiran

ANALYSIS: PENDING Overlaps with RAN5/Jason's request ;-)
Solution? Disable private calls over pre-established sessions

© ETSI

Observation 19: Key exchanging mechanism in first-to-answer pre-established session calls

Description- One of the modifications that were introduced in Rel.16 to 3GPP TS 24.379 comprised adapting the key exchange for first-to-answer on demand sessions. Instead of sending the mikey-sakke message with the key material in the initial INVITE, according to Rel 16 the "first to answer" destination shall introduce mikey-sakke message with the key material in the 200 OK. This solution was necessary as long as the caller would not know who the other party of the private call will be (so the caller can not generate the appropriate key material) till somebody actually answers. So, in this specific case the callee is the responsible of generating the appropriate key material for media encryption.

During the MCX Plugtests a discussion took place regarding whether this solution should be adapted for pre-established session scenarios. Currently first-to-answer and other private calls over pre-established sessions share the same key exchanging procedures. As it has been already appreciated by CT1 (in the on demand session solution) first-to-answer calls key exchanging has to be adapted from other private calls procedures. With the current core specs status first-to-answer calls over pre established sessions can not be performed with media encryption.

Solution - NA

ANALYSIS: Under discussion

© ETSI

Observation 20 :(Bootstrapping) provision and configuration of the client_id in IDMS

Description : According to TS 33.180, chapter B.4.2.2, the 'client_id' should be known on the IdMS server before the Authentication Request:

There may 2 possible ways to achieve it:

- either statically or out of band provided client-ids (and client-secrets);
- follow the "Dynamic Client Registration" procedure of OpenId Connect (https://openid.net/specs/openid-connect-registration-1_0.html</nowiki>).

Furthermore, 3GPP TS 24.379, clause 4.10, mandates that the ‘MCPTT client ID' should be generated client-side, so that the provisioning should be UE to IdMS.

In both cases there are some values that should be configured beforehand (in case 2, a "Registration Endpoint" is needed), but neither of them could be found in standard configuration documents.

It would be helpful if someone could clarify that it is different entity from the client_id used for IdMS procedures.

Solution - Starting with getting a official statement that the two client-ids are two separate entities, possible solutions are either:

- Add a <idms-registration-endpoint> alongside <idms-auth-endpoint> and <idms-token-endpoint> in MCS UE initial configuration document; or

ANALYSIS: Under discussion

- Replace <idms-auth-endpoint> and <idms-token-endpoint> elements with a <discovery-endpoint> element which serves all the configuration details as described in https://openid.net/specs/openid-connect-discovery-1_0.html#toc</nowiki>

© ETSI

Observations from FRMCS Plugtests (2021)

© ETSI

Observation 21: Mismatch between per-functional alias status information between 9A.3.1.2 and 9A.2.2.2.7

Description - The content of the pidf in the NOTIFY as a result of a per-functional alias status information subscription differs in which id atribute of the <tuple> element.

Solution – Suggestion to change 9A.3.1.2 5) element to the MCPTT ID

FRMCS O1

© ETSI

Observation 22: PAS/CAS to be in the media path of the IPCONN GRE tunnels being optional/mandatory (1/2)

Description - In TS 24.282 Subclause 20.1.3 (i.e. for the CAS), the CAS replacing the IP of the SDP with his own one seems to be not mandatory "shall replace the IP address for the offered media stream in the received SDP offer with the IP address of the controlling MC Data function, if required". This would allow e2e GRE tunnels without PAS/CAS becoming endpoints:

SIGNALLING => ORIGPAS CAS TERMPAS

MCDATA1 o==========o MCDATA2

vs.

MCDATA1 o===o ORIGPAS o===o CAS o===o TERMPAS o===o MCDATA2

However, later, in Subclause 20.4.1 (for the CAS) it states "1) shall interact with the media plane as specified in 3GPP TS 24.582" assuming it needs to be always in the media path.

Similarly, in 24.582 itself (i.e. Subclauses 13.2 and 13.3) the need for both PAS and CAS to be end points is

clear:

"13.2 Participating MCData function procedures

The participating MCData function shall provide an endpoint for an IP tunnel towards the MCData client, and a second endpoint for an IP tunnel towards the controlling MCData function. " .... "Additionally the participating MCData function shall act as an IP relay for the IP traffic between these two IP tunnels."

FRMCS O2

© ETSI

Observation 22: PAS/CAS to be in the media path of the IPCONN GRE tunnels being optional/mandatory (2/2)

"13.3 Controlling MCData function procedures

The controlling MCData function shall provide an endpoint for an IP tunnel towards the MCData originating participating MCData function, and a second endpoint for an IP tunnel towards the terminating participating MCData function. Additionally the controlling MCData function shall act as an IP relay for the IP traffic between these two IP tunnels."

Solution - Clarify the meaning of "if required" or simply remove it if PAS and CAS need to be in the media path.

FRMCS O2

© ETSI

Observation 23: [COMMENT] Usage of <functional-alias-URI> in chat group call

Description - The only mechanism to convey the functional-alias-URI to the other members of a chat group seems to be the SIP INVITE request, limited to very particular situations: subclause 10.1.2.2.1.6, “MCPTT client receives a SIP INVITE request for an MCPTT group call”, which is only used for MCPTT emergency and MCPTT imminent peril calls when the MCPTT client is affiliated but not joined to the chat group. Therefore this would be the only case where the MCPTT client “may display to the MCPTT user the functional alias of the inviting MCPTT user”.

Solution - NA

FRMCS O3

© ETSI

Observation 24: Forwarding the <call-to-functional-alias-ind> from the Controlling to the callees

Description - From subclauses 11.1.1.[3-4] is not clear if the intermediate components include the mcptt-info with the <call-to-functional-ind> element

Solution - NA

FRMCS O4

© ETSI

Observation 25: Not explicit inclusion of call-to-functional-alias-ind in first to answer over prestablished sessions

Description - Subclause 11.1.1.2.2.1 does not define the mechanism to be used for stating the URI in the RLS to be a functional alias.

Some ongoing discussion in CT1 (C1-212194).

Solution - Use the proposal in the aforementioned CR (straighfoward) involving adding the <call-to-functional-alias-ind> to the mcpttinfo in the REFER

FRMCS O5

© ETSI

Observation 26: Forwarding of SIP INFO with non acknowledged user information when using pre-stablished sessions (1/2)

Description - Subclause 6.3.3.3 defines the behaviour of the controlling server in terms of TNG1 timer handling and non acknowledged user information. When all the conditions are met the the controlling MCPTT function may generate a SIP INFO request including the Info-Package header field set to g.3gpp.mcptt-info in the SIP INFO request and n application/vnd.3gpp.mcptt-info+xml MIME body as specified in clause F.1 with a <non-acknowledged-user> element containing the MCPTT ID of each of the invited members that have not sent a SIP 200 (OK) response; and send the SIP INFO request towards the inviting MCPTT client in the dialog created by the SIP request from the inviting MCPTT client.

The controlling behaviour would also apply to prearranged group calls over pre-established sessions but how/whether the SIP INFO will be forwarded by the originating participating to the caller is not explicitely addressed.

The only not-that-similar reference is the behaviour of the participating when a SIP INFO is received from the controlling in emergency call resulting on a REINVITE in 6.3.2.1.8.5:

FRMCS O6

© ETSI

Observation 26: Forwarding of SIP INFO with non acknowledged user information when using pre-stablished sessions (2/2)

Description - Upon receipt of a SIP INFO request from the controlling MCPTT function within the dialog of the SIP INVITE request for an MCPTT emergency call or MCPTT imminent peril call, the participating MCPTT function:

1) shall generate a SIP re-INVITE request according to 3GPP TS 24.229 [4] to be sent within the SIP dialog of the pre-established session;

2) shall include in the SIP re-INVITE request an SDP offer based upon the previously negotiated SDP for the pre-established session;

Of course such behaviour would not apply here since the SIP INFO only conveys information to be shown at the caller and does not demand any change in the SDP.

Furthermore the Warning header in the 200 does not arrive at the caller.

Solution - Assume SIP INFO in the dialog of REFER originating the call and no 200 OK equivalent information.

FRMCS O6

© ETSI

Observation 27: [Editorial] Behaviour upon reaching the maximum number of simultaneous successful service authorisations while using third-party registration and publish differ

Description - Step 2a) in 7.3.2 in 3GPP TS 24.379 defines the behaviour does not specify the result:

2a) shall check if the number of maximum simultaneous authorizations supported for the MCPTT user as specified in the <max-simultaneous-authorizations> element of the <anyExt> element contained in the <OnNetwork> element of the MCPTT service configuration document (see the service configuration document in 3GPP TS 24.484 [50]) has been reached. If reached, the MCPTT server shall not continue with the rest of the steps in this subclause;

while Step 3a) in 7.3.3 (for PUBLISH does)

3a) shall check if the number of maximum simultaneous authorizations supported for the MCPTT user as specified in the <max-simultaneous-authorizations> element of the <anyExt> element contained in the <OnNetwork> element of the MCPTT service configuration document (see the service configuration document in 3GPP TS 24.484 [50]) has been reached. If reached, the MCPTT server shall send a SIP 486 (Busy Here) response towards the MCPTT client with the warning text set to: "164 maximum number of service authorizations reached" in a Warning header field as specified in subclause 4.4, and shall not continue with the rest of the steps in this subclause;

Solution - Editorial

FRMCS O7

© ETSI

Observation 28: Clarification of the fa-fencing (similar to geofencing) feature (i.e. affiliation/de-affiliation to a group upon FA (de)activation

Description - Subclause 8.3.2.7 in 3GPP TS 24 484 states that the affiliation rules need to be evaluated upon a change in the activated/deactivated status of a specific FA to trigger the (de)affiliation but it's not clear in which combination the de-activation triggers the de-affiliation (as the feature would typically look like)

Solution - NA

FRMCS O8

© ETSI

Observation 29: Format of the m= line in the SDP for IPCONN's INVITE

Description - From TS 24.282, Subclause 20.1.1:

"depending on the service operator policy, the client shall add a zero port number value to the media descriptions of the SDP offer, in order to inform network entities that media resources are not requested for the session , or add a specific port number value to reserve the necessary media resources to be used in the data exchange" and "MCData client shall include an SDP offer/answer according to subclause 6.1.2 of 3GPP TS 24.229"

Unlike other sections in TS 24.282 there is no explicit reference to the content of the m= line and the role of the port and network resources considering that later GRE tunnels will be used to convey Application data back/forward through MCData nodes and not any transport protocol.

From TS 24.379, subclause 16.2.1.3:

in the application/vnd.3gpp.mcptt-regroup+xml MIME body is contained in the incoming SIP MESSAGE request:

a) if a <users-for-regroup> element is included in that MIME body, shall store the value of the <mcptt-regroup-uri> element as the temporary group identity and associate that with the group identity received in the <mcptt-regroup-uri> element, along with the information that the created regroup is a user regroup and should store the contents of the <users-for-regroup> element as the list of users that are part of that user regroup: or

But in the terminating participating that information seems to be removed according to subclause 16.3.2.4 Step 3e:

e) shall copy the contents of the application/vnd.3gpp.mcptt-regroup+xml MIME body received in the incoming SIP MESSAGE request into an application/vnd.3gpp.mcptt-regroup+xml MIME body included in the outgoing SIP MESSAGE request, with the exceptions that any <users-for-regroup> elements shall not be copied;

Solution – Clarification needed

FRMCS O9

© ETSI

Observation 30: Content of mcptt-regroup+xml and behaviour of the terminating clients when receiving a notification of creation of a regroup

Description - From TS 24.379, Section 16.2.1.3:

in the application/vnd.3gpp.mcptt-regroup+xml MIME body is contained in the incoming SIP MESSAGE request:

a) if a <users-for-regroup> element is included in that MIME body, shall store the value of the <mcptt-regroup-uri> element as the temporary group identity and associate that with the group identity received in the <mcptt-regroup-uri> element, along with the information that the created regroup is a user regroup and should store the contents of the <users-for-regroup> element as the list of users that are part of that user regroup: or

But in the terminating participating that information seems to be removed according to Section 16.3.2.4 Step 3e:

e) shall copy the contents of the application/vnd.3gpp.mcptt-regroup+xml MIME body received in the incoming SIP MESSAGE request into an application/vnd.3gpp.mcptt-regroup+xml MIME body included in the outgoing SIP MESSAGE request, with the exceptions that any <users-for-regroup> elements shall not be copied;

Solution – Clarification needed

FRMCS O10

© ETSI

Observation 31: Clarification on pidf+xml body for FA deactivation (1/5) + affiliation

Description - In clause 9A.2.1.2 in 3GPP TS 24379 is reported

4) if the MCPTT client requests to activate one or more functional aliases, shall set the Expires header field according to IETF RFC 3903</nowiki> [37], to 4294967295

5) if the MCPTT client requests to deactivate one or more functional aliases, shall set the Expires header field according to IETF RFC 3903</nowiki> [37], to zero

6) shall include an application/pidf+xml MIME body indicating per-user functional alias information according to subclause 9A.3.1. In the MIME body, the MCPTT client:

shall include all functional aliases where the MCPTT user <u>requests activation for the MCPTT ID</u>

This is ambiguous because in a deactivation user do not request activations so it is not clear what has to be indicated in deactivation requests.

In Plugtests, for affiliation “absolute interest” has been used so that the whole list of affliated list was typically published. Currently for FA two interpretations have been shown:

in deactivation FA to be deactivated have to be listed as in activation (as indicated in TS 103564 7.13.2)

In activation FA to be activated have to be listed, while in deactivation the listed FA are maintained and the active FA not indicated are deactivated.

#

FRMCS O11

© ETSI

Observation 31: Clarification on pidf+xml body for FA deactivation (2/5)

So, the same request

PUBLISH sip:mcptt-orig-part-server-psi@example.com</nowiki>

Expires: 0

multipart: MCPTT-INFO:...<mcptt-info>

<mcptt-Params>:...<mcptt-request-uri Type="Normal"><mcpttURI>sip:mcptt_id_clientA@example.com</nowiki></mcpttURI></mcptt-request-uri>

...</mcptt-Params>

</mcptt-info>...| PIDF: ...<presence entity="sip:mcptt_id_clientA@example.com</nowiki>"><mcpttPIFA10:p-id-fa>UNIQUEFAID</mcpttPIFA10:p-id-fa><tuple id="urn:uuid:00000000-0000-1000-8000-AABBCCDDEEFF</nowiki>">

<status>

<mcpttPIFA10:functionalAlias functionalAliasID="FA_A1"/>

<mcpttPIFA10:functionalAlias functionalAliasID="FA_A2"/>

</status>

</tuple></presence>

can lead both to

deactivate FA_A1 and FA_A2

deactivate all FA '''BUT''' FA_A1 and FA_A2

Proposal - Clarify the right interpretation

© ETSI

Observation 31b: Clarification on pidf+xml body for FA deactivation (3/5) REVISION OF AFFILIATION

In subclause 9.2.1.2 in 3GPP TS 24.379 in order:
- to indicate that an MCPTT user is interested in one or more MCPTT group(s) at an MCPTT client;
- to indicate that the MCPTT user is no longer interested in one or more MCPTT group(s) at the MCPTT client;
- to refresh indication of an MCPTT user interest in one or more MCPTT group(s) at an MCPTT client due to near expiration of the expiration time of an MCPTT group with the affiliation status set to the "affiliated" state received in a SIP NOTIFY request in subclause 9.2.1.3;
- to send an affiliation status change request in mandatory mode to another MCPTT user;

.

In the SIP PUBLISH request, the MCPTT client:

.

1) shall set the Request-URI to the public service identity identifying the originating participating MCPTT function serving the MCPTT user;
2) shall include an application/vnd.3gpp.mcptt-info+xml MIME body. In the application/vnd.3gpp.mcptt-info+xml MIME body, the MCPTT client shall include the <mcptt-request-uri> element set to the MCPTT ID of the MCPTT user;
3) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcptt" (coded as specified in 3GPP TS 24.229 [4]), in a P-Preferred-Service header field according to IETF RFC 6050 [9];
4) if the targeted MCPTT user is interested in at least one MCPTT group at the targeted MCPTT client, shall set the Expires header field according to IETF RFC 3903 [37], to 4294967295;
NOTE 2: 4294967295, which is equal to 232-1, is the highest value defined for Expires header field in IETF RFC 3261 [24].
5) if the targeted MCPTT user is no longer interested in any MCPTT group at the targeted MCPTT client, shall set the Expires header field according to IETF RFC 3903 [37], to zero; and
6) shall include an application/pidf+xml MIME body indicating per-user affiliation information according to subclause 9.3.1. In the MIME body, the MCPTT client:
a) shall include all MCPTT groups where the targeted MCPTT user indicates its interest at the targeted MCPTT client;

© ETSI

Observation 31b: Clarification on pidf+xml body for FA deactivation (4/5) REVISION OF AFFILIATION

...

We see the following points unclear:
Step 4 is covering "Interest" meaning affiliation
Step 5 covers "no longer interested" meaning deaffiliation
Step 6 (a) only talks about interest (seems to not cover "no longer interested")?
" change request in mandatory mode to another MCPTT user" Shows up only once in the spec and is not explained. It seems it's related to step 2, but not clear?.
If step 6 would be interpreted to also include "no longer interested" and refresh, the proposed solution could look like:
Rephrase step 6 a) to be clear that it covers besides "Interested" also the cases "no longer interested" and refresh. And clarify how to treat the other groups the user is already affiliated (not included in the list in step 6 a).

© ETSI

Observation 31b: Clarification on pidf+xml body for FA deactivation (5/5)

For functional alias in clause 9A.2.1.2 Functional alias status change procedure we have additional comments to observation 11

In order:
- to indicate that an MCPTT user requests to activate one or more functional aliases;
- to indicate that the MCPTT user requests to deactivate one or more functional aliases;
- to refresh indication of an MCPTT user interest in one or more functional aliases due to near expiration of the expiration time of a functional alias with the status set to the "activated" state received in a SIP NOTIFY request in subclause 9A.2.1.3;

...

In the SIP PUBLISH request, the MCPTT client:
...
4) if the MCPTT client requests to activate one or more functional aliases, shall set the Expires header field according to IETF RFC 3903 [37], to 4294967295;
NOTE 2: 4294967295, which is equal to 232-1, is the highest value defined for Expires header field in IETF RFC 3261 [24].
5) if the MCPTT client requests to deactivate one or more functional aliases, shall set the Expires header field according to IETF RFC 3903 [37], to zero; and
NOTE 3: Activation and deactivation of functional alias cannot be performed with the same PUBLISH request.
6) shall include an application/pidf+xml MIME body indicating per-user functional alias information according to subclause 9A.3.1. In the MIME body, the MCPTT client:
a) shall include all functional aliases where the MCPTT user requests activation for the MCPTT ID;

Step 4 is covering activation
Step 5 covers deactivation
Step 6 (a) only talks about activation (seems to not cover deactivation)?
If step 6 would be interpreted to also include deactivation and refresh, the proposed solution:
Possible proposal: rephrase step 6 a) to be clear that it covers besides activation also the cases deactivation and refresh. And clarify how to treat the other functional aliases already activated (not includes in the list in step 6 a).

© ETSI