**3GPP TSG-SA WG6 Meeting #39-e S6-201374**

**e-meeting, 31st August – 8th September 2020 (revision of S6-xxxxxx)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | **0270** | **rev** | **1** | **Current version:** |  |  |
|  | | | | | | | | |
| *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 |  | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Clarification of MCX Administrator | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | FirstNet | | | | | | | | | |
| ***Source to TSG:*** | S6 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | enh3MCPTT | | | | |  | ***Date:*** | | | 2020-09-04 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **D** |  | | | | | ***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-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | SA6 agreed to investigate issues from the last ETSI plugtest in S6-191525. One issue asked for clarification of how an MCPTT Administrator is identified. The issue is reproduced below:  PT2)10.1.1 MCPTT Administrator designation and checks  Not only on TS 24.484, but on other MCPTT related standards, the "MCPTT Administrator" is mentioned several times. In no single document is specified how this special MCPTT User is identified or distinguished from other regular MCPTT users. For CMS in particular, it is important to clarify this point, as this is the only user that can provision/manage configuration documents in this server. The checking mechanism should be specified. It is suggested to check the MCPTT ID of the access token against a configured value in the CMS.  The role of the Administrator is defined in TS 22.280. However, in SA6 MC specifications the use of the term Administrator is varied and complicated.  Most of the time it is used as follows:  “The administrator/authorized user/dispatcher….”  There are other examples including a configuration table TS 23.280 where the administrator is used as an example of a participant type.  >> Participant type for the group (group membership information). The particpant type values are defined and configured by the Mission Critical Organisation (e.g.first responder, second responder, dispatcher, dispatch supervisor, MC service administrator).  It seems clear that an MC service administrator is just a user of an MC service client with special priviliges and that it should be identified by an MC service ID just like a dispatcher or other authorized user. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Add a statement clarifying the role of the MC service administrator and other authorized users. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | There will continue to be confusion on the role of the Administrator. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 8.1.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  |  | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  |  | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  |  | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

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

### 8.1.2 MC service user identity (MC service ID)

The MC service user identity is also known as the MC service ID. The MC service ID is a globally unique identifier within the MC service that represents the MC service user. The MC service ID identifies an MC service user. The MC service ID may also identify one or more MC service user profiles for the user at the application layer.

There are attributes associated with the MC service ID configured in the MC service that relate to the human user of the MC service. Typically this information identifies the MC service user, by name or role, may also identify a user's organization or agency, and may also identify MC service user's service subscription to one or more MC services. Such attributes associated with an MC service ID can be used by the MC service server to make authorization decisions about the MC service granted to the user. For example, if the MC service user is subscribed to MCPTT service, an attribute that identifies a user's role as an incident commander could automatically be used by the MCPTT service to grant the user additional administrative rights over the creation of groups, or access to privileged talk groups.

The MC service ID shall be a URI. The MC service ID uniquely identifies an MC service user in an MC system. The MC service ID indicates the MC system where the MC service ID is defined.

When required by the MC service provider, the MC service ID is hidden from the signalling control plane.

A default or temporary MC service ID may be used where a user is not yet associated with a device. When a user would like to use one or more MC services but has not been authenticated by the identity management server, a default or temporary MC service ID and a corresponding MC service user profile may be used.

For the purposes of this document, an MC service administrator, MC service dispatcher, or MC service authorized user is an MC service user that has been granted special privileges within the context of the client function being performed (e.g. MC service client, group management client, configuration management client, key management client). For example, the MC service ID of a group management client of a MC service administrator can be authorized within the group management server to create new groups and add members to groups (i.e. administrative function), but is not authorized to dynamically create group or user regroups (i.e. operational function). Alternatively, for example, the MC service ID of a dispatcher will typically be authorized to create group and user regroups, but is not authorized to create new groups or add/delete members to groups. The MC service authorization framework is defined in TS 33.180 [25].

\* \* \* End of First Change \* \* \* \*

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