**3GPP TSG-SA3 Meeting #106-e *S3-220291***

**e-meeting, 14 - 25 February 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.180** | **CR** | **0189** | **rev** | **1** | **Current version:** | **17.5.0** |  |
|  |
| *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 |  | Radio Access Network |  | Core Network |  |

|  |
| --- |
|  |
| ***Title:***  | Authorization between MCData message store and MCData Server |
|  |  |
| ***Source to WG:*** | Samsung |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | MCXSec2 |  | ***Date:*** | 2022-01-10 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***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 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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | TS 24.282 and TS 23.282 defines the communication between MCData server and MCData message store. During an active MCData communication, the participating function on the MCData server of a MCData user participant shall, if the configuration to store the MCData communication is enabled for and if requested by the MCData user, deposit messages and files exchanged in the conversation to the MCData user's storage area in the MCData message store. The following Editor’s Note is captured in TS 24.282:Editor's note: [eMCData2, CR 0168, C1-204022] The security mechanism for communication from the MCData server acting as an HTTP client and the Message store function acting as an HTTP server is FFS. |
|  |   |
| ***Summary of change:*** | It is proposed to have the authorized MCData server list configured at the MCData message store based on local policy and handling of such list is out of scope of TS 33.180. |
|  |  |
| ***Consequences if not approved:*** | Incomplete specification. |
|  |  |
| ***Clauses affected:*** | 8.6.0 |
|  |  |
|  | **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:*** |  |

***\*\*\*\*\*Start of change\*\*\*\*\****

## 8.6 MCData message store security

### 8.6.0 Functional model

The functional model for the MCData message store is shown in figure 8.6.0-1.



Figure 8.6.0-1: MCData message store functional model

In the functional model shown in figure 8.6.0-1, the reference points MCData-7 and MCData-8 provide direct communications with the MCData message store from the MCData UE message store client and the MCData server capabilities function, respectively. Reference point(s) MCData-cap-n provide MCData message store functionality between the MCData client capabilities function and the MCData message store via the MCData server capabilities function. Security for the MCData message store reference points are described in clause 8.6.1.

HTTP requests from the MCData message store client to the MCData message store shall include an appropriately scoped access token for MCData. If the access token cannot be validated by the MCData message store, the HTTP request shall be rejected. To validate access tokens, the MCData message store shall validate the signature of the access token. The method used to provision the MCData message store with the IdMS signature validation credentials is out of scope of this document.Based on the local policy, the MCData message store shall be configured with an authorized MCData server list for the MCData Client. The configured list shall contain allowed public service identities of MCData servers of the MC service provider for the MCData Client.

NOTE: Handling (creating and revocation) of the list is out of scope of this document and left to implementation.

HTTP requests from the MCData capabilities function client to the MCData server capabilities function shall include an appropriately scoped access token for MCData. If the access token cannot be validated by the MCData server, the HTTP request shall be rejected.

If required by the MC domain operator, data and information stored at the MCData message store related to the SDS, FS or DS services shall be stored protected. The mechanism used to protect the data and information while not actively in use is out of scope of this document.

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