**3GPP TSG-SA3 Meeting #108-e *S3-222271***

**e-meeting, 22 - 26 August 2022 *was S3-221741***

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.180** | **CR** | **0190** | **rev** | **1** | **Current version:** | **14.10.0** |  |
|  |
| *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 | **x** |

|  |
| --- |
|  |
| ***Title:***  | [33.180] R14 Incorrect reference |
|  |  |
| ***Source to WG:*** | Motorola Solutions, Inc |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | MCSec |  | ***Date:*** | 2022-08-22 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-14 |
|  | *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:*** | The Authorization Code flow reference in Figure 5.1.4.2-2 (first arrow) is carried over from R13 and incorrectly points to a non-existent clause. This leads to confusion and can cause identity management implementation issues. |
|  |  |
| ***Summary of change:*** | Correct the reference in figure 5.1.4.2-2 from “Authorization Code Flow (clause B.3.1.0-1)” to “Authorization Code Flow (Annex B.4)”. |
|  |  |
| ***Consequences if not approved:*** | Possible incompatible identity management implementations. |
|  |  |
| ***Clauses affected:*** | 5.1.4.2 |
|  |  |
|  | **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 1st CHANGE \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 5.1.4.2 Inter-domain identity management functional model

The inter-domain identity management functional model is shown in Figure 5.1.4.2-1.



Figure 5.1.4.2-1: Functional Model for Inter-Domain MC Identity Management

In figure 5.1.4.2-1, the IdMS located in the primary domain (MCX Domain A) is the home identity management server for the user. The partner IdMS is located in a second domain (MCX Domain B) and is home to the service where the primary user requires group authorization.

The CSC-1 reference point between the UE IdM client and the partner IdM server endpoints shall be a direct connection and shall be protected with HTTPS (TLS).

The primary IdMS certificate(s) used to validate the user credentials at the partner IdMS are provisioned into the partner IdMS using an out of band mechanism beyond the scope of this document.

As defined in clause 5.1.2 an access token is required for user service authorisation. The same principle applies for inter-domain user service authorisation, in that the user must present a valid access token issued from the partner IdMS in MCX Domain B for authorisation to any group services located in MCX Domain B.

The MCX UE, after performing user service authorisation within the primary domain, may determine that the user is a member of a group service that is located in a partner domain (as indicated in the user profile).

In order for the UE to obtain this MCX Domain B access token, the token exchange procedure with the primary IdM service (MCX Domain A) shall be used to obtain a security token that identifies the user to the partner IdM service. This security token shall be specific to the partner IdM service, signed by the primary IdM service per IETF RFC 7515 [35]. Upon validation of the security token, the partner IdM service shall provide an access token to the UE specifically scoped for that user. This access token shall provide the user with authorisation to the group service(s) in the partner domain (MCX Domain B).

Figure 5.1.4.2-2 shows the token exchange and authentication procedure.



Figure 5.1.4.2-2: Token exchange procedure

The token exchange profile for accessing the partner identity management service shall consist of [45] and [46] and shall be profiled as defined in Annex B.7.

NOTE: A specific and independent security token is required for each partner identity management domain.

Once the UE obtains the access token specific to the partner group service(s), the UE shall follow the user service authorisation procedure defined in clause 5.1.3 to access the group services within the partner domain.

The token exchange procedure shall be repeated for each partner identity management domain where the UE requires access and authorisation to group service(s) within that partner domain.

Annex C.2 shows the detailed flow for inter-domain MC user service authorization using the OAuth 2.0 token exchange procedure.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END of 1st CHANGE \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*