**3GPP TSG-SA3 Meeting #108-e *S3-222274***

**e-meeting, 22 - 26 August 2022 *revision of S3-221744***

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.180** | **CR** | **0193** | **rev** |  | **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:***  | [33.180] R17 Incorrect reference (mirror) |
|  |  |
| ***Source to WG:*** | Motorola Solutions, Inc |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | MCSec |  | ***Date:*** | 2022-08-22 |
|  |  |  |  |  |
| ***Category:*** | **A** |  | ***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:*** | 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 the first arrow of 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 Identity Management

In Figure 5.1.4.2-1, the IdMS located in the primary Identity Management Domain (MC Domain A) is the home identity management server for the user. The partner IdMS is located in a second Identity Management Domain (MC Domain B) and provides identity mangement services for the primary user when authorising to partner group services or when the MC user is attempting to migrate.

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 MC client must present a valid access token issued from the partner IdMS in MC Domain B for authorisation to services located in MC Domain B.

The inter-domain identity management procedure shall be triggered when an MC client, after performing user service authorisation within the primary Identity Management Domain, determines that the user is a member of a group service that is located in a partner IdMS domain (as indicated in the user profile).

Additionally, the inter-domain identity management procedure shall be triggered when a user attempts to migrate from their primary MC system to a partner MC system.

In order for the MC client to obtain the MC Domain B authorisation access token(s), the token exchange procedure with the primary IdM service (MC 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 and signed by the primary IdM service per IETF RFC 7515 [35]. Upon validation of the security token, the partner IdM service shall provide the access token(s) to the MC client specifically scoped for that user. The access token(s) shall provide the user with authorisation to the service(s) in the partner Identity Management Domain (MC Domain B) which may include services related to migration.

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 (steps 1-5 in Figure 5.1.4.2-2) 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.

Within a single MC System with interconnected MC domains, once the MC client obtains the access token specific to the partner group service(s) (step 5 in Figure 5.1.4.2-2), the MC client shall follow the user service authorisation procedure defined in clause 5.1.3 to access the group service(s) within the partner domain.

For migration of an MC user from their primary MC domain to a partner MC domain, once the MC client obtains the access token specific to the partner MC system (step 5 in Figure 5.1.4.2-2), the MC client shall follow the user service authorisation procedure defined in clause 5.1.5.

The token exchange procedure shall be repeated for each partner identity management domain where the MC client requires access and authorisation to group service(s) within that partner MC domain or when the user migrates from their primary MC system to a partner MC system.

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 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*