**3GPP TSG- Meeting #**

**, , - was S3-244906**

|  |
| --- |
| *CR-Form-v12.3* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** |  | **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:***  | [33.180] MCRec ID Introduction |
|  |  |
| ***Source to WG:*** |  |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** |  |  | ***Date:*** |  |
|  |  |  |  |  |
| ***Category:*** |  |  | ***Release:*** |  |
|  | *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-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19) Rel-20 (Release 20)* |
|  |  |
| ***Reason for change:*** | Introducing MCRec ID for the ID Token and Access Token according to SA6 specification. |
|  |  |
| ***Summary of change:*** |  Add MCRec ID to the ID token and access token  |
|  |  |
| ***Consequences if not approved:*** | The recording admin and replay feature is subject to fraud and exposure to unauthorized actors. |
|  |  |
| ***Clauses affected:*** | 5.1.2.1, B.2.1.3, B.2.2.3 |
|  |  |
|  | **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:*** |  |

\* \* \* \* Start of changes \* \* \* \*

\* \* \* \* First change \* \* \* \*

#### 5.1.2.1 Identity management functional model

The mission critical Identity Management functional model is shown in figure 5.1.2.1-1 and consists of the identity management server located in the MCX common services core and the identity management client located in the MCX UE. The IdM server and the IdM client in the MCX UE establish the foundation for MCX user authentication and user authorization.

Note that use of the term "IdM client" in this document is generically used to represent any identity management service endpoint within an MC UE that communicates with the IdM Server (authorization endpoint or token endpoint) over the CSC-1 reference point for MC identity management services. It does not imply any specific client implementation of the client-side identity management service.

The CSC-1 reference point, between the IdM client in the UE and the Identity Management server, provides the interface for user authentication. CSC-1 is a direct HTTP interface between the IdM client in the UE and the IdM server and shall support OpenID Connect 1.0 ([19], [20] and [21]).

The OpenID Connect profile for MCX shall be implemented as defined in annex B. MCX user authentication, MCX user service authorization, OpenID Connect 1.0, and the OpenID Connect profile for MCX shall form the basis of the identity management architecture.

In alignment with the OpenID Connect 1.0 [21] and OAuth 2.0 standards [19] and [20], CSC-1 shall consist of two identity management interfaces; the authorization endpoint and the token endpoint. These endpoints are separate and independent from each other, requiring separate and independent IP addressing. The authorization endpoint server and the token endpoint server may be collectively referred to as the IdM server in this document.

The HTTP connection between the Identity Management client and the Identity management server shall be protected using HTTPS.



Figure 5.1.2.1-1: Functional Model for MC Identity Management

To support MCX user authentication, the IdM server (IdMS) shall be provisioned with the user's MC ID and MC service IDs (the MC service ID may be the same as the MC ID). A mapping between the MC ID and MC service ID(s) shall be created and maintained in the IdMS. When an MCX user wishes to authenticate with the MCX system, the MC ID and credentials are provided via the UE IdM client to the IdMS (note that the primary authentication method used to obtain the MC ID and credentials is out of scope of the present document). The IdMS receives and verifies the MC ID and credentials, and if valid returns an ID token, refresh token, and access token to the UE IdM client specific to the credentials. The MCX client learns the user's MC service ID(s) from the ID token. Table 5.1.2.1-1 shows the MCX tokens and their usage.

Table 5.1.2.1-1: MC tokens

|  |  |  |
| --- | --- | --- |
| Token Type | Consumer of the Token | Description (See Annex B for details) |
| ID token | UE client(s) | Contains the MC service ID for at least one authorised service (MCPTT ID, MCVideo ID, MCData ID, MCRec ID). Also may contain other info related to the user that is useful to the client. |
| Access token | KMS, MCPTT server, etc. (Resource Server) | Short-lived token (definable in the IdMS) that conveys the user's identity. This token contains the MC service ID for at least one authorised service (MCPTT ID, MCVideo ID, MCData ID, MCRec ID). |
| Refresh token | IdM server (Authorization Server) | Allows UE to obtain a new access token without forcing user to log in again. |
| Security token | Partner IdM server (Authorisation server) | Short-lived token (definable in the IdMS) that conveys the user's identity to an Identity management server in a partner MC domain. User access to services within the partner domain are based on the validation of this token. |

\* \* \* \* Second change \* \* \* \*

### B.2.1.3 MCX claims

The MCX Connect profile extends the OpenID Connect standard claims with the additional claims shown in table B.2.1.3-1.

Table B.2.1.3-1: ID token MCX claims

|  |  |
| --- | --- |
| Parameter | Description |
| mcptt\_id | REQUIRED for MCPTT. The MCPTT ID of the current MCPTT user of the MCPTT client. |
| mcvideo\_id | REQUIRED for MCVideo. The MCVideo ID of the current MCVideo user of the MCVideo client. |
| mcdata\_id | REQUIRED for MCData. The MCData ID of the current MCData user of the MCData client. |
| mcrec\_id | REQUIRED for MC recording admin and replay services. The MCRec ID of the current recording administrator and/or replay user of the recording admin client and/or replay client. |

\* \* \* \* Third change \* \* \* \*

### B.2.2.3 MCX claims

The MCX Connect profile extends the standard claims defined in IETF RFC 7662 [33] with the additional claims shown in table B.2.2.3-1.

Table B.2.2.3-1: Access token MCX claims

|  |  |
| --- | --- |
| Parameter | Description |
| mcptt\_id | REQUIRED for MCPTT. The MCPTT ID of the current MCPTT user of the MCPTT client. |
| mcvideo\_id | REQUIRED for MCVideo. The MCVideo ID of the current MCVideo user of the MCVideo client. |
| mcdata\_id | REQUIRED for MCData. The MCData ID of the current MCData user of the MCData client. |
| mcrec\_id | REQUIRED for MC recording admin and replay services. The MCRec ID of the current recording administrator and/or replay user of the recording admin client and/or replay client. |

\* \* \* \* End of changes \* \* \* \*