**3GPP TSG-SA3 Meeting #108-e *S3-221750r1***

**e-meeting, 22 - 26 August 2022 *was S3-221750***

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** |  | **rev** | **1** | **Current version:** | **17.6.0** |  |
|  |
| *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] R18 MC client clarification |
|  |  |
| ***Source to WG:*** | Motorola Solutions, Inc |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | MCXSec3 |  | ***Date:*** | 2022-08-22 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-18 |
|  | *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:*** | MC UEs that are MC Gateway UEs, relays, or non-3GPP devices are implied but not clearly identified in 33.180. |
|  |  |
| ***Summary of change:*** | Add clarifying text for MC Gateway UEs, relays, and non-3GPP devices in 33.180. |
|  |  |
| ***Consequences if not approved:*** | MC security may not be implemented properly for MC Gateway UEs, relays, and non-3GPP devices. |
|  |  |
| ***Clauses affected:*** | 5.1.1, 5.1.2.1 |
|  |  |
|  | **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 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 5.1.1 General

In the context of this specification, a MCX UE is any device which can be used to consume MC services. The MCX UE utilizes a MCX client, IdM Client, and SIP Client to obtain various MC services. The term MCX UE is not limited to devices, which are directly attaching to the 3GPP radio access network, but also includes devices which use gateway UEs or relays, or any other mechanism to establish IP connectivity for the purposes of obtaining MCX services (i.e. Identity Management, Key Management, Voice, Data or Video).  This means that all aspects of MCX security applicable to MCX UEs also apply to all other MCX devices independent from whether they are directly connected to a 3GPP radio access network or using another mechanism for connectivity (like gateways or relays), and every MCX UE regardless of its connectivity method shall perform user authentication and authorisation prior to receiving MCX services.

The generic steps for MCX user authentication and authorisation is shown in figure 5.1.1-1.



Figure 5.1.1-1: MCX authentication and authorisation

At UE power-on, the MCX UE performs EPS UE authentication as specified in TS 33.401 [14] or 5GS UE authentication as specified in TS 33.501 [55], depending on the system. The MCX UE then performs the following steps to complete authentication of the user, authorisation of the user, MCX service registration, and identity binding between signalling layer identities and the MC service ID(s).

- A: MCX user authentication.

- B: SIP Registration and Authentication.

- C: MCX Service Authorization.

These procedures are described in more detail in subsequent clauses.

Steps A and B may be performed in either order or in parallel. For scenarios where this order has an impact on the identity bindings between signalling layer identities and the MC service ID(s), a re-registration (Step B) to the SIP Core may be performed to update the registered signalling layer identity.

If an MCX UE completes SIP registration in Step B prior to performing MCX user authentication in Step A and MCX user service authorization as part of Step C, the MCX UE shall be able to enter a 'limited service' state. In this limited state, where the MCX user is not yet authorized with the MCX service, the MCX UE shall be able to use limited MCX services (e.g. an anonymous MCX emergency communication). The MCX Server is informed of the registration of the MC UE with the SIP core though Step B-2.

Additionally, an HTTP-1 authentication mechanism is used.

NOTE: Mechanisms for confidentiality and integrity protection (not defined in this clause) may be combined only with certain authentication procedures.

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

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START of 2nd 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. All MC devices such as 3GPP MC UEs, non-3GPP MC UEs, MC Gateway UEs (or other relays), and 3GPP/non-3GPP MC devices connecting through an MC Gateway UE, shall perform identity management prior to accessing MC services.

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]).

For an MC Gateway UE (or other relay device), the CSC-1 reference point as defined in Figure 5.1.2.1-1 shall apply between the MC Gateway UE (or other relay device) and the IdMS. For an MC device (either 3GPP or non-3GPP) attempting to obtain services through an MC Gateway UE (or other relay), the CSC-1 reference point as defined in Figure 5.1.2.1-1 shall apply between the the 3GPP or non-3GPP MC UE, securely tunneling through the MC Gateway UE (or other relays) to the IdMS.

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). 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). |
| 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. |

In support of MCX user authorization, the access token(s) obtained during user authentication is used to gain MCX services for the user. MCX user service authorisation is defined in clause 5.1.3.

To support the MCX service identity functional model, the MC service ID(s) shall be:

- Provisioned into the IdM database and mapped to MC IDs.

- Provisioned into the KMS and mapped to identity associated keys.

- Provisioned into the MCX user database and mapped to a user profile; and

- Provisioned into the GMS(s) and mapped to Group IDs.

Further details of the user authorization architecture are found in clause 5.1.3.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END of 2nd CHANGE \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*