**3GPP TSG-SA3 Meeting #119 S3-245148**

Orlando, US, 11 -15 November 2024 revision of S3-24465

|  |
| --- |
| *CR-Form-v12.1* |
| **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] Additions to access token for recording authorization |
|  |  |
| ***Source to WG:*** | Motorola Solutions, Airbus |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | MCXSec4 |  | ***Date:*** | 2024-11-11 |
|  |  |  |  |  |
| ***Category:*** | B |  | ***Release:*** | Rel-19 |
|  | *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:*** | SA6 has added the Recording (a.k.a. Logging) feature. SA3 needs to update the access token to authorize recording actions. |
|  |  |
| ***Summary of change:*** | Add recording authorizations to the access token |
|  |  |
| ***Consequences if not approved:*** | Recording feature will be vulnerable to spoofing and exposure to unauthorized actors.  |
|  |  |
| ***Clauses affected:*** | 5.1.3.1, B.4.2.2 |
|  |  |
|  | **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 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 5.1.3.1 General

This clause expands on the MCX user service authorization step shown in figure 5.1.1-1 step C.

MCX User Service Authorization is the function that validates whether or not a MCX user has the authority to access certain MCX services. In order to gain access to MCX services, the MCX client in the UE presents an access token (acquired during user authentication as described in subclause 5.1.2) to each service of interest (i.e. Key Management, MCX server, Configuration Management, Group Management, etc.). If the access token is valid, then the user is granted the use of that service. Figure 5.1.3.1-1 shows the flow for user authorization which covers key management authorization, MCX user service authorization, configuration management authorization, and group management authorization.

NOTE: All HTTP traffic between the UE and HTTP proxy, and all HTTP traffic between the UE and KMS (if not going through the HTTP proxy) is protected using HTTPS.

For key management authorization, the KM client in the UE presents an access token to the KMS over HTTP. The access token shall be scoped for key management services as defined in annex B.4.2.2. The KMS validates the access token and if successful, provides one or more sets of user specific key material back to the UE KM client based on the MC service ID(s) present in the access token (MCPTT ID, MCVideo ID and/or MCData ID). User specific key material includes identity based key information for media and signalling protection. If an interworking key management record (InterKMRec) exists and is associated to the requesting MC service ID (see clause 11.2.3), the KMS shall also provide the InterKMRec. This key management authorisation may be repeated for each KM service the user is authorised to use (MCPTT, MCVideo, MCData). In order to secure the transfer of user specific key material from the KMS to the KM client when using the TrK and InK, the KM client includes the TrK-ID and the InK-ID in the key management authorization request.

For MCPTT user service authorization, the MCPTT client in the UE presents an access token to the MCPTT server over SIP. The access token shall be scoped for MCPTT services as defined in annex B.4.2.2. The MCPTT server validates the access token and if successful, authorizes the user for full MCPTT services and sends an acknowledgement back to the MCPTT client. The MCPTT server then maps and maintains the IMPU to MCPTT ID association. The MCPTT ID to IMPU association shall only be known to the application layer. The SIP message used to convey the access token from the MCPTT client to the MCPTT server may be either a SIP REGISTER or SIP PUBLISH message.

For MCVideo service authorization, the MCVideo client in the UE presents an access token to the MCVideo server over SIP. The access token shall be scoped for MCVideo services as defined in annex B.4.2.2. The MCVideo server validates the access token and if successful, authorizes the user for full MCVideo services and sends an acknowledgement back to the MCVideo client. The MCVideo server then maps and maintains the IMPU to MCVideo ID association. The MCVideo ID to IMPU association shall only be known to the application layer. The SIP message used to convey the access token from the MCVideo client to the MCVideo server may be either a SIP REGISTER or SIP PUBLISH message.

For MCData user service authorization, the MCData client in the UE presents an access token to the MCData server over SIP. The access token shall be scoped for MCData services as defined in annex B.4.2.2. The MCData server validates the access token and if successful, authorizes the user for full MCData services and sends an acknowledgement back to the MCData client. The MCData server then maps and maintains the IMPU to MCData ID association. The MCData ID to IMPU association shall only be known to the application layer. The SIP message used to convey the access token from the MCData client to the MCData server may be either a SIP REGISTER or SIP PUBLISH message.

For recording user (recording administrator or replay user) service authorization, the recording admin client or the replay client in the UE presents an access token to the recording server. The access token shall be scoped for recording services (recording admin or replay, respectively) as defined in annex B.4.2.2. The recording server validates the access token and if successful, authorizes the user for recording services and sends an acknowledgement back to the recording admin client or the replay client. A recording administrator may set and modify target users and target groups for recording. A replay user is authorized to retrieve and replay saved recordings.

The UE can now perform configuration management authorization and download the user profile for the service(s) (MCPTT, MCVideo, MCData). Following the flow described in subclause 10.1.4.3 of 3GPP TS 23.280 [36] "MC service user obtains the MC service user profile(s) from the network", the Configuration Management (CM) client in the UE sends an access token in the user profile query to the Configuration Management server over HTTP. The access token shall be scoped for configuration management services as defined in annex B.4.2.2. The CM server receives the request and validates the access token, and if valid, the CM server uses the identity from the access token (MCPTT ID, MCVideo ID, MCData ID) to obtain the user profile from the MCX user database. The CM server then sends the user profile back to the CM client over HTTP. This configuration management authorisation may be repeated for each CM service the user is authorised to use (MCPTT, MCVideo, MCData).

Upon receiving each user profile, the Group Management (GM) client in the UE can now perform group management authorization. The GM client obtains the user's group membership information from the user profile, and following the flow shown in clause 10.1.5.2 of 3GPP TS 23.280 [36] "Retrieve group configurations at the group management client", the Group Management (GM) client in the UE sends an access token in the Get group configuration request to the host GM server of the group membership over HTTP. The access token shall be scoped for group management services as defined in annex B.4.2.2. The GM server validates the access token, and if valid, completes the flow. As part of group management authorization, group key information is provided as per subclause 5.7 of the present document. This group management authorisation may be repeated for each GM service the user is authorised to use (MCPTT, MCVideo, MCData).

For MC UEs that support mission critical location services, authorization is accomplished by including an access token in each location message (i.e. location information report, location reporting trigger, etc.) sent by the location management client to the location management server. The access token shall be scoped for location management services as defined in annex B.4.2.2. The location management server validates the access token and (if successful) processes the message (e.g. accepts and stores the location information report). If an access token cannot be validated, local policy may dictate an action to be taken within the location management server with regards to the received location message (e.g. the local policy may require storage of the location information report as an emergency provision).



Figure 5.1.3.1-1: MCX user service authorization

The user authorization procedure in Step C of Figure 5.1.1-1 is further detailed into 5 sub steps that comprise the MCX user service authorization process:

Step C-1a: If not already done, establish a secure HTTP tunnel using HTTPS between the MCX UE and MCX proxy server. Subsequent HTTP messaging makes use of this tunnel.

Step C-1b: When required by the MCX system, establish a secure HTTP tunnel using HTTPS between the MCX KM client and the KMS. When supported, subsequent HTTP messaging between the MCX KM client and the KMS makes use of this tunnel in lieu of the tunnel set up in Step C-1a.

Step C-2: The KM client in the MCX UE presents an access token to the KMS over HTTP. The KMS authorizes the user for key management services based upon the MC service ID(s) provided and replies to the client with identity specific key information. This step may be repeated to authorise the user with additional KM services (MCPTT, MCVideo, MCData) as necessary.

Step C-3: The MCX client in the UE presents an access token to the MCX server over SIP as defined in clause 5.1.3.2 of the present document. This step may be repeated to authorise the user with additional MCX services (MCPTT, MCVideo, MCData, MC Recording) as necessary.

Step C-4: The CM client in the UE follows the "MCX user obtains the user profile (UE initiated)" flow from clause 10.1.4.3 of 3GPP TS 23.280 [36], presenting an access token in the Get MCX user profile request over HTTP. If the token is valid, then the CM server authorizes the user for configuration management services. Completion of this step results in the CM server providing the user's profile to the CM client. This step may be repeated as necessary to obtain the user profile for additional services (MCPTT, MCVideo, or MCData).

Step C-5: The GM client in the UE follows the "Retrieve group configurations at the group management client" flow as shown in clause 10.1.5.2 of 3GPP TS 23.280 [36], presenting an access token in the Get group configuration request over HTTP. If the token is valid, the GMS authorizes the user for group management services. Completion of this step results in the GMS sending the user's group policy information and group key information to the GM client. This step may be repeated to authorise the user for additional group services (MCPTT, MCVideo, MCData) as necessary.

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

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START of 2nd CHANGE \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### B.4.2.2 Authentication request

As described in OpenID Connect 1.0, the IdM client constructs a request URI by adding the following parameters to the query component of the authorization endpoint's URI using the "application/x-www-form-urlencoded" format, redirecting the user's web browser to the authorization endpoint of the IdM server. The standard parameters shown in table B.4.2.2-1 are required by the MCX Connect profile. Other parameters defined by the OpenID Connect specification are optional.

Table B.4.2.2-1: Authentication Request standard required parameters

|  |  |
| --- | --- |
| Parameter | Values |
| response\_type | REQUIRED. For native clients the value shall be set to "code". |
| client\_id | REQUIRED. The identifier of the client making the API request. It shall match the value that was previously registered with the IdM server of the MCX service provider. |
| scope | REQUIRED. Scope values are expressed as a list of space-delimited, case-sensitive strings which indicate which MCX resource servers the client is requesting access to (e.g. MCPTT, MCVideo, MCData, KMS, etc.). If authorized, the requested scope values will be bound to the access token returned to the client.The scope value "openid" is defined by the OpenID Connect standard and is mandatory, to indicate that the request is an OpenID Connect request, and that an ID token should be returned to the client.This profile further defines the following additional authorization scopes: - *"*3gpp:mc:ptt\_service*"* - *"*3gpp:mc:video\_service*"* - *"*3gpp:mc:data\_service*"* *- "*3gpp:mc:ptt\_key\_management\_service*"* *- "*3gpp:mc:video\_key\_management\_service*"* *- "*3gpp:mc:data\_key\_management\_service*"* *- "*3gpp:mc:ptt\_config\_management\_service*"* *- "*3gpp:mc:video\_config\_management\_service*"* *- "*3gpp:mc:data\_config\_management\_service*"* *- "*3gpp:mc:ptt\_group\_management\_service*"* *- "*3gpp:mc:video\_group\_management\_service*"* *- "*3gpp:mc:data\_group\_management\_service*"* *- "*3gpp:mc:location\_management\_service*"* *- "*3gpp:mc:recording\_admin\_service*"* *- "*3gpp:mc:recording\_replay\_service*"*Others may be added in the future as new MCX resource servers are introduced by 3GPP (see note). |
| redirect\_uri | REQUIRED. The URI of the client to which the IdM server will redirect the authentication response in order to return the authorization code. The URI shall match the redirect URI registered with the IdM server during the client registration phase. |
| state | REQUIRED. An opaque value used by the client to maintain state between the authentication request and authentication response. The IdM server includes this value in its authentication response. |
| acr\_values | REQUIRED. Space-separated string that specifies the acr values that the IdM server is being requested to use for processing this authentication request, with the values appearing in order of preference. For minimum interoperability requirements, a password-based ACR value is mandatory to support. "3gpp:acr:password" as per the OpenID Connect 1.0 specification [21]. |
| code\_challenge | REQUIRED. The base64url-encoded SHA-256 challenge derived from the code verifier, to be verified against later. |
| code\_challenge\_method | REQUIRED. The hash method used to transform the code verifier to produce the code challenge. This profile current requires the usage of "S256" |
| NOTE: The order in which they are expressed does not matter. |

An example of an authentication request for MCX Connect might look like:

EXAMPLE:

GET/as/authorization.oauth2?response\_type=code&client\_id=idm\_client&scope=openid

3gpp:mc:ptt\_service&redirect\_uri=[http://3gpp.mcptt/cb&state=abc123&acr\_values=3gpp:acr:password&code\_challenge=0x123456789abcdef&code\_challenge\_method=S256](http://3gpp.mcptt/cb%26state%3Dabc123%26acr_values%3D3gpp%3Aacr%3Apassword%26code_challenge%3D0x123456789abcdef%26code_challenge_method%3DS256)

HTTP/1.1
Host: IdMS.server.com:9031
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded

Upon receiving the authentication request from the client, the IdM server performs user authentication. Note that user authentication should be completely opaque to the MC services on the client.

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