**3GPP TSG-CT WG1 Meeting #141eC1-23xxxx**

**Online 17– 21 April 2023**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  | **24.482** | **CR** | **0017** | **rev** | **1** | **Current version:** | **17.1.0** |  |
|  |
| *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 | **x** | Radio Access Network |  | Core Network |  |

|  |
| --- |
|  |
| ***Title:***  | Token endpoint of the partner system IdM server obtained from MCS user profile configuration document |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | eMCSMI\_IRail |  | ***Date:*** | 2023-04-19 |
|  |  |  |  |  |
| ***Category:*** | **C** |  | ***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-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19)* |
|  |  |
| ***Reason for change:*** | As can be seen from the following text in TS 23.280 and the CT1 agreement in C1-231033, *The MC service user and MC service UE first follow the MC service UE configuration and MC service user authorization steps described in subclause 10.1.1.1 to obtain one or more MC service user profiles from the primary MC system. Each user profile received from the primary MC system contains a list of partner MC systems to which migration is permitted using that user profile, together with the access information needed to communicate with the application plane servers of the partner MC system. See Annex A.3 for more information. The MC service user also obtains the necessary security parameters needed to authenticate and become service authorized on the partner MC system; the process for this is specified in 3GPP TS 33.180 [25].  At this point, the MC UE is configured sufficiently for the partner system so that the MC service user is capable of utilizing "limited services" as described in 3GPP TS 33.180 [25].**NOTE 1:  The above steps which enable migration to take place may be carried out some time in advance of migration. The MC service user could repeatedly obtain migrated MC service, e.g. on successive days while located in the area of the partner MC system, without needing to obtain the initial configuration afresh in advance of each period of migrated MC service. The user profile from the primary MC system must be retained to provide the access information to permit this.*The configuration information for migration is not preconfigured, i.e., it is signalled from the primary MC system to the UE.However, TS 24.482 specifies that the token endpoint of the partner system IdM server is specified in the MC service user profile MO. |
|  |  |
| ***Summary of change:*** | The token endpoint of the partner system IdM server is obtained from an MCS user profile configuration document. |
|  |  |
| ***Consequences if not approved:*** | The token endpoint of the partner system IdM server cannot be found and hence migration failure. |
|  |  |
| ***Clauses affected:*** | 2, 6.2.3 |
|  |  |
|  | **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:*** |  |

\* \* \* First Change \* \* \*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] Void.

[3] 3GPP TS 22.179: "Mission Critical Push To Talk (MCPTT) over LTE".

[4] Void.

[5] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".

[6] "OpenID Connect Core 1.0 incorporating errata set 1".

[7] W3C.REC-html401-19991224: "HTML 4.01 Specification".

[8] 3GPP TS 23.379: "Functional architecture and information flows to support mission critical communication services".

[9] Void.

[10] IETF RFC 2818: "HTTP Over TLS".

[11] 3GPP TS 24.483: "Mission Critical Services (MCS) Management Object (MO)".

[12] 3GPP TS 24.379: "Mission Critical Push To Talk (MCPTT) call control Protocol specification".

[13] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[14] IETF RFC 6750: "The OAuth 2.0 Authorization Framework: Bearer Token Usage".

[15] 3GPP TS 24.109: "Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details".

[16] 3GPP TS 23.280: "Common functional architecture to support mission critical services; Stage 2".

[17] 3GPP TS 33.180: "Security of the Mission Critical Service".

[18] IETF RFC 8693: "OAuth 2.0 Token Exchange".

 [19] IETF RFC 7523: "JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants".

[20] IETF RFC 7159: "The JavaScript Object Notation (JSON) Data Interchange Format".

[21] 3GPP TS 24.281: "Mission Critical Video (MCVideo) signalling control; Protocol specification".

[22] 3GPP TS 23.282: "Mission Critical Data (MCData) signalling control; Protocol specification".

[23] IETF RFC 7230: "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing".

[24] IETF RFC 7231: "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content".

[25] 3GPP TS 24.484: "Mission Critical Services (MCS) configuration management; Protocol specification".

\* \* \* Next Change \* \* \*

### 6.2.3 Token request to a partner system IdM server

Upon an indication from the MC service client to acquire an access token from a partner IdM server to authorise the MC service user to access the resources of a partner system, the IdM client:

1) shall obtain a valid security token appropriate for inclusion in a Token Request message to be sent to the targeted partner IdM server by the procedures specified in subclause 6.2.2 if the IdM client has not already done so; and

2) shall generate a Token Request message as specified in the OpenID Connect 1.0 [6] and IETF RFC 6749 [5] with the following clarifications:

a) If the IdM client is attempting to acquire an access token from a partner IdM server not for the purpose of migration, the IdM client shall establish a TLS tunnel to the configured URL of the token endpoint of the partner system IdM server as specified in the MC service user profile MO with the following clarifications:

i) for MCPTT, use the token endpoint defined in the "/<x>/<x>/OnNetwork/GroupServerInfo/IDMSTokenEndpointList/<x>/Entry/IDMSTokenID" leaf node as defined in the MCPTT service user profile MO 3GPP TS 24.483 [11];

ii) for MCData, use the token endpoint defined in the "/<x>/<x>/OnNetwork/MCDataGroupList/<x>/Entry/IdMSTokenEndPointList/<x>/IdMSTokenEndPoint" leaf node as defined in the MCData service user profile MO 3GPP TS 24.483 [11]; and

iii) for MCVideo, use the token endpoint defined in the "/<x>/<x>/OnNetwork/MCVideoGroupList/<x>/Entry/IdMSTokenEndPointList/<x>/IdMSTokenEndPoint" leaf node as defined in the MCVideo service user profile MO 3GPP TS 24.483 [11].

NOTE 1: The specific IDM token endpoint can be found by finding the server information for a particular MC service group.

NOTE 2: The specific IDM token endpoint can also be found in the respective MC service user profile document (see 3GPP TS 24.483 [11]) in the parameters corresponding to those identified in steps i), ii) and iii) above.

 If the IdM client is attempting to acquire an access token from a partner IdM server for the purpose of migration, the IdM client shall establish a TLS tunnel to the configured URL of the token endpoint of the partner system IdM server as specified in the MC service user profile configuration document with the following clarifications:

i) for MCPTT, use the token endpoint defined in the <idms-token-endpoint> element in the <App-Server-Info> element in the <on-network> element in the <mcptt-UE- initial-configuration> in the <AccessInformationForPartnerMCPTTSystem> element in the <MigratablePartnerMCPTTSystemInfo> element in the <anyExt> element in the <OnNetwork> element in the <mcptt-user-profile> document as defined in 3GPP TS 24.484 [25];

ii) for MCData, use the token endpoint defined in the <idms-token-endpoint> element in the <App-Server-Info> element in the <on-network> element in the <mcptt-UE- initial-configuration> in the <AccessInformationForPartnerMCDataSystem> element in the <MigratablePartnerMCDataSystemInfo> element in the <anyExt> element in the <OnNetwork> element in the <mcdata-user-profile> document as defined in 3GPP TS 24.484 [25]; and

iii) for MCVideo, use the token endpoint defined in the <idms-token-endpoint> element in the <App-Server-Info> element in the <on-network> element in the <mcptt-UE- initial-configuration> in the <AccessInformationForPartnerMCVideoSystem> element in the <MigratablePartnerMCVideoSystemInfo> element in the <anyExt> element in the <OnNetwork> element in the <mcvideo-user-profile> document as defined in 3GPP TS 24.484 [25].

b) The IdM client shall generate an HTTP POST request method according to IETF RFC 7231 [24] including in the entity body the following parameters using the "application/x-www-form-urlencoded" format as specified in W3C.REC-html401-19991224 [7]:

i) the grant\_type parameter set to value of "urn:ietf:params:oauth:grant-type:jwt-bearer" as specified in subclause B.7.4 of 3GPP TS 33.180 [17] and IETF RFC [19]; and

ii) all other required parameters specified in subclause B.7.4 of 3GPP TS 33.180 [17]; and

c) The IdM client shall send the HTTP POST request method towards the token endpoint of the partner system IdM server.

\* \* \* End of Change(s) \* \* \*