**3GPP TSG-CT WG1 Meeting #124-eC1-203294**

**Electronic meeting, 2-10 June 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.282** | **CR** | **0168** | **rev** | **-** | **Current version:** | **16.3.0** |  |
|  | | | | | | | | |
| *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 | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Resolving EN for identifying user between MCData Server and MCData message store | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | AT&T | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eMCData2 | | | | |  | ***Date:*** | | | 2020-05-24 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***Release:*** | | | Rel-16 |
|  | *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 can be 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-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | Editor's note: How the user is identified in communication between the MCData Server and MCData message store function (MCData-8) is FFS | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | * Removed the editor’s note. * Added a Note as to how MCData ID is used to identify the user over the interafce between MCData Server and MCData message store function. * Added further clarification for the usage of the procedures specified in clause 21 by both interfaces   + MCData message store client and MCData message store function and   + MCData Server and MCData message store function) | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | TS 24.282 spec will not be as clear/complete as it needs to be. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 21.1, 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 as well as C1-203645 both introduce a new “Note 3”. Please ensure one of the Note 3 is renumbered to become Note 4 when both CRs are incorporated into the spec. | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | | * 24.482 nore 33.180 spec cover NE-to-NE authorization aspect (this was not realized in the original CR). * Hence had to adjust the CR accordingly by referring to the based Authorization framework OAuth 2.0 RFC 6749 (which 33.180 is based on) for the bare minimum specification in TS 24.282 unti an LS to SA3 is sent and a resolution by SA3 is provided (note: once SA3 provides a resolution to identified underspecifed issue then, subclause 21.1 would require update to refer to SA3 specification accordingly) * Moved Note 1 to the top of the subclause for better information flow in light of the newly added statements in this revisied CR. * Added the reference to RFC 6749 in subclause 2 | | | | | | | | |

\* \* \* \* \* \* \* FIRST CHANGE \* \* \* \* \* \* \*

## 21.1 General

This clause defines procedures for communication between MCData message store client and MCData message store function as well as MCData server and MCData message store function as specified in subclause 7.13.1 of 3GPP TS 23.282[2]. The communication between the MCData message store client and MCData message store function shall use HTTP over TLS as specified in annex A of 3GPP TS 24.482 [24].

The MCData message store function shall act as an HTTP server as defined in annex A of 3GPP TS 24.482 [24].

The MCData message store client in the role of an HTTP client shall include the MCData access token (with the “Bearer” authentication scheme) in the Authorization header field of an HTTP request as specified in 3GPP TS 24.482 [24].

NOTE 1: In procedures for communication between MCData message store client and MCData message store function, the MCData ID which is the identity of the MCData user is part of MCData access token as specified in 3GPP TS 24.482 [24].

The MCData server in the role of an HTTP client shall use the OAuth 2.0 framework to obtain an access token (i.e. MCData access token) following the Client Credentials Grant type as specified in RFC 6749 [x]. The scope of the access token shall enable the MCData server to have access to the entire MCData message store accounts. MCData server shall include the access token (with the “Bearer” authentication scheme) in the Authorization header field of an HTTP request as specified in RFC 6749 [x].

NOTE 2: In procedures for communication between MCData server and MCData message store function, since the access token obtained by the MCData server is not associated with any single user account, the MCData ID which is the identity of the MCData user is not part of the access token. As a result, the identity of the MCData user is provided as the value of the resource URL variable, "boxId" as specified in subclause 5.2 of OMA-TS-REST\_NetAPI\_NMS-V1\_0-20190528-C [66].

Editor's note: Whether Mission Critical security framework specs (24.482 & 33.180) are futher specified to include Network Element to Network Element authorization using OAuth 2.0 “client credential” grant type is FFS

The HTTP server (i.e. MCData message store) shall validate the MCData access token as specified in 3GPP TS 24.482 [24].

The interface between MCData message store client and MCData message store function (i.e. MCData-7) as well as the interface between MCData server and MCData message store function (i.e. MCData-8) shall be based on the RESTful API as specified in OMA-TS-REST\_NetAPI\_NMS-V1\_0-20190528-C [66].

NOTE 3: Procedures defined for communication between the MCData message store client and MCData message store function as well as MCData server and MCData message store function in the following sections reference subclause 6 “Detailed specification of the resources” of OMA-TS-REST\_NetAPI\_NMS-V1\_0-20190528-C [66]. Additional information related to RESTful resources, data types and sequence diagrams are found in subclause 5 and JSON examples in appendix D of OMA-TS-REST\_NetAPI\_NMS-V1\_0-20190528-C [66].

\* \* \* \* \* \* \* NEXT 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] 3GPP TS 23.282: "Functional architecture and information flows to support Mission Critical Data (MCData); Stage 2";

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

[4] IETF RFC 3261 (June 2002): "SIP: Session Initiation Protocol".

[5] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[6] IETF RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messaging".

[7] IETF RFC 6050 (November 2010): "A Session Initiation Protocol (SIP) Extension for the Identification of Services".

[8] IETF RFC 3841 (August 2004): "Caller Preferences for the Session Initiation Protocol (SIP)".

[9] IETF RFC 4826 (May 2007): "Extensible Markup Language (XML) Formats for Representing Resource Lists".

[10] 3GPP TS 24.379: "Mission Critical Push To Talk (MCPTT) call control Protocol specification".

[11] 3GPP TS 24.481: "Mission Critical Services (MCS) group management Protocol specification".

[12] 3GPP TS 24.484: "Mission Critical Services (MCS) configuration management Protocol specification".

[13] IETF RFC 4483 (May 2006): "A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages.

[14] IETF RFC 4122 (July 2005): "A Universally Unique IDentifier (UUID) URN Namespace".

[15] 3GPP TS 24.582: "Mission Critical Data (MCData) media plane control Protocol specification";

[16] IETF RFC 3840 (August 2004): "Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)".

[17] IETF RFC 4975 (September 2007): "The Message Session Relay Protocol (MSRP)".

[18] IETF RFC 5366 (October 2008): "Conference Establishment Using Request-Contained Lists in the Session Initiation Protocol (SIP)".

[19] IETF RFC 6135 (February 2011): "An Alternative Connection Model for the Message Session Relay Protocol (MSRP) ".

[20] IETF RFC 6714 (August 2012): "Connection Establishment for Media Anchoring (CEMA) for the Message Session Relay Protocol (MSRP)".

[21] IETF RFC 6086 (January 2011): "Session Initiation Protocol (SIP) INFO Method and Package Framework".

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

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

[24] 3GPP TS 24.482: "Mission Critical Services (MCS) identity management Protocol specification.

[25] 3GPP TS 24.334: "Proximity-services (ProSe) User Equipment (UE) to Proximity-services (ProSe) Function Protocol aspects; Stage 3".

[26] 3GPP TS 33.180: "Security of the Mission Critical Service".

[27] IETF RFC 3856 (August 2004): "A Presence Event Package for the Session Initiation Protocol (SIP)".

[28] W3C: "XML Encryption Syntax and Processing Version 1.1", <https://www.w3.org/TR/xmlenc-core1/>.

[29] W3C: "XML Signature Syntax and Processing (Second Edition)", <http://www.w3.org/TR/xmldsig-core/>.

[30] IETF RFC 4648 (October 2006): "The Base16, Base32, and Base64 Data Encodings".

[31] 3GPP TS 23.003: "Numbering, addressing and identification".

[32] IETF RFC 2045 (November 1996): "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies".

[33] IETF RFC 2392 (August 1998): "Content-ID and Message-ID Uniform Resource Locators".

[34] IETF RFC 3903 (October 2004): "Session Initiation Protocol (SIP) Extension for Event State Publication".

[35] IETF RFC 4354 (January 2006): "A Session Initiation Protocol (SIP) Event Package and Data Format for Various Settings in Support for the Push-to-Talk over Cellular (PoC) Service".

[36] IETF RFC 6665 (July 2012): "SIP-Specific Event Notification".

[37] 3GPP TS 29.283: "Diameter Data Management Applications".

[38] IETF RFC 4028 (April 2005): "Session Timers in the Session Initiation Protocol (SIP)".

[39] IETF RFC 3856 (August 2004): "A Presence Event Package for the Session Initiation Protocol (SIP)".

[40] IETF RFC 3863 (August 2004): "Presence Information Data Format (PIDF)".

[41] IETF RFC 4661 (September 2006): "An Extensible Markup Language (XML)-Based Format for Event Notification Filtering".

[42] 3GPP TS 24.483: "Mission Critical Services (MCS) Management Object (MO)".

[43] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[44] IETF RFC 5627 (October 2009): "Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP)".

[45] IETF RFC 4567 (July 2006): "Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP)".

[46] IETF RFC 3986 (January 2005): "Uniform Resource Identifier (URI): Generic Syntax".

[47] 3GPP TS 23.032: "Universal Geographical Area Description (GAD)".

[48] 3GPP TS 29.582: "Mission Critical Data (MCData) signalling control interworking with LMR systems; Protocol specification".

[49] 3GPP TS 29.214: "Policy and Charging Control over Rx reference point".

[50] IETF RFC 5245 (April 2010): "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer Answer Protocols".

[51] IETF RFC 3515 (April 2003): "The Session Initiation Protocol (SIP) Refer Method".

[52] IETF RFC 7647 (September 2015): "Clarifications for the use of REFER with RFC6665".

[53] IETF RFC 4488 (May 2006): "Suppression of Session Initiation Protocol (SIP) REFER Method Implicit Subscription".

[54] IETF RFC 4538 (June 2006): "Request Authorization through Dialog Identification in the Session Initiation Protocol (SIP)".

[55] IETF RFC 6509 (February 2012): "MIKEY-SAKKE: Sakai-Kasahara Key Encryption in Multimedia Internet KEYing (MIKEY)".

[56] 3GPP TS 23.468: "Group Communication System Enablers for LTE (GCSE\_LTE); Stage 2".

[57] 3GPP TS 29.468: "Group Communication System Enablers for LTE (GCSE\_LTE); MB2 reference point; Stage 3".

[58] Void.

[59] IETF RFC 5761 (April 2010): "Multiplexing RTP Data and Control Packets on a Single Port".

[60] IETF RFC 5795 (March 2010): "The RObust Header Compression (ROHC) Framework".

[61] IETF RFC 3095 (July 2001): "RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed".

[62] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3".

[63] 3GPP TS 23.203: "Policy and charging control architecture".

[64] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)".

[65] 3GPP TS 29.199-09: "Open Service Access (OSA); Parlay X web services; Part 9: Terminal location".

[66] OMA-TS-REST\_NetAPI\_NMS-V1\_0-20190528-C: "RESTful Network API for Network Message Storage".

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

\* \* \* \* \* \* \* END CHANGES \* \* \* \* \* \* \*