**3GPP TSG-SA3 Meeting #123 draft\_S3-253002-r1**

Goteborg, Sweden, 25 - 29 August 2025

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | **0223** | **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:*** | Clarification about security for MC over IOPS | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | MCXSec4 | | | | |  | ***Date:*** | | | 2025-08-18 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | B |  | | | | | ***Release:*** | | | Rel-20 |
|  | *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-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | SA3 agreed to reuse MC mechanisms in TS 33.180 to address MC user authentication in the case of MC services in the IOPS mode of operation. The clarifications in this paper includes:   * update the reference, definition and abbreviation clauses of TS 33.180 to reflect the above agreement. * Due to the fact that different identifiers are used in IOPS mode, the TS 33.180 needs clarification to reflect the above agreement. * As per TS 23.180, only the MCPTT and MCData are supported when using IOPS mode, thus the token claims when using IOPS mode needs to be clarified. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Update definition and abbreviation of TS 33.180 to cover the MC over IOPS mode. Add clarification to TS 33.180 to add the identifiers used in IOPS mode. Add clarification to TS 33.180 to restrict the token claim in IOPS mode only includes the mcptt\_id and mcdata\_id. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Not clear how IOPS mode is supported by the existing MCX mechanisms. Claims may misalign with the supported MC services in IOPS mode. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 2, 3.1, 3.2, 5.1.1, Annex X (new), B.2.1.3, B.2.2.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\* \* \* \* 1st 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 23.379: "Functional architecture and information flows to support Mission Critical Push To Talk (MCPTT); Stage 2".

[3] 3GPP TS 22.179: "Mission Critical Push To Talk (MCPTT); Stage 1".

[4] 3GPP TS 33.210: ''3G security; Network Domain Security (NDS); IP network layer security''.

[5] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[6] 3GPP TS 33.203: "3G security; Access security for IP-based services".

[7] 3GPP TS 33.179 Release 13: "Security of Mission Critical Push To Talk (MCPTT) over LTE".

[8] 3GPP TS 33.328: ''IP Multimedia Subsystem (IMS) media plane security''.

[9] IETF RFC 6507: ''Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption (ECCSI)''.

[10] IETF RFC 6508: ''Sakai-Kasahara Key Encryption (SAKKE)''.

[11] IETF RFC 6509: ''MIKEY-SAKKE: Sakai-Kasahara Key Encryption in Multimedia Internet KEYing (MIKEY)''.

[12] IETF RFC 3550: ''RTP: A Transport Protocol for Real-Time Applications''.

[13] IETF RFC 3711: "The Secure Real-time Transport Protocol (SRTP)".

[14] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".

[15] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[16] 3GPP TS 33.222: "Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)".

[17] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[18] NIST FIPS 180-4: "Secure Hash Standard (SHS)".

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

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

[21] OpenID Connect 1.0: "OpenID Connect Core 1.0 incorporating errata set 1", <http://openid.net/specs/openid-connect-core-1_0.html>.

[22] IETF RFC 3830: "MIKEY: Multimedia Internet KEYing".

[23] IETF RFC 3602: "The AES-CBC Cipher Algorithm and Its Use with IPsec".

[24] IETF RFC 4771: "Integrity Transform Carrying Roll-Over Counter for the Secure Real-time Transport Protocol (SRTP)".

[25] IETF RFC 6043: "MIKEY-TICKET: Ticket-Based Modes of Key Distribution in Multimedia Internet KEYing (MIKEY)".

[26] IETF RFC 7714: ''AES-GCM Authenticated Encryption in the Secure Real-time Transport Protocol (SRTP)''.

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

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

[29] IETF RFC 5905: "Network Time Protocol Version 4: Protocol and Algorithms Specification".

[30] IETF RFC 5480: "Elliptic Curve Cryptography Subject Public Key Information".

[31] IETF RFC 6090: "Fundamental Elliptic Curve Cryptography Algorithms".

[32] IETF RFC 7519: "JSON Web Token (JWT)".

[33] IETF RFC 7662: "OAuth 2.0 Token Introspection".

[34] IETF RFC 3394: "Advanced Encryption Standard (AES) Key Wrap Algorithm".

[35] IETF RFC 7515: "JSON Web Signature (JWS)".

[36] 3GPP TS 23.280: "Common functional architecture to support mission critical services; Stage 2".

[37] 3GPP TS 23.281: "Functional architecture and information flows for mission critical video; Stage 2".

[38] 3GPP TS 23.282: "Functional model and information flows for Mission Critical Data".

[39] 3GPP TS 23.002: "Network Architecture".

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

[41] IETF RFC 2392: "Content-ID and Message-ID Uniform Resource Locators".

[42] NIST Special Publication 800-38D: "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC".

[43] IETF RFC 5116: "An Interface and Algorithms for Authenticated Encryption".

[45] IETF RFC 7521: "Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants".

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

[47] 3GPP TS 22.280: " Mission Critical Services Common Requirements; Stage 1".

[48] 3GPP TS 23.283: " Mission Critical Communication Interworking with Land Mobile Radio Systems; Stage 2".

[49] 3GPP TS 24.379: "Mission Critical Push To Talk (MCPTT) call control; Protocol specification."

[50] 3GPP TS 24.282: "Mission Critical Data (MCData) signalling control; Protocol specification. "

[51] IETF RFC 3711 Errata ID 3712, <https://www.rfc-editor.org/errata/eid3712>.

[52] IANA: "Multimedia Internet KEYing (MIKEY) Payload Name Spaces", <https://www.iana.org/assignments/mikey-payloads/mikey-payloads.xhtml>.

[53] IETF RFC 7636: "Proof Key for Code Exchange by OAuth public clients".

[54] 3GPP TS 23.289: "Mission Critical services over 5G System; Stage 2".

[55] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[X] 3GPP TS 23.180: " Mission critical services support in the Isolated Operation for Public Safety (IOPS) mode of operation, Stage 2".

\* \* \* \* 2nd change \* \* \* \*

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**Authorised Identity**: An application identity given to an authorised user or network entity (e.g. MC Service ID) containing authorisation information.

**External KMS:** The KMS which is the root of trust for a specific External Security Domain.

**External Security Domain**: A security domain that the user is not a member of, but with which the user may communicate.

**Floor:** Floor(x) is the largest integer smaller than or equal to x.

**Home KMS:** The KMS that is the root of trust of the Home Security Domain.

**Home Security Domain**: The MCX user's primary security domain.

**Identity Management Domain**: The MC clients and MC functions that share an Identity Management Server (IdMS). To be specific, the MC clients request access tokens from the same primary IdMS, and the MC functions accept access tokens from this IdMS.

**IOPS mode of operation:** As described in 3GPP TS 23.180 [X].

**KMS Certificate:** A certificate containing the security parameters for a security domain. This is required to support identity-based cryptography and differs from X.509 certificates used for traditional PKI. See Annex D.3.1 for details.

**KMS URI:** A unique identifier for a security domain, or equivalently, a logical KMS.

**MCX**: Mission critical services where “MCX” may be substituted with the term “MCPTT”, “MCVideo”, “MCData”, or any combination thereof.

**Migration KMS:** The KMS that is the root of trust of a specific Migration Security Domain.

**Migration Security Domain**: A security domain that a user is a (temporary) member of, and may be keyed to use, but is not the user's Home security domain.

**Partner domain**: A secondary MC domain which may support MC services for MC users who are home to a different MC domain. See also External Security Domain.

**Primary domain**: The “home” MC domain where MC users receive their primary identity management and MC services. See also Home Security Domain.

**Privileged signalling**: Signalling which is performed by an authorised user and allows the authorised userto cause an intrusive action on a target client without the target user’s permission.

**Security Domain**: A security domain is a group of MCX users who share common security requirements and policies for their communications. From a technical perspective, users within a security domain share a KMS and KMS certificate. MCX users may be members of one or more security domains.

\* \* \* \* 3rd change \* \* \* \*

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

CMS Configuration Management Server

CS Crypto Session

CSB-ID Crypto Session Bundle Identifier

CSC Common Services Core

CSK Client-Server Key

CSK-ID Client-Server Key Identifier

DPCK MCData Payload Cipher Key

DPPK MCData Payload Protection Key

DPPK-ID MCData Payload Protection Key Identifier

GBA Generic Bootstrapping Architecture

GMK Group Master Key

GMK-ID Group Master Key Identifier

GMS Group Management Server

GUK-ID Group User Key Identifier

IdM Identity Management

IdMS Identity Management Server

InK Integrity Key

InK-ID Integrity Key Identifier

InterKMRec Interworking Key Management Record

InterKMRec-ID Interworking Key Management Record Identifier

InterSD Interworking Security Data

IOPS Isolated Operation for Public Safety

IWF InterWorking Function

JSON JavaScript Object Notation

JWS JSON Web Signature

JWT JSON Web Token

KDF Key Derivation Function

KFC Key For Control Signalling

KFC-ID Key for Floor Control Identifier

KMS Key Management Server

MBCP Media Burst Control Protocol

MCData Mission Critical Data

MCPTT Mission Critical Push to Talk

MCVideo Mission Critical Video

MCX Mission Critical Services

MKFC Multicast Key for Floor Control

MSCCK MBMS subchannel control key

MSRP Message Session Relay Protocol

MuSiK Multicast Signalling Key

MKI Master Key Identifier

NTP Network Time Protocol

NTP-UTC Network Time Protocol – Coordinated Universal Time

OIDC OpenID Connect

PCK Private Call Key

PCK-ID Private Call Key Identifier

PKCE Proof Key for Code Exchange

PSK Pre-Shared Key

SEG Security Gateway

SeGy Security Gateway

SPK Signalling Protection Key

SRTCP Secure Real-Time Transport Control Protocol

SRTP Secure Real-Time Transport Protocol

SSRC Synchronization Source

TBCP Talk Burst Control Protocol

TGK Traffic Generating Key

TrK KMS Transport Key

TrK-ID KMS Transport Key Identifier

UID User Identifier for MIKEY-SAKKE (referred to as the 'Identifier' in RFC 6509 [11])

XPK XML Protection Key

\* \* \* \* 4th change \* \* \* \*

### Annex X (Normative)

### Security aspects of MC over Isolated Operation for Public Safety (IOPS)

NOTE 1: The network layer connection supporting security aspects of MC over IOPS is applicable to the LTE network.

### X.1 User authentication and authorisation

In case of the MC services in the IOPS mode of operation, both user authentication and user service authorisation are required before a client to use an IOPS service (e.g. Configuration Management, Key Management, Group Management, MCPTT services, and MCData services [X]).

The user authentication mechanisms as specified in clause 5.1.2 of present document are reused to get the access token, with the following modificiation:

* The MC ID is replaced with IOPS MC ID
* The MC service ID is replaced with IOPS MC service ID, i.e. IOPS MCPTT ID and IOPS MCData ID.

The user service authorisation mechanisms as specified in clause 5.1.3 of present document are reused to get the access token, by replacing MC service ID with IOPS MC service ID, i.e. IOPS MCPTT ID and IOPS MCData ID.

### X.2 Key management

Key Management is required as part of the MC over IOPS and the mechanism in clause 5.2 applies. The detailed key management procedurs for specifc scenarios of the MC over IOPS are list as follows:

* user key management reuses mechanism in clause 5.3.
* Key management from MC client to MC server reuses mechanism in clause 5.4, the MC server can be either IOPS MC connectivity function or signalling application server.
* Key management for private communication follows the procedures in clauses 5.6 and 7.2.
* Key management for Group communication follows the procedures in clauses 5.7.
* For specific services (i.e. MCPTT and MC Data in 23.180), clauses 7 and 8 are reused.

The storage and persistence requirements in clause 5.11 of present document needs to be followed in case of the MC services in the IOPS mode of operation.

### X.3 Private communications

The MCPTT and MC Data private call security for the for MC over IOPS scenario reuses the mechanisms as specificed in clause 5.6, 7.2 and 8.3 of present document.

### X.4 Group communications

The MCPTT and MC Data group call security for the for MC over IOPS scenario reuses the mechanisms as specificed in clause 5.7, 7.3 and 8.4 of present document. Only pre-configured group(s) applies.

\* \* \* \* 5th 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. |

NOTE: Only the mcptt\_id and mcdata\_id (i.e. IOPS MCPTT ID and IOPS MCData ID) can be included when using the IOPS mode of operation, as specified in TS 23.180 [X].

\* \* \* \* 6th 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. |

NOTE: Only the mcptt\_id and mcdata\_id (i.e. IOPS MCPTT ID and IOPS MCData ID) can be included when using the IOPS mode of operation, as specified in TS 23.180 [X].

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