**3GPP TSG-CT WG4 Meeting #110-eC4-223329**

**E-Meeting, 12th – 20th May 2022 Revision of C4-223167**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **29.571** | **CR** | **0342** | **rev** | **4** | **Current version:** | **17.5.0** |  |
|  |
| *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:***  | MBS Security Context (MSK/MTK) Definitions |
|  |  |
| ***Source to WG:*** | Samsung |
| ***Source to TSG:*** | C4 |
|  |  |
| ***Work item code:*** | 5MBS |  | ***Date:*** | 2022-05-17 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** | Rel-17 |
|  | *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:*** |  This CR adds support of MBS Security Context (MSK/MTK).CT4 CR# C4-222328 was agreed in CT4# 109-e. This revision further adds following changes on top of that CR:MSK Lifetime is introduced in MbsKeyInfo so as to allow MBSF provide this information to MBSTF. Also, MSK is made conditional as it need not be present in MSK\_Request from MBSTF to MBSF. |
|  |  |
| ***Summary of change:*** | * Addition of data-types for MBS Security Context
* Addition of MSK Lifetime in MbsKeyInfo
* Made MSK Conditional in MbsKeyInfo
 |
|  |  |
| ***Consequences if not approved:*** | MBS Traffic cannot be decrypted by the UE. |
|  |  |
| ***Clauses affected:*** | 2, 5.9.4.X, 5.9.4.Y, A.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:*** | The CR adds backward compatible new feature to CommonData.yaml API file. |
|  |  |
| ***This CR's revision history:*** | Rev1: Removed changes to MbsSession IE, changed MSK/MTK to type BytesRev2: Support for disabling security protectionRev3: Updated MbsKeyInfo to include MSK Lifetime. Made MSK conditional.Rev4: Removed support for disabling security protection |

\* \* \* \* 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] 3GPP TS 29.501: "5G System; Principles and Guidelines for Services Definition; Stage 3".

[3] OpenAPI: "OpenAPI Specification Version 3.0.0", <https://spec.openapis.org/oas/v3.0.0>.

[4] IETF RFC 1166: "Internet Numbers".

[5] IETF RFC 5952: "A recommendation for IPv6 address text representation".

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

[7] 3GPP TS 23.003: "Numbering, addressing and identification".

[8] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[9] IETF RFC 7807: "Problem Details for HTTP APIs".

[10] IETF RFC 3339: "Date and Time on the Internet: Timestamps".

[11] 3GPP TS 38.413: "NG-RAN; NG Application Protocol (NGAP) ".

[12] IETF RFC 6901: "JavaScript Object Notation (JSON) Pointer".

[13] 3GPP TS 24.007: "Mobile radio interface signalling layer 3; General aspects".

[14] IETF RFC 6902: "JavaScript Object Notation (JSON) Patch".

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

[16] 3GPP TS 36.413: "Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP)".

[17] IETF RFC 7042: "IANA Considerations and IETF Protocol and Documentation Usage for IEEE 802 Parameters".

[18] IETF RFC 6733: "Diameter Base Protocol".

[19] 3GPP TS 32.422: "Telecommunication management; Subscriber and equipment trace; Trace control and configuration management".

[20] 3GPP TS 24.501: "Non-Access-Stratum (NAS) Protocol for 5G System (5GS); Stage 3".

[21] 3GPP TS 29.002: "Mobile Application Part (MAP) specification".

[22] Void.

[23] 3GPP TS 23.032: "Universal Geographical Area Description (GAD)".

[24] ITU-T Recommendation Q.763 (1999): "Specifications of Signalling System No.7; Formats and codes".

[25] 3GPP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".

[26] 3GPP TS 23.015: "Technical Realization of Operator Determined Barring".

[27] 3GPP TR 21.900: "Technical Specification Group working methods".

[28] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[29] 3GPP TS 29.510: "5G System; Network Function Repository Services; Stage 3".

[30] 3GPP TS 23.316: "Wireless and wireline convergence access support for the 5G System (5GS)".

[31] IEEE Std 802.11-2012: "IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

[32] CableLabs WR-TR-5WWC-ARCH: "5G Wireless Wireline Converged Core Architecture".

[33] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access; Stage 2".

[34] BBF TR-069: "CPE WAN Management Protocol".

[35] BBF TR-369: "User Services Platform (USP)".

[36] 3GPP TS 23.287: "Architecture enhancements for 5G System (5GS) to support Vehicle-to-Everything (V2X) services".

[37] BBF TR-470: "5G Wireless Wireline Convergence Architecture".

[38] IEEE "Guidelines for Use of Extended Unique Identifier (EUI), Organizationally Unique Identifier (OUI), and Company ID (CID)", <https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/tutorials/eui.pdf>

[39] 3GPP TS 36.331: "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification".

[40] IETF RFC 5580: "Carrying Location Objects in RADIUS and Diameter".

[41] BBF TR-456: "".

[42] 3GPP TS 38.331: "NR; Radio Resource Control (RRC); Protocol specification".

[43] 3GPP TS 29.572: "5G System; Location Management Services; Stage 3".

[x] 3GPP TS 33.246: "Security of Multimedia Broadcast/Multicast Service (MBMS)".

[y] 3GPP TS 33.501: "Security architecture and procedures for 5G system; Stage 2".

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

5.9.4.X Type: MbsSecurityContext

**Table 5.9.4.X-1: Definition of type MbsSecurityContext**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description |
| keyList | map(MbsKeyInfo) | M | 1..N | One or more MSK/MTK(s) and associated IDs. The key of the map shall be a (unique) valid JSON string per clause 7 of IETF RFC 8259 [22], with a maximum of 32 characters |

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

5.9.4.Y Type: MbsKeyInfo

**Table 5.9.4.Y-1: Definition of type MbsSecurityContext**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description |
| keyDomainId | Bytes | M | 1 | Key Domain ID = MCC || MNC as defined in 3GPP TS 33.246 [x].It shall be encoded as a string with format "byte" as defined in OpenAPI Specification [3], i.e. base64-encoded characters, representing the Key Domain ID (encoded in 3 bytes). |
| mskID | Bytes | M | 1 | MSK ID as defined in 3GPP TS 33.246 [x]. It shall be encoded as a string with format "byte" as defined in OpenAPI Specification [3], i.e. base64-encoded characters, representing the MSK ID (encoded in 4 bytes). |
| msk | Bytes | C | 0..1 | MSK as defined in 3GPP TS 33.246 [x]. The IE shall not be present when MBSTF requests updated MSK from MBSF after, e.g. lifetime expiry. Shall be present otherwise.When present, it shall be encoded as a string with format "byte" as defined in OpenAPI Specification [3], i.e. base64-encoded characters, representing the MSK (encoded in 16 bytes). |
| mskLifetime | DateTime | O | 0..1 | MSK Lifetime as defined in 3GPP TS 33.501 [y]. |
| mtkID | Bytes | C | 0..1 | MTK ID as defined in 3GPP TS 33.246 [x]. Shall be present if available. It shall be encoded as a string with format "byte" as defined in OpenAPI Specification [3], i.e. base64-encoded characters, representing the MTK ID (encoded in 2 bytes). |
| mtk | Bytes | C | 0..1 | MTK as defined in 3GPP TS 33.246 [x]. Shall be present if available. It shall be encoded as a string with format "byte" as defined in OpenAPI Specification [3], i.e. base64-encoded characters, representing the MTK (encoded in 16 bytes). |

Editor's Note: Encoding of the keyDomainId for an SNPN is FFS.

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

A.2 Data related to Common Data Types

openapi: 3.0.0

info:

 version: '1.3.0-alpha.5'

 title: 'Common Data Types'

 description: |

 Common Data Types for Service Based Interfaces.

 © 2022, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).

 All rights reserved.

externalDocs:

 description: 3GPP TS 29.571 Common Data Types for Service Based Interfaces, version 17.5.0

 url: 'https://www.3gpp.org/ftp/Specs/archive/29\_series/29.571/'

paths: {}

components:

 schemas:

…

…

[Skipped for clarity]

 MbsSecurityContext:

 description: A map (list of key-value pairs) where a (unique) valid JSON string serves as key of MbsSecurityContext

 type: object

 additionalProperties:

 $ref: '#/components/schemas/MbsKeyInfo'

 minProperties: 1

 MbsKeyInfo:

 description: MBS Security Key Data Structure

 type: object

 properties:

 keyDomainId:

 $ref: '#/components/schemas/Bytes'

 mskId:

 $ref: '#/components/schemas/Bytes'

 msk:

 $ref: '#/components/schemas/Bytes'

 mskLifetime:

 $ref: '#/components/schemas/DateTime'

 mtkId:

 $ref: '#/components/schemas/Bytes'

 mtk:

 $ref: '#/components/schemas/Bytes'

 required:

 - keyDomainId

 - mskId

…

…

[Skipped for clarity]

\* \* \* \* End of Changes \* \* \* \*