**3GPP TSG-SA3 Meeting #105-e *draft\_S3-214422-r2***

**e-meeting, 08 – 19 November 2021 Revision of S3-214009**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | **draft-CR** | **rev** | **-** | **Current version:** | **<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 | **x** | Radio Access Network |  | Core Network | **x** |

|  |
| --- |
|  |
| ***Title:***  | Living CR for 5MBS |
|  |  |
| ***Source to WG:*** | Huawei, HiSilicon |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | 5MBS |  | ***Date:*** |  2021-10-19 |
|  |  |  |  |  |
| ***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:*** | It’s the living CR with the Security aspects for the MBS.  |
|  |  |
| ***Summary of change:*** | The contribution adds skeleton and security aspects related to the MBSF/MBSTF and the interface. Security mechanisms for MBS traffic transmission are added as well. |
|  |  |
| ***Consequences if not approved:*** | Security aspects are absent for MBS. |
|  |  |
| ***Clauses affected:*** | New Annex clause |
|  |  |
|  | **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\*\*\*\*\*\*\*

# 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*.

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

[yy] 3GPP TS 23.247: “Architectural enhancements for 5G multicast-broadcast services".

[zz] 3GPP TS 33.535: “Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

\*\*\*\*\*\*\*\*\*\*\*\* END OF 1st CHANGE\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\* START OF 2nd 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].

5GC 5G Core Network

5G-AN 5G Access Network

5G-RG 5G Residential Gateway

NG-RAN 5G Radio Access Network

5G AV 5G Authentication Vector

5G HE AV 5G Home Environment Authentication Vector

5G SE AV 5G Serving Environment Authentication Vector

ABBAAnti-Bidding down Between Architectures

AEAD Authenticated Encryption with Associated Data

AES Advanced Encryption Standard

AKA Authentication and Key Agreement

AMF Access and Mobility Management Function

AMF Authentication Management Field

NOTE: If necessary, the full word is spelled out to disambiguate the abbreviation.

ARPF Authentication credential Repository and Processing Function

AUSF Authentication Server Function

AUTN AUthentication TokeN

AV Authentication Vector

AV' transformed Authentication Vector

BAP Backhaul Adaptation Protocol

BH Backhaul

CCA Client Credentials Assertion

Cell-ID Cell Identity as used in TS 38.331 [22]

CHO Conditional Handover

CIoT Cellular Internet of Things

cIPX consumer's IPX

CKSRVCC Cipher Key for Single Radio Voice Continuity

CP Control Plane

cSEPP consumer's SEPP

CTR Counter (mode)

CU Central Unit

DN Data Network

DNN Data Network Name

DU Distributed Unit

EAP Extensible Authentication Protocol

EDT Early Data Transmission

EMSK Extended Master Session Key

ENSI External Network Slice Inforamtion

EPS Evolved Packet System

FN-RG Fixed Network RG

gNB NR Node B

GUTI Globally Unique Temporary UE Identity

HRES Hash RESponse

HXRES Hash eXpected RESponse

IAB Integrated Access and Backhaul

IKE Internet Key Exchange

IKSRVCC Integrity Key for Single Radio Voice Continuity

IPUPS Inter-PLMN UP Security

IPX IP exchange service

KSI Key Set Identifier

KSISRVCC Key Set Identifier for Single Radio Voice Continuity

LI Lawful Intercept

MBSF Multicast/Broadcast Service Function

MBSTF Multicast/Broadcast Service Transport Function

MN Master Node

MO-EDT Mobile Originated Early Data Transmission

MT-EDT Mobile Terminated Early Data Transmission

MR-DC Multi-Radio Dual Connectivity

MSK Master Session Key

N3IWF Non-3GPP access InterWorking Function

NAI Network Access Identifier

NAS Non Access Stratum

NDS Network Domain Security

NEA Encryption Algorithm for 5G

NF Network Function

NG Next Generation

ng-eNB Next Generation Evolved Node-B

ngKSI Key Set Identifier in 5G

N5CW Non-5G-Capable over WLAN

N5GC Non-5G-Capable

NIA Integrity Algorithm for 5G

NR New Radio

NR-DC NR-NR Dual Connectivity

NSSAI Network Slice Selection Assistance Information

NSSAA Network Slice Specific Authentication and Authorization

PDN Packet Data Network

PEI Permanent Equipment Identifier

pIPX producer's IPX

PRINS PRotocol for N32 INterconnect Security

pSEPP producer's SEPP

PUR Preconfigured Uplink Resource

QoS Quality of Service

RES RESponse

SCG Secondary Cell Group

SEAF SEcurity Anchor Function

SCP Service Communication Proxy

NOTE: Void. Security Gateway

SEPP Security Edge Protection Proxy

SIDF Subscription Identifier De-concealing Function

SMC Security Mode Command

SMF Session Management Function

SN Secondary Node

SN Id Serving Network Identifier

SUCI Subscription Concealed Identifier

SUPI Subscription Permanent Identifier

TLS Transport Layer Security

TNAN Trusted Non-3GPP Access Network

TNAP Trusted Non-3GPP Access Point

TNGF Trusted Non-3GPP Gateway Function

TWAP Trusted WLAN Access Point

TWIF Trusted WLAN Interworking Function

TSC Time Sensitive Communication

UE User Equipment

UEA UMTS Encryption Algorithm

UDM Unified Data Management

UDR Unified Data Repository

UIA UMTS Integrity Algorithm

ULR Update Location Request

UP User Plane

UPF User Plane Function

URLLC Ultra Reliable Low Latency Communication

USIM Universal Subscriber Identity Module

XRES eXpected RESponse

\*\*\*\*\*\*\*\*\*\*\*\* END OF 2nd CHANGE\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\* START OF 3rd CHANGE\*\*\*\*\*\*

Annex X (normative): Security for Multicast/Broadcast Service for 3GPP service

X.1 General

Editor's Note: This clause will describe the general part on Multicast/Broadcast Service.

This clause describes the security requirements, procedures and handling for 5G Multicast/Broadcast Service (MBS).The general features for 5G MBS are described in TS 23.247 [yy].

NOTE: Security for Multicast-broadcast service for roaming is not supported in this release.

X.2 Security requirements

Editor's Note: This clause will describe security requirements and features of Multicast/Broadcast Service.

X.2.1 Requirements of MBSF

The security requirements on the NEF described in clause 5.9.2.3 of present specification also apply to MBSF.

X.2.2 Requirements of MBSTF

The security requirements on the NEF described in clause 5.9.2.3 of present specification also apply to MBSTF.

X.3 Security mechanisms for xMB-C/MB2-C and xMB-U/MB2-U interface

The security aspects defined in clause 12 in present specification is applicable for both MBSF and MBSTF. TLS based solution are reused to protect the interface xMB-C/MB2-C and xMB-U/MB2-U between AF and 5GC in MBS.

X.4 Security mechanisms for MBS traffic transmission

### X.4.1 Key derivation, management and distribution

#### X.4.1.1 Control-plane procedure

The multicast session security context consists of the MBS session ID, MBS keys and the corresponding key ID. The MBS keys include MBS Service Key (MSK) and MBS Traffic Key (MTK). MBS traffic is protected with the MTK. The MSK is used to protect the MTK when the MTK is delivered to the UE. The MSK ID and MTK ID are determined as specified in Clause 6.3.2.1 and clause 6.3.3.1 of TS 33.246 [xx].

The MBSF generates the MSK and its key ID for a MBS session and distributes the MSK to the MB-SMF and MBSTF. The MBSF shall distribute them to MB-SMF either upon request by the MB-SMF (i.e., pull) or when a new MSK is generated (i.e., push). The MBSF may also include the MSK lifetime when it distributes the MSK to MBSTF.

The MBSTF generates the MTK and its key ID for the MBS traffic protection. A new MTK may be generated based on the MBS session security policy. When the MBSTF generates a new MTK, the MBSTF shall multicast the MTK after protecting it using the MSK as specified in TS 33.246 [xx]. The MBSTF shall also provide the new MTK to the MBSF.

In the multicast session join and session establishment procedure, the SMF interacts with the MB-SMF to retrieve the multicast session security context. The SMF shall provide the multicast session security context to the UE if the UE is authorized to use the required multicast service. The UE uses the received MTK to process the protected MBS traffic until it receives a new MTK update over the user-plane.

The MSK may be updated based on the request from MB-SMF or AS (e.g., due to the change of authorization information) or based on the local policy (e.g., key lifetime expiration). When the MSK is updated, the MBSF shall send the new MSK to the MB-SMF and then the MB-SMF shall trigger the session update as specified in clause 7.2.6 in TS 23.247 [yy]. The MSK and the corresponding key ID are delivered to the UEs that has joined the multicast session. The MBSF shall also send the new MSK to the MBSTF. The MBSTF may request a MSK to the MBSF when it does not have a valid MSK (e.g., due to the current MSK expiration).

The MTK may be updated based on the change of the authorization information or based on the local policy (e.g. key lifetime expiration). In such cases, the MBSF or MB-SMF may trigger the MTK update to the MBSFT. The key update request message shall include the MBS session ID. If the MBSFT has generated a new MTK, the MBSFT shall provide the new MTK to the MBSF. To improve the efficiency of MTK update, the updated MTK is delivered from MBSTF to the UE using MIKEY over UDP as specified in clause 6.3.3.2 in TS 33.246 [xx]. The MSK is used to protect the updated MTK. The UE shall not send an error message to the MBSTF as a result of receiving an MTK message.

#### X.4.1.2 User-plane procedure

The UE registers to the MBS service and receives the MBS traffic as specified in TS 33.246 [xx] with the following changes.

* MBSTF takes the role of the BM-SC in TS 33.246 [xx].
* The UE authenticates to the MBSTF based on the GBA as in MBMS security (see TS 33.246 [xx]) or based on the AKMA (see TS 33.535 [zz]). When the AKMA is used, the MRK is derived from the KAF as specified in Annex F of TS 33.246 [xx] by replacing the Ks\_NAF for the GBA\_ME run with KAF. Furthermore, when the AKMA is used, the MUK is set to KAF.

Editor’s Note: When the AKMA is used, how the MBSTF obtains the authorization information is FFS.

### X.4.2 Protection of the traffic transmission

The actual method of protection may vary depending on the type of data being transmitted, e.g. media streaming application or file download. Clause 6.6.2 and clause 6.6.3 in TS 33.246 [xx] apply to the protection of streaming data and protection of download data, respectively.

### X.4.3 Authentication and authorization aspects for the multicast session

The support for the optional-to-use authentication and authorization procedure for a 5G multicast session is specified in this clause.

NOTE: Roaming is not supported for 5G MBS according to TS 23.247 [yy].

Editor's Note: secondary authentication procedure for multicast PDU session will be added if confirmed by SA WG2.

AKMA/GBA is supported for authentication and authorization in user-plane procedure for security protection of MBS traffic, as specified in clause X.4.1.2 of present document.

X.5 Security protection for interworking between 5MBS and eMBMS

Interworking between 5G MBS and eMBMS is supported at service layer. The procedures for inter system mobility with interworking at service layer is specified in clause 7.4 in TS 23.247 [yy].

The joint BM-SC+MBSF/MBSTF functionality provides the security protection for MBS traffic. During inter-system mobility, when the target system is EPS, the security protection specified in TS 33.246 [xx] applies. The security protection specified in present document applies to the case when the target system is 5GS.

\*\*\*\*\*\*\*\*\*\*\*\* END OF 3rd CHANGE\*\*\*\*\*\*\*\*\*