**3GPP TSG-WG SA4 Meeting #119E e-meeting  *S4-220665***

**Elbonia, May 11th – 19th, 2022 (revision of S4-220426)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **DRAFT CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **26.502** | **CR** | **XXXX** | **rev** | **-** | **Current version:** | **17.0.0** |  |
|  | | | | | | | | |
| *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:*** | Security mechanisms for MBS traffic | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon | | | | | | | | | |
| ***Source to TSG:*** | SA4 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5MBUSA | | | | |  | ***Date:*** | | | 2022-04-28 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***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 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:*** | | Security part for MBS depending on SA3 progress is still missing. The SA3 Rel-17 5MBS work is completed and alignments are needed. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Add the sercuity mechanism for MBS traffic, including the general description, parameter exchanges between MBSF and MBSTF. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Security part is missing. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.5, 4.8, 7.2. | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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's revision history:*** | | 1. Add update of MSK/MTK in clause 4.5.2. 2. Continue the discussion after SA4#118e. | | | | | | | | |

\* \* \* \* 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 23.501: "System architecture for the 5G System (5GS)".

[3] 3GPP TS 23.502: "Procedures for the 5G System (5GS)".

[4] 3GPP TS 23.503: "Policy and charging control framework for the 5G System (5GS); Stage 2".

[5] 3GPP TS 23.247: "Architectural enhancements for 5G multicast-broadcast services; Stage 2".

[6] 3GPP TS 26.348: "Northbound Application Programming Interface (API) for Multimedia Broadcast/Multicast Service (MBMS) at the xMB reference point".

[7] 3GPP TS 26.501: "5G Media Streaming (5GMS); General description and architecture".

[8] IETF RFC 3500: "RTP: A Transport Protocol for Real-Time Applications".

[9] IETF RFC 2250: "RTP Payload Format for MPEG1/MPEG2 Video".

[10] 3GPP TS 26.247: "Transparent end-to-end Packet-switched Streaming Service (PSS); Progressive Download and Dynamic Adaptive Streaming over HTTP (3GP-DASH)".

[11] 3GPP TS 26.531: "Data Collection and Reporting; General Description and Architecture".

[12] 3GPP TS 23.468: "Group Communication System Enablers for LTE (GCSE\_LTE)".

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

\* \* \* \* Second change \* \* \* \*

### 4.3.3 MBSTF

#### 4.3.3.1 General

The functionality of the MBSTF is defined in clause 5.3.2.12 of TS 23.247 [5]. It receives User Plane data traffic at reference point Nmb8 and sends MBS data packets to the MB‑UPF via reference point Nmb9.

NOTE: The MBSTF may not be present in all deployments of the MBS System. However, the MBSTF is an integral and necessary component of MBS User Services and the present document is not concerned with deployments in which it is absent.

The present document defines additional User Plane functionalities of the MBSTF to support MBS User Services as follows:

1. Receiving MBS Distribution Session configurations from the MBSF at reference point Nmb2.

2. Sending notification events to the MBSF, e.g. data ingest failure, session terminated, delivery started via reference point Nmb2.

3. Based on the MBS Distribution Session configuration:

a) MBS delivery of ingested objects or sequences of objects to the MBS Client using the Object Distribution Method (see clause 6.1). This may be used to support real-time distribution of media segments (as special objects) including CMAF segments.

b) MBS delivery of ingested packet streams to the MBS Client using the Packet Distribution Method (see clause 6.2).

c) Delivery of MBS User Service Announcement information (including updates as necessary) within the MBS Session.

d) User plane authentication and UE authorization via MBS-4-MC (see clause 4.8.3).

\* \* \* \* Third change \* \* \* \*

### 4.4.1 Overview

The following reference points defined in clause 5.1 of TS 23.247 [5] are relevant to MBS User Services architecture: Nmb1, Nmb2, Nmb5, Nmb8, Nmb9, Nmb10 and Nmb12.

The following additional reference points are defined by the present document:

**- MBS-4-MC:** Mixed unidirectional multicast distribution of content from the MBSTF to the MBS Client and bidirectional unicast authentication/authorization between MBSTF and the MBS Client.

**- MBS-4-UC:** File-based unicast repair between the MBS Client and the MBS AS.

**- MBS-5:** Interactions between the MBS Client and the MBSF for the purpose of MBS control plane and service handling.

**- MBS-6:** API exposed by the MBS Client and used by the MBS-Aware Application to manage and control MBS User Services.

**- MBS-7:** API exposed by the MBS Client and used by the MBS-Aware Application to receive user data information distributed using MBS User Services.

**- MBS-8:** Announcement of MBS User Services to the MBS-Aware Application by the MBS Application Provider.

In addition, the following reference points are defined inside the MBS Client function:

- **MBS‑6′:** API exposed by the MBSTF Client and used by the MBSF Client to (de)activate reception of an MBS Session by the MBSTF. The reception parameters are supplied by the MBSF Client.

This reference point is outside the scope of MBS User Services and is not described further in the present document.

- **MBS‑7′:** API exposed by the MSTF Client and used by the MBSTF to supply MBS Session configuration information that has been received from reference point MBS‑4‑MC.

This reference point is outside the scope of MBS User Services and is not described further in the present document.

\* \* \* \* Forth change \* \* \* \*

## 4.5 Domain model

### 4.5.1 User Services domain model

The domain model for MBS User Services addresses different service and session concepts that are established between the different functional entities of the MBS User Services architecture, as shown in figure 4.5.1‑1.



Figure 4.5.1-1: MBS User Services domain model

In the above figure:

1. The MBS Application Provider initiates *MBS User Service Provisioning* with the MBSF to provision an *MBS User Service*.

2. Subsequently, the MBS Application Provider provisions a number of time-bound MBS User Data Ingest Sessions within the scope of the newly provisioned MBS User Service, also by means of MBS User Service Provisioning.

When the current time enters the time window of a provisioned MBS User Data Ingest Session:

3. The MBSF establishes an *MBS User Service Session* of the parent MBS User Service by establishing an MBS Session in the MBS System. The reception parameters of the MBS Session are advertised in an MBS User Service Announcement, as defined in clause 4.5.2 below. The MBS User Service Announcement is optionally passed back to the MBS Application Provider by means of MBS User Service Provisioning (see step 7bis).

4. The MBSTF establishes an *MBS User Data Ingest Session* between itself and the MBS Application Provider for the purpose of ingesting objects or packets, according to the type of distribution method provisioned.

5. The MBSTF establishes an *MBS Distribution Session* and begins to transmit objects or packets on it according to the configured distribution method as and when they are available from the MBS User Data Ingest Session. Optionally, the MBSTF client may initiate the user plane authentication and authorization with MBSTF as defined in clause 4.8.3 below.

When an MBS User Service is established:

6. The MBS-Aware Application instructs the MBSF Client to activate an MBS User Service by means of *MBS User Service Control*.

7. The MBSF Client may acquire the MBS User Service Announcement from the MBSF via the MBS User Service [or via the MBS Distribution Session] and pass selected application-facing parameters (such as the service class and service names) up to the MBS-Aware Application by means of *MBS User Service Control*.

7bis. Alternatively, the MBS User Service Announcement may be made available to the MBS Application Provider, in which case the MBS-Aware Application obtains it via an application-private *MBS Application Service* and then provides it to the MBSF Client by means of MBS User Service Control.

8. The MBS-Aware Application selects the announced MBS User Service via MBS User Service Control and, as a result, the MBSF Client activates reception of the corresponding MBS Distribution Session in the MBSTF Client.

9. An *MBS Application Data Session* is established between the MBSTF Client and the MBS-Aware Application to supply the latter with received (and possibly repaired) user data.

### 4.5.2 Static information model

Figure 4.5.2‑1 shows how the different service and session concepts depicted in figure 4.5.1‑1 above relate to each other. In this figure:

1. The MBS Application Provider provisions the parameters of a new MBS User Service by invoking the Nmbsf service either directly, or via the NEF.

2. The MBS Application Provider provisions a number of time-bound MBS User Data Ingest Sessions within the scope of the MBS User Service by invoking the Nmbsf service either directly, or via an equivalent service provided by the NEF. Each MBS User Data Ingest Session includes the details of one or more MBS Distribution Sessions. In the case of a multicast MBS Distribution Session, the MBS Application Provider may set the *Transport security protection mode* to indicate that whether control plane or user plane transport security protection is required for the MBS Distribution Session in question.

The MBSF provisions additional MBS Distribution Session parameters (denoted in table 4.5.6‑1 as assigned by the MBSF) and exposes some of them back to the MBS Application Provider (as indicated by the NOTE to table 4.5.6‑1).

NOTE: The MBSF typically allocates a Temporary Mobile Group Identity (TMGI) for each MBS Distribution session (see step 4 below), but it is also possible for the Nmbsf service invoker to nominate a particular value during this provisioning step if TMGI allocations are managed externally to the MBSF.

[3. The MBS Application Provider may additionally provision an MBS Consumption Reporting Configuration within the scope of the MBS User Service by invoking the Nmbsf service either directly, or via the NEF.]

Shortly before the current time enters the time window of a provisioned MBS User Data Ingest Session:

4. The MBSF provisions an MBS Session in the MBS System by invoking the Nmbsmf service on the MB‑SMF (see clause 9 of TS 23.247 [5]) to allocate a TMGI (if one has not already been allocated) for each MBS Distribution Session and to create an MBS Session Context for each one. In response, the MB-SMF provides the MB-UPF ingest information (specifically, the MB‑UPF tunnel endpoint address and traffic flow information to be used by the MBSTF) to the MBSF.

5. If transport security protection was provisioned in step 2 above, the MBSF generates a *Multicast session security context* for each MBS Distribution Session comprising an MBS Service Key (MSK) and its key ID, and distributes these to the MB-SMF.

In case the MSK needs to be updated based on the request from MB-SMF or or based on the local policy (e.g., key lifetime expiration), the the MBSF shall send the new MSK with MBS session ID and its key ID to the MB-SMF and MBSTF.

6. The MBSF provisions an MBS Distribution Session in the MBSTF by invoking the Nmbstf service at reference point Nmb2 using the parameters from the newly created MBS Session Context. In response, the MBSTF may provide the MBS Session ID, MBS Traffic Key (MTK) and the MTK ID to the MBSF as defined by clause W.4.1.2 of TS 33.501 [X].

In case the MTK needs to be updated based on the change of the authorization information or based on the local policy (e.g. key lifetime expiration), MBSF may trigger the MTK update with MBS Session ID to the MBSTF. In response, the MBSTF provides the new MTK to the MBSF.

7. Using the parameters from the MBS Distribution Session and from the newly created MBS Session Context, the MBSF compiles an MBS User Service Announcement to advertise the availability of the MBS User Service.



NOTE: Parameters not exposed to the MBS Application Provider via the Nmbsf service at reference point Nmb10 are annotated with the dagger symbol †.

Figure 4.5.2-1: MBS User Services static information model

### 4.5.3 MBS User Service parameters

This entity models an MBS User Service, as provisioned by the MBS Application Provider and as managed by the MBSF. The baseline parameters of an MBS User Service are listed in table 4.5.3‑1 below:

Table 4.5.3‑1: Baseline parameters of MBS User Service entity

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter | Cardinality | Assigner | Description |
| User Service Identifier | 1..1 | MBSF | A unique identifier for this MBS User Service in the MBSF. |
| External service identifiers | 1..\* | MBS Application Provider | A unique identifier for this MBS User Service that is also present in the MBS User Service Announcement.  If assigned in a globally unique manner, this identifier may be useful in correlating this MBS User Service with the same service delivered by a different system. |
| Service class | 1..1 | The class of this MBS User Service, expressed as a term identifier from a controlled vocabulary. |
| Service announcement modes | 1..\* | Determines whether the MBS User Service Announcement compiled by the MBSF is advertised to the MBSF Client at reference point MBS‑5[, and/or advertised to the MBSF Client via the MBS Session] and/or passed back to the MBS Application Provider. |
| Target service areas | 0..\* | The service areas in which this MBS User Service is to be made available. |
| Service names | 1..\* | A set of distinguishing names for this MBS User Service, one per language. |
| Service descriptions | 1..\* | A set of descriptions of this MBS User Service, one per language. |
| Service language | 0..1 | The main language of this MBS User Service. |

MBS User Data Ingest Sessions (see clause 4.5.5) are separately provisioned within the scope of an MBS User Service. It is valid for an MBS User Service to have no MBS User Data Ingest Sessions currently provisioned.

[An MBS Consumption Reporting Configuration (see clause 4.5.4 below) may be separately provisioned within the scope of an MBS User Service.]

### 4.5.4 MBS Consumption Reporting Configuration parameters

Consumption reporting for MBS User Services is for future study.

### 4.5.5 MBS User Data Ingest Session parameters

This entity models an MBS User Data Ingest Session, as provisioned by the MBS Application Provider and as managed by the MBSF. The baseline parameters for an MBS User Data Ingest Session are listed in table 4.5.5‑1 below:

Table 4.5.5‑1: Baseline parameters of MBS User Data Ingest Session entity

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter | Cardinality | Assigner | Description |
| Data Ingest Session Identifier | 1..1 | MBSF | An identifier for this MBS User Data Ingest Session that is unique in the scope of the parent MBS User Service (see clause 4.5.3). |
| Active periods | 0..\* | MBS Application Provider | Periods of time during which the MBS User Data Ingest Session is active in the MBS System.  If omitted, the session is active until further notice. |

The MBS User Data Ingest Session is composed of one or more MBS Distribution Sessions (see clause 4.5.6 below) and these shall be provisioned in the same operation as the enclosing MBS User Data Ingest Session. It is not valid for an MBS User Data Ingest Session to have no MBS Distribution Sessions defined.

### 4.5.6 MBS Distribution Session parameters

This entity models an MBS Distribution Session, as provisioned by the MBS Application Provider and as managed by the MBSF. This MBSF subsequently uses this information to provision a corresponding MBS Distribution Session in the MBSTF.

The baseline parameters for an MBS Distribution Session that are common to all distribution methods are listed in table 4.5.6‑1 below. All parameters are exposed to the MBS Application Provider except where noted otherwise.

Table 4.5.6‑1: Common baseline parameters of MBS Distribution Session entity

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter | Cardinality | Assigner | Description |
| Distribution Session Identifier | 1..1 | MBSF | An identifier for this MBS Distribution Session that is unique within the scope of the MBS User Service (see clause 4.5.3). |
| State | 1..1 | The current state of the MBS Distribution Session: INACTIVE, ESTABLISHED, ACTIVE or DEACTIVATING (see clause 4.6.1). |
| MBS Session Context | 1..1 | As defined in clause 6.9 of TS 23.247 [5] (see NOTE 1). |
| MB‑UPF tunnel endpoint address | 1..1 | The tunnel endpoint address of the MB‑UPF that supports this MBS Distribution Session at reference point Nmb9 (see NOTE 1). |
| MB‑UPF traffic flow information | 1..1 | Details of the traffic flow to be used by the MBSTF for this MBS Distribution Session, including the multicast group destination address and port number (see NOTE 1). |
| Multicast session security context | 0..1 | Security parameters (including MSK and MSK ID) used to protect the MBS Traffic Key when the MTK is delivered to the MBS Client (see NOTE 1 and NOTE 2).  The same session security context shall be used in all *Target service areas*. |
| Temporary Mobile Group Identity | 0..1 | MBSF or MBS Application Provider | The Temporary Mobile Group Identity (TMGI) of the MBS Session supporting this MBS Distribution Session.  Allocated by the MBSF in conjunction with the MB‑SMF unless supplied by the MBS Application Provider at the time of provisioning. |
| QoS information | 1..1 | MBS Application Provider | A 5G QoS Identifier (5QI) [2] to be applied to the traffic flow for this MBS Distribution Session. |
| Maximum bit rate | 1..1 | The maximum bit rate for this MBS Distribution Session. |
| Maximum delay | 0..1 | The maximum end-to-end distribution delay that is tolerated for this MBS Distribution Session by the MBS Application Provider. |
| Distribution method | 1..1 | The distribution method for this MBS Distribution Session, as defined in clause 6. |
| Distribution operating mode | 0..1 | The operating mode in the case where multiple modes are defined in clause 6 for the indicated distribution method. |
| FEC configuration | 0..1 | Configuration for FEC information added by the MBSTF to protect this MBS Distribution Session. |
| Transport security protection mode | 0..1 | The transport security protection to be enabled for this MBS Distribution Session, including control plane security, user plane security and no security (see NOTE 2). |
| NOTE 1: Internal parameter not exposed to the MBS Application Provider.  NOTE 2: Applicable only when the parent MBS User Session is distributed via Multicast MBS Session(s). | | | |

An MBS User Service Announcement (see clause 4.5.7 below) shall be associated with an MBS Distribution Session when the latter is in the ESTABLISHED or ACTIVE state.

The following MBS Distribution Session parameters are additionally relevant when the distribution method is the Object Distribution Method:

Table 4.5.6‑2: Additional MBS Distribution Session parameters for Object Distribution Method

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter | Cardinality | Assigner | Description |
| Object acquisition method | 1..1 | MBS Application Provider | Indicates whether the objects(s) are to be pushed into the MBSTF by the MBS Application Provider or whether they are to be pulled from the MBS Application Provider by the MBSTF. |
| Object acquisition identifiers | 1..1 | Identifies the object(s) to be ingested and distributed by the MBSTF during this MBS Distribution Session.  This could be the ingest URL of the object, or the ingest URL of a manifest describing a set of objects, or a reference into a manifest describing a set of objects. |
| Content ingest base URL | 0..1 | A prefix substituted by the MBSTF with the content distribution base URL prior to distribution of ingested objects. |
| Content distribution base URL | 0..1 | A prefix substituted by the MBSTF in place of the content ingest base URL prior to distribution of ingested objects. |

The following parameters are additionally relevant when the distribution method is the Packet Distribution Method:

Table 4.5.6‑3: Additional MBS Distribution Session parameters for Packet Distribution Method

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter | Cardinality | Assigner | Description |
| MBSTF tunnel endpoint address | 1..1 | MBSF | An endpoint address to which an MBS Application Provider establishes a unicast tunnel at reference point Nmb8 prior to the commencement of this MBS User Data Ingest Session. |
| MBSTF traffic flow information | 1..1 | Details of the User Plane data traffic flow to be used by the MBS Application Provider for this MBS Distribution Session, including the multicast group destination address and port number. |

### 4.5.7 MBS User Service Announcement parameters

This entity models an MBS User Service Announcement, which is compiled by the MBSF and used to advertise the current or imminent availability of an MBS User Service in the MBS System. The baseline parameters for an MBS User Service Announcement are listed in table 4.5.7‑1 below:

Table 4.5.7‑1: Baseline parameters of MBS User Service Announcement entity

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter | Cardinality | Assigner | Description |
| Temporary Mobile Group Identity | 1..1 | MB‑SMF | The Temporary Mobile Group Identity (TMGI) of the MBS Session supporting the parent MBS Distribution Session. |
| External service identifiers | 1..\* | MBS Application Provider | A unique identifier used by the MBSF Client to distinguish between MBS User Services.  If assigned in a globally unique manner, this identifier may be useful to the MBSF Client in correlating the MBS User Service with the same service delivered by a different system. |
| Service class | 1..1 | The class of the MBS User Service, expressed as a term identifier from a controlled vocabulary. |
| Start date–time | 0..1 | The point in time from which this MBS User Service Announcement is valid.  If not present, the announcement is already valid. |
| End date–time | 0..1 | The point in time after which this MBS User Service Announcement is no longer valid.  If not present, the announcement is valid indefinitely. |
| Service names | 1..\* | A set of distinguishing names for the MBS User Service, one per language. |
| Service descriptions | 1..\* | A set of descriptions of the MBS User Service, one per language. |
| Service language | 0..1 | The main language of the MBS User Service. |
| Distribution method | 1..1 | The distribution method for this MBS User Service, as defined in clause 6. |
| Distribution operating mode | 0..1 | The operating mode in the case where multiple modes are defined in clause 6 for the indicated distribution method. |
| Session Description parameters[ ] | 1..1 | MBSF | Additional parameters needed to receive the MBS Session supporting this MBS User Service, including relevant User Plane traffic flow parameters. |
| Transport security protection parameters | 0..1 | The security parameters needed for protecting the MBS Service, including MSK ID, key managment server address, etc. |

\* \* \* \* Fifth change \* \* \* \*

## 4.8 Security

### 4.8.1 General

As defined in TS 33.501 [X], security protection of MBS traffic can be supported by use of either a control plane procedure or a user plane procedure at the service layer.

### 4.8.2 Control plane security procedure

As defined in TS 33.501 [X], control plane security procedures apply to multicast MBS Sessions only. In the context of the present document, transport security may be applied to MBS Distribution Sessions that are distributed using a multicast MBS Session as indicated by the *Service type* of the parent MBS User Service.

For each such multicast MBS Distribution Session, the MBSF determines whether control plane transport security protection is to be applied based on the *Transport security protection mode* provisioned by the MBS Application Provider or, if this is not provisioned, based on local policy.

If transport security protection is to be applied, the following procedure defined in clause W.4.1.2 of TS 33.501 [X] is followed:

1. The MBSF shall generate the MBS Service Key (MSK) and the MSK ID and distribute them to the MB-SMF and MBSTF together with the associated MBS Session ID.

2. Subsequently, the MBSTF shall generate an MBS Traffic Key (MTK) associated with the MSK and the MTK ID, and shall provide them to the MBSF together with the associated MBS Session ID.

The MBSTF shall protect the MBS traffic of the multicast Distribution Session in question with the MTK.

When the MTK is distributed to the MBS Client over the User Plane, the MSK is used to protect the MTK.

The MBSF includes the *Transport security protection parameters* in the MBS Distribution Session Announcement, e.g. the MSK ID and key management server address (i.e. MBSTF address).

During the multicast join procedure, the SMF provides the multicast session security context to the MBS Client. The MBS Client shall use the MTK in the received multicast session security context to decrypt the protected multicast MBS Session.

When the MSK expires, or when the authorization information related to the MBS Session changes, the MBSF shall generate a new MSKand a new MSK ID and shall send them to the MB‑SMF and to the MBSTF together with the associated MBS Session ID.

### 4.8.3 User plane security procedure

As defined in TS 33.501 [X], user plane security procedures apply to multicast MBS Sessions and broadcast MBS Sessions. Similarly, the MBSF can determine whether user plane transport security protection is to be applied based on the *Transport security protection mode* provisioned by the MBS Application Provider or, if this is not provisioned, based on local policy.

When the user-plane security procedure is used, the following MBS service authorization procedure defined in clause W.4.1.3 of TS 33.501 [X] is followed.

The UE authenticates to the MBSTF based on the GBA as in MBMS security or based on the AKMA as defined in TS 33.501 [X].

After receiving the MBS Distribution Session Annoucement, the MBS Client contacts the key management server (i.e. MBSTF) at reference point MBS-4-MC to authorise access to the MBS Distribution Session in question. The MBS Distribution Session shall be identified by the MBS Session Identifier advertised in the MBS Distribution Session Announcement and the user shall be identified by an identifier appropriate to the security mechanism in use (e.g. IMPI for GBA or GPSI for AKMA).

If it does not already have a valid copy cached, the MBSTF invokes the Nmbsf\_MBSDistributionSession\_‌Authorize service operation provided by the MBSF at reference point Nmb2 for retrieval of authorization results from the UDM before authorising the MBS Client to access the MBS Distrubutuon Session.

\* \* \* \* Sixth change \* \* \* \*

## 7.2 MBSF Services

### 7.2.1 General

The following table illustrates the set of Network Function services exposed by the MBSF.

Table 7.2-1: NF services provided by MBSF

|  |  |  |  |
| --- | --- | --- | --- |
| Service name | Service operation name | Operation semantics | Example consumer(s)  (see NOTE) |
| Nmbsf\_MBSUserService | Create | Request/Response | AF, NEF |
| Retrieve | Request/Response | AF, NEF |
| Update | Request/Response | AF, NEF |
| Destroy | Request/Response | AF, NEF |
| Nmbsf\_MBSUserDataIngestSession | Create | Request/Response | AF, NEF |
| Retrieve | Request/Response | AF, NEF |
| Update | Request/Response | AF, NEF |
| Destroy | Request/Response | AF, NEF |
| StatusSubscribe | Subscribe/Notify | AF, NEF |
| StatusUnsubscribe | AF, NEF |
| StatusNotify | AF, NEF |
| Nmbsf\_MBSDistributionSession | Authorize | Request/Response | MBSTF |
| NOTE: Service exposure to the AF is for further study. | | | |

### 7.2.2 Nmbsf MBS User Service operations

#### 7.2.2.1 Nmbsf\_MBSUserService\_Create service operation

**Service operation name:** Nmbsf\_MBSUserService\_Create

**Description:** Provision a new MBS User Service. The general data model is illustrated in figure 4.5.2-1.

**Input (Required, Optional):** Parameters in table 4.5.3-1 assigned by the MBS Application Provider.

**Output (Required, Optional):** Parameters in table 4.5.3-1.

#### 7.2.2.2 Nmbsf\_MBSUserService\_Retrieve service operation

**Service operation name:** Nmbsf\_MBSUserService\_Retrieve

**Description:** Used by the NF/NEF to retrieve the properties of an existing MBS User Service.

**Input (Required, Optional):** MBS User Service Identifier

**Output (Required, Output):** Parameters in table 4.5.3-1.

#### 7.2.2.3 Nmbsf\_MBSUserService\_Update service operation

**Service operation name:** Nmbsf\_MBSUserService\_Update

**Description:** Update the properties of an existing MBS User Service.

**Input (Required, Optional):** MBS User Service Identifier. Parameters in table 4.5.3-1 assigned by the MBS Application Provider.

**Output (Required, Optional):** Result indication. Parameters in table 4.5.3-1.

#### 7.2.2.4 Nmbsf\_MBSUserService\_Destroy service operation

**Service operation name:** Nmbsf\_MBSUserService\_Destroy

**Description:** Release the resources of the associated MBS User Service.

**Input (Required, Optional):** MBS User Service Identifier.

**Output (Required, Optional):** Result indication.

### 7.2.3 Nmbsf MBS User Data Ingest Session operations

#### 7.2.3.1 Nmbsf\_MBSUserDataIngestSession\_Create service operation

**Service operation name:** Nmbsf\_MBSUserDataIngestSession\_Create

**Description:** Create an MBS User Data Ingest Session, including a set of subordinate MBS Distribution Session(s).

**Input (Required, Optional):** Parameters in table 4.5.5‑1 and table 4.5.6‑1, and either table 4.5.6‑2 or table 4.5.6‑3 assigned by the MBS Application Provider, depending on the distribution method.

**Output (Required, Optional):** Result indication. MBS User Data Ingest Session Identifier.

#### 7.2.3.2 Nmbsf\_MBSUserDataIngestSession\_Retrieve service operation

**Service operation name:** Nmbsf\_MBSUserDataIngestSession\_Retrieve

**Description:** Used by the AF/NEF to retrieve the properties of an existing MBS User Data Ingest Session.

**Input (Required, Optional):** MBS User Data Ingest Session Identifier.

**Output (Required, Optional):** Result indication. Parameters in table 4.5.5‑1 and table 4.5.6‑1, and either table 4.5.6‑2 or table 4.5.6‑3, depending on the distribution method.

#### 7.2.3.3 Nmbsf\_MBSUserDataIngestSession\_Update service operation

**Service operation name:** Nmbsf\_MBSUserDataIngestSession\_Update

**Description:** Update the properties of an existing MBS User Data Ingest Session and its set of subordinate MBS Distribtion Session(s).

**Input (Required, Optional):** MBS User Data Ingest Session Identifier. Parameters in table 4.5.5‑1 and table 4.5.6‑1, and either table 4.5.6‑2 or table 4.5.6‑3, depending on the distribution method.

**Output (Required, Optional):** Result indication.

#### 7.2.2.4 Nmbsf\_MBSUserDataIngestSession\_Destroy service operation

**Service operation name:** Nmbsf\_MBSUserDataIngestSession\_Destroy

**Description:** Destroy an MBS User Data Ingest Session along with its subordinate MBS Distribution Session(s).

**Input (Required, Optional):** MBSUser Data Ingest Session Identifier.

**Output (Required, Optional):** Result indication.

#### 7.2.2.5 Nmbsf\_MBSUserDataIngestSession\_StatusSubscribe operation

**Service operation name:** Nmbsf\_MBSUserDataIngestSession\_StatusSubscribe

**Description:** Invoked by AF/NEF on the MBSF when it needs to create a subscription to monitor at least one event relevant to the MBS User Data Ingest Session. The AF may subscribe to multiple events in a subscription.

**Input (Required, Optional):** MBS User Data Ingest Session Identifier, Event ID(s), notification target address.

**Output (Required, Optional):** When the subscription is accepted: Subscription correlation ID.

#### 7.2.2.6 Nmbsf\_MBSUserDataIngestSession\_StatusUnsubscribe operation

**Service operation name:** Nmbsf\_MBSUserDataIngestSession\_StatusUnsubscribe

**Description:** Remove an existing subscription.

**Input, Required:** Subscription correlation ID.

**Output, Required:** Result Indication.

#### 7.2.2.7 Nmbsf\_MBSUserDataIngestSession\_StatusNotify operation

**Service operation name:** Nmbsf\_MBSUserDataIngestSession\_StatusNotify

**Description:** Used by the MBSF to notify AF/NEF about the status change of the MBS User Data Ingest Session or the status of a file.

**Input (Required, Optional):** MBS User Data Ingest Session Identifier, Event ID(s).

**Output, Required:** Result indication.

### 7.2.4 Nmbsf MBS Distribution Session operations

#### 7.2.4.1 Nmbsf\_MBSDistributionSession\_Authorize service operation

**Service operation name:** Nmbsf\_MBSDistributionSession\_Authorize

**Description:** Used by the MBSTF to acquire authorization results from the UDM via the MBSF.

**Input (Required, Optional):** MBS Session Identifier, User Identifier.

**Output (Required, Optional):** Authorization result.

\* \* \* \*Seventh change \* \* \* \*

### 7.3.2 Nmbstf\_MBSDistributionSession service

#### 7.3.2.1 Nmbstf\_MBSDistributionSession\_Create service operation

**Service operation name:** Nmbstf\_MBSDistributionSession\_Create

**Description:** Create a new MBS Distribution Session within the MBSTF.

**Input (Required, Optional):** Parameters in table 4.5.6‑1 and either table 4.5.6‑2 or table 4.5.6‑3, depending on the distribution method.

**Output, Required:** Result indication.

**Output, Optional:** MBS Session ID, MTK and the corresponding MTK ID.

#### 7.3.2.2 Nmbstf\_MBSDistributionSession\_Retrieve service operation

**Service operation name:** Nmbstf\_MBSSession\_Retrieve

**Description:** Retrieve the parameters of an existing MBS Distribution Session.

**Input (Required, Optional):** MBS Distribution Session Identifier.

**Output, Required:** Parameters in table 4.5.6‑1and either table 4.5.6‑2 or table 4.5.6‑3, depending on the distribution method.

#### 7.3.2.3 Nmbstf\_MBSDistributionSession\_Update service operation

**Service operation name:** Nmbstf\_MBSDistribtionSession\_Update

**Description:** Update an existing MBS Distribution Session, for example to change the session stop time, object delivery session, application session, packets delivery session, files, and ancillary information.

**Input (Required, Optional):** MBS Distribution Session Identifier. Parameters in table 4.5.6‑1and either table 4.5.6‑2 or table 4.5.6‑3, depending on the distribution method.

**Output, Required:** Result indication.

**Output, Optional:** MBS Session ID, MTK and the corresponding MTK ID.

#### 7.3.2.4 Nmbstf\_MBSDistribtutionSession\_Destroy service operation

**Service operation name:** Nmbstf\_MBSDistributionSession\_Update

**Description: D**estroy an existing MBS Distribution Session.

**Input (Required, Optional):** MBS Distribution Session Identifier.

**Output, Required:** Result indication.

#### 7.3.2.5 Nmbstf\_MBSDistributionSession\_StatusSubscribe operation

**Service operation name:** Nmbstf\_MBSDistirbutionSession\_StatusSubscribe

**Description:** Invoked by MBSF on the MBSTF when it needs to monitor at least one event relevant to the MBS Distribution session. The MBSF may subscribe to multiple events in a subscription.

**Input (Required, Optional):** MBS Distribution Session Identifier, Event ID(s), notification target address.

**Output:** When the subscription is accepted: Subscription correlation ID.

#### 7.3.2.6 Nmbstf\_MBSDistributionSession\_StatusUnsubscribe operation

**Service operation name:** Nmbstf\_MBSDistributionSession\_StatusUnsubscribe

**Description:** Remove an existing subscription.

**Input (Required, Optional):** Subscription correlation ID.

**Output:** Result indication.

#### 7.3.2.7 Nmbstf\_MBSDistributionSession\_StatusNotify operation

**Service operation name:** Nmbstf\_MBSDistributionSession\_StatusNotify

**Description:** Used by the MBSTF to notify the MBSF about the status change of the MBS Distribution Session or the status of the file.

**Input (Required, Optional):** MBS Distribution Session Identifier, Event ID(s).

**Output:** Result indication.

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