**3GPP TSG-WG SA4 Meeting #124  *S4-230873***

**Berlin, Germany, May 22 – 26, 2023**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **26.502** | **CR** | **0023** | **rev** | **-**  | **Current version:** | **17.4.0** |  |
|  |
| *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:***  | Security mechanisms for MBS traffic |
|  |  |
| ***Source to WG:*** | Huawei, HiSilicon, BBC |
| ***Source to TSG:*** | SA4 |
|  |  |
| ***Work item code:*** | 5MBUSA |  | ***Date:*** | 2023-05-16 |
|  |  |  |  |  |
| ***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 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:*** | In LS S4-230346 sent in Feb meeting, SA4 recommends SA3 to use the MBSSF as a logic function to handle both the control plane and user plane security procedures. In S3-232690, SA3 is disucssing how to resolve the inconsistency issue. This paper intends to add necessary clarifications in SA4 specs.  |
|  |  |
| ***Summary of change:*** | Add support of the sercuity mechanism for MBS traffic.* add security support in static information model and the MBS Distribution Session (Announcement) parameters,

add general description for the MBS security mechanism refering TS 33.501.  |
|  |  |
| ***Consequences if not approved:*** | Security part is missing. |
|  |  |
| ***Clauses affected:*** | 4.5.2, 4.5.6, 4.8. |
|  |  |
|  | **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:*** |  |

\* \* \* \* 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 3550: "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)".

[13] 3GPP TS 26.517: "5G Multicast–Broadcast User Services; Protocols and Formats".

[14] 3GPP TS 23.468: "Group Communication System Enablers for LTE (GCSE\_LTE)".

[15] 3GPP TS 29.522: "5G System; Network Exposure Function Northbound APIs; Stage 3".

[16] OMA: "OMNA BCAST Service Class Registry", <https://technical.openmobilealliance.org/OMNA/bcast/bcast-service-class-registry.html>.

[17] IANA: "Reliable Multicast Transport (RMT) FEC Encoding IDs and FEC Instance IDs", <https://www.iana.org/assignments/rmt-fec-parameters/rmt-fec-parameters.xhtml#rmt-fec-parameters-1>.

[18] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

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

Second change

### 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. This specifies which of the *Service announcement modes* are to be used to advertise the MBS User Service, as well as descriptive metadata for inclusion in the MBS User Service Announcement.

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 Nnef service provided by the NEF. Each MBS User Data Ingest Session includes the details of one or more MBS Distribution Sessions.

- To indicate that it has a restricted MBS service area (i.e. corresponding to a local MBS Service, as defined in clause 6.2.2 of TS 23.247 [5]), an MBS Distribution Session may specify one or more *Target service areas*. In line with [5], MBS data is not transmitted outside the MBS service area derived from the indicated *Target service areas*.

- To provision location-dependent variants of an MBS User Service (see clause 6.2.3 of TS 23.247 [5]), a number of MBS Distribution Sessions conveying different MBS data may be provisioned within the scope of the same MBS User Service by setting the *Location-dependent service flag* on the MBS Distribution Sessions of each variant. Location-dependent MBS Distribution Session variants shall have the same *MBS Session Identifier*, but they shall have disjoint *Target service areas*.

- When the *Multiplexed service flag* is set on the MBS Distribution Session, all MBS Distribution Sessions with an identical (or empty) set of *Target service areas* shall be multiplexed onto the same MBS Session. The *MBS Session Identifier* shall be the same for all MBS Distribution Sessions within the multiplex. This feature may be combined with the *Location-dependent service flag*, in which case each location-dependent multiplex of MBS Distribution Sessions is mapped into a separate MBS Session.

- The MBS Application Provider may set the *Transport security protection* flagto indicate that transport security protection (as specified in annex W of TS 33.501 [18]) is required for the MBS Distribution Session. When the flag is set, the MBSSF chooses between the control plane or user plane security procedure.

 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 1: The MBSF typically allocates an *MBS Session Identifier*, such as a Temporary Mobile Group Identity (TMGI) for each MBS Distribution session (see step 4 below) as a side-effect of provisioning, 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.

NOTE 2: Reception reporting for MBS User Services is for future study.

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. The parameters of the MBS Session Context shall be populated as specified in clause 4.5.9. 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. 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.

6. 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 and makes this service access information available by one or more of the *Service announcement modes* provisioned in the MBS User Service.



NOTE 1 Square brackets after a parameter name indicate multiplicity; parameter names rendered in italics with parentheses are optional. See the following clauses for details.

NOTE 2: Parameters and entities not exposed to the MBS Application Provider via the Nmbsf service at reference point Nmb10 are annotated with the dagger symbol †.

NOTE 3: MBS Session Identifier is defined by clause 6.5.1 of TS 23.247 [5] as a Temporary Mobile Group Identity (TMGI) or a Source-Specific Multicast (SSM) IP address.

Figure 4.5.2-1: MBS User Services static information model

Third change

### 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 following parameters assigned by the MBS Application Provider may be updated by the MBS Application Provider at any time:

- Target service areas,

- MBS Frequency Selection Area (FSA) Identifier (applicable only to broadcast Service type)

- QoS information.

With the exception of the *MBS Session Identifier* (which is immutable after initial assignment) and the *Location-dependent service flag* (which is immutable after creation), all other parameters assigned by the MBS Application Provider may be updated by the MBS Application Provider when the MBS Distribution Session is in the INACTIVE state.

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..\* |  | As defined in clause 6.9 of TS 23.247 [5] (see NOTE 1).There shall be one MBS Session Context associated with the MBS Distribution Session unless multiple *Target service areas* are specified (see below). |
| MB‑UPF tunnel endpoint address | 0..1 |  | The tunnel endpoint address of the MB‑UPF that supports this MBS Distribution Session at reference point Nmb9 (see NOTE 1, NOTE 4). |
| MBMS GW tunnel endpoint address | 0..1 |  | The tunnel endpoint address of the MBMS GW that supports this MBS Distribution Session at reference point SGi‑mb (see NOTE 1, NOTE 4). |
| User Plane traffic flow information | 0..1 |  | Details of the MBS-4-MC User Plane traffic flow to be used by the MBSTF for this MBS Distribution Session, including the multicast group destination address and port number to be used inside the unicast tunnel at reference point Nmb9 (see NOTE 1).This parameter is mandatory except in the case of Packet Distribution Method operating in Forward-only mode, in which case multicast-addressed packets ingested at reference point Nmb8 are relayed to Nmb9 without changing their address. |
| MBS Session Identifier | 0..1 | MBSF or MBS Application Provider | The Temporary Mobile Group Identity (TMGI) or Source-Specific Multicast (SSM) IP address of the MBS Session supporting this MBS Distribution Session (see NOTE 2).Multiple MBS Distribution Sessions within the scope of the same MBS User Service may share the same value if they are location-dependent MBS Services, as defined in clause 6.2.3 of TS 23.247[5].TMGI values are allocated by the MBSF in conjunction with the MB‑SMF unless supplied by the MBS Application Provider at the time of provisioning. |
| Target service areas | 0..\* | MBS Application Provider | The set of regions comprising the MBS service area in which this MBS Distribution Session is to be made available (see NOTE 2).The provided set of regions shall be disjoint with that of every other MBS Distribution Session sharing the same MBS Session Identifier.A unique MBS Session Context shall be associated with the MBS Distribution Session for each declared service area, distinguishable by its Area Session Identifier. |
| MBS Frequency Selection Area (FSA) Identifier | 0..1 |  | (Applicable only to broadcast *Service type*.) Identifies a preconfigured area within which, and in proximity to, the cell(s) announce the MBS FSA ID and the associated frequency corresponding to this MBS Distribution Session (see NOTE 3). |
| Location-dependent service flag | 0..1 |  | An indication that this MBS Distribution Session corresponds to a location-dependent MBS Session.If the flag is unset or omitted, the MBS Distribution Session is not location-dependent. |
| Multiplexed service flag | 0..1 |  | If set, all MBS Distribution Sessions in the scope of the same parent MBS User Data Ingest Session with identical or empty sets of *Target service areas* shall be multiplexed onto the same MBS Session.All MBS Distribution Sessions in the multiplex shall be assigned the same MBS Session Identifier. |
| Restricted membership flag | 0..1 |  | (Applicable only to multicast *Service type*.) An indication that this MBS Distribution Session is restricted to a set of UEs according to their current subscription status in the MBS System.If the flag is set, only UEs in the restricted set are permitted to join thls MBS Distribution Session; otherwise, any UE is permitted to join. |
| QoS information | 0..1 |  | A 5G QoS Identifier (5QI) [2] to be applied to the traffic flow for this MBS Distribution Session (see NOTE 2).The 5QI information is used by the MBSF to set the Quality of Service for the MBS Session by interacting with the PCF at reference point Nmb12. |
| Maximum content bit rate | 1..1 |  | The maximum bit rate for content in this MBS Distribution Session. |
| Maximum content delay | 0..1 |  | The maximum end-to-end content 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. |
| 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 Application Level FEC (AL-FEC) information added by the MBSTF to protect this MBS Distribution Session.The AL‑FEC scheme shall be identified using a term from the Reliable Multicast Transport (RMT) controlled vocabulary of FEC Encoding IDs [17] expressed as a fully-qualified URI, e.g. urn:ietf:rmt:fec:encoding:0.The overhead of AL‑FEC protection shall be specified as a proportion of the (unprotected) MBS data, e.g. 1.1 for 10% overhead.Additional scheme-specific parameters may be signalled in the form of uncontrolled name–value pairs. |
| Transport security protection | 1..1 |  | A flag indicating whether transport security protection is required by the MBS Application Provider for this MBS Distribution Session.The MBSSF determines whether the control plane security procedure (see NOTE 5) or the user plane security procedure is selected. (See annex W of TS 33.501 [18] for details of these procedures.) |
| Traffic marking information | 0..1 | MBS Application Provider or MBSF | Information (e.g. a Differentiated Services Code Point) used by the MBSTF to mark the multicast packets that it conveys to the MB‑UPF at reference point Nmb9. |
| NOTE 1: Internal parameter not exposed to the MBS Application Provider.NOTE 2: Parameter not relevant to the MBSTF.NOTE 3: Used to guide frequency selection by the UE for a broadcast MBS Session.NOTE 4: At least one of *MB‑UPF tunnel endpoint address* or *MBMS GW tunnel endpoint address* shall be present.NOTE 5: The control plane security procedure (see clause W.4.1.2 of TS 33.501 [18]) is applicable only to Multicast MBS Session(s). |

An MBS Distribution Session Announcement (see clause 4.5.8 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 as part of the corresponding MBS User Data Ingest Session.In the latter case, the *Object acquisition method* indicates whether the object(s) are to be retrieved once from the MBS Application Provider at the start of each active period of the corresponding MBS User Data Ingest Session, or whether the MBSTF is required to check their validity periodically, for example once per rotation of an object carousel. |
| Object acquisition identifiers | 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. |
| Object ingest base URL | 0..1 | MBS Application Provider or MBSF | A URL prefix substituted by the MBSTF with the *Object distribution base URL* prior to distribution of ingested objects.Assigned by the MBS Application Provider for the pull-based *Object acquisition method*. Assigned by the MBSF for push-based object acquisition.If omitted, nothing is removed from the content ingest URL when forming the object distribution URL |
| Object distribution base URL | 0..1 | MBS Application Provider | A URL prefix substituted by the MBSTF in place of the *Object ingest base URL* prior to distribution of ingested objects.If present, the optional *Object ingest base URL* shall also be present.If omitted, the object distribution URL is the same as the object ingest URL. |
| Object repair base URL | 0,,1 | MBSF | A URL prefix substituted by the MBSTF Client in place of the *Object distribution base URL* when repairing objects not received completely intact from this MBS Distribution Session (see NOTE). The value shall point to the MBS AS.Present only when object repair is provisioned for this MBS Distribution Session. |
| NOTE: Parameter not relevant to the MBSTF. |

The following MBS distribution session 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 |
| Packet ingest method | 1..1 | MBS Application Provider | Indicates whether packets are to be ingested using multicast ingest or unicast ingest.Multicast ingest is valid for Proxy mode only. In this case, the MBSTF shall join a Source-Specific Multicast (SSM) group indicated in *MBSTF ingest endpoint addresses* parameter.Unicast ingest is valid for Proxy mode and Forward-only mode. In this case, the MBSTF shall allocate a listening IP address and port number for packet ingest and shall return it to the MBSF in the *MBSTF ingest endpoint addresses* parameter below. |
| MBSTF ingest endpoint addresses | 1..1 | MBS Application Provider, MBSF, MBSTF | The endpoint addresses used by the MBS Application Provider and MBSTF to establish a connection at reference point Nmb8 prior to the commencement of this MBS User Data Ingest Session.In the case of Proxy mode, this shall be the Source-Specific Multicast (SSM) endpoint addresses (including the source IP address, destination multicast group address and destination UDP port) nominated by the MBS Application Provider or else by the MBSF.In the case of Forward-only mode, this shall be the IP addresses and UDP port numbers at the source and destination ends of the content ingest tunnel, nominated respectively by the MBS Application Provider and the MBSTF. |

\* \* \* \* Fourth change \* \* \* \*

### 4.5.8 MBS Distribution Session Announcement parameters

This entity models an MBS Distribution Session Announcement, which is compiled by the MBSF and used to advertise the current or imminent availability of an MBS Distribution Session in the MBS System. The baseline parameters for an MBS Distribution Session Announcement are listed in table 4.5.8‑1 below:

Table 4.5.8‑1: Baseline parameters of MBS Distribution Session Announcement entity

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter | Cardinality | Assigner | Description |
| MBS Session Identifier | 1..1 | MB‑SMF | The Temporary Mobile Group Identity (TMGI) or Source-Specific Multicast (SSM) IP address of the MBS Distribution Session from which this announcement is derived. |
| MBS Frequency Selection Area (FSA) Identifier | 0..1 | MBS Application Provider or MB-SMF | (Broadcast MBS Session only.) Identifies a preconfigured area within which, and in proximity to, the cell(s) are announcing the MBS FSA ID and the associated frequency corresponding to this MBS Distribution Session Announcement. (see NOTE) |
| Distribution method | 1..1 | MBS Application Provider | The distribution method (as defined in clause 6) of the MBS Distribution Session from which this announcement is derived. |
| Session Description parameters | 1..\* | MBSF | Additional parameters needed to receive the MBS Distribution Session from which this announcement is derived, including relevant User Plane traffic flow parameters. |
|  Service protection description | 0..1 | The security parameters for the MBS Distribution Session (see clause W.4.2 of TS 33.501), including:- Which form of transport security protection is in force, whether UICC key management (see TS 33.246 [X]) is selected and/or whether 2G GBA security (see TS 33.246 [X]) is selected.- The MBS Session Key (MSK) identifier and key domain.- The address of the key management server (FQDN of the MBSSF) when user plane security is in force. |
| NOTE: Used to guide frequency selection by the UE for a broadcast MBS Session. |

The following session announcement parameters are additionally relevant when *Distribution method* above indicates the Object Distribution Method:

Table 4.5.8‑2: Additional MBS Distribution Session Announcement parameters for Object Distribution Method

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter | Cardinality | Assigner | Description |
| Object distribution schedule | 0..1 | MBS Application Provider | A schedule indicating when individual objects are to be delivered on the corresponding MBS Distribution Session.Present only when this information has been provided in the *Object acquisition identifiers* of the corresponding MBS Distribution Session (see table 4.5.6‑2). |
| Object distribution base URL | 0..1 |  | A URL prefix substituted by the MBSTF Client with the *Object repair base URL* when repairing objects not received completely intact from the corresponding MBS Distribution Session.Present only when object repair is provisioned for the corresponding MBS Distribution Session. |
| Object repair base URL | 0..1 | MBSF | The base URL of the MBS AS to be used for object repair of the corresponding MBS Distribution Session.Present only when object repair is provisioned for the corresponding MBS Distribution Session. |

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

## 4.8 Security

The security protection of MBS traffic is supported by use of either a control plane procedure or a user plane procedure at the service layer as defined in annex W of TS 33.501 [18]. The control plane procedure is only applicable for multicast sessions, while the user plane procedure is applicable for both multicast sessions and broadcast sessions. The MBSSF, as a logical function co-located with either the MBSF or the MBSTF, is responsible for key generation, management and distribution, including both MBS Session Keys and MBS Traffic Keys defined by [18]).

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