**3GPP TSG-SA3 Meeting #107-e *draft\_S3-220858-r1***

**e-meeting, 16 – 20 May 2022 Revision of S3-22xxxx**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **1373** | **rev** | **-** | **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 | **x** | Radio Access Network |  | Core Network | **x** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Removing the Editor’s Note and add clarifications in the security mechanisms for MBS | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5MBS | | | | |  | ***Date:*** | | | 2022-04-17 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | Some statements in the clause on the MBS security mechanisms require further clarification and corrections in order to avoid confusion. For example:   1. The detailed description for “security protection” is required. It would be helpful if this ambiguity could be resolved. 2. Rewording is needed for the HTTP POST message to avoid ambiguity. It reuses the specification in TS 33.246 for 5G MBS rather than the message itself in MBMS. 3. Based on the reply LS on secondary authentication for multicast PDU session (S2-2200069), the editor’s note is not needed. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Corrections and clarifications in the security mechanisms for MBS. The editor’s note is converted to the normative text. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Incomplete and misleading description of the security mechanisms for MBS | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | Annex W.4, W.4.1.3, W.4.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\*\*\*\*\*\*\*\*\*\*\*\* START OF 1st CHANGE\*\*\*\*\*\*\*

# W.4 Security mechanisms for MBS traffic transmission

If the security protection of MBS traffic is required, it includes confidentiality and integrity protection, as specified in clause 5.3 of TS 33.246 [102]. The control-plane procedure and user-plane procedure are optionally supported in service layer. The user plane security between UE and RAN shall be deactivated when 5GC shared MBS traffic delivery method for MBS data transmission is used to avoid redundant protection.

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

\*\*\*\*\*\*\*\*\*\*\* START OF 2nd CHANGE\*\*\*\*\*\*\*

### W.4.1.3 User-plane procedure

The UE registers to the MBS service and receives the MBS traffic as specified in TS 33.246 [102] with the following changes.

- MBSTF takes the role of the BM-SC in TS 33.246 [102].

- The UE authenticates to the MBSTF based on the GBA as in MBMS security (see TS 33.246 [102]) or based on the AKMA (see TS 33.535 [104]). When the AKMA is used, the MRK is derived from the KAF as specified in Annex F of TS 33.246 [102] by replacing the Ks\_NAF for the GBA\_ME run with KAF. Furthermore, when the AKMA is used, the MUK is set to KAF. When the authorization of MBS service to the UE is required, the user id (e.g., GPSI) provided to the MBSTF by the AAnF shall be used.

- The identifier(s) of MBS user service(s) in TS 26.502[108] is included in local configuration in MBSTF or in UDM as part of MBS subscription data for a UE, which identifies the user service(s) that the UE is allowed to join. After receiving the HTTP POST message, as specified in clause 6.3.2 of TS 33.246 [102], which includes the identifier(s) of MBS user service(s), MBSTF shall authorize the UE based on local configuration if available. If no local configuration is available, the MBSTF should send verification request with user id (e.g., IMPI in GBA or GPSI in AKMA) and identifier(s) of MBS user service(s) to UDM via MBSF/NEF to acquire the authorization result. If the UE is authorized, the MBSTF registers the UE to the MBS user service(s).

NOTE: the local configuration in MBSTF may be preconfigured or provided by AF.

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

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

## W.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.

The secondary authentication for multicast session is not specified in the present document. AKMA/GBA is supported for authentication and authorization in user-plane procedure for security protection of MBS traffic, as specified in clause W.4.1.3 of the present document.

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