**3GPP TSG-SA3 Meeting #106-e *draft\_S3-220164-r1***

**e-meeting, 14 – 25 February 2022 Merger of S3-220164 and S3-220092**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **1276** | **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 |  | Radio Access Network |  | Core Network | **x** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Corrections and clarifications in the security mechanisms for MBS | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5MBS | | | | |  | ***Date:*** | | | 2022-01-17 |
|  |  | | | |  | |  | | |  |
| ***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. Rewording is needed in the requirements for key identification in order to align with the mechanisms and terminology of TS 33.246. 2. In the description of the message exchanges, some security parameters are missing such as the key identifiers. 3. Several typos such as in the abbreviation of MBSTF. 4. Etc. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Corrections and clarifications in the security mechanisms for MBS | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Incomplete and misleading description of the security mechanisms for MBS | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | Annex W.4.1.2, 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

…

### W.4.1.2 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 identification for every MSK and MTK are determined as specified in Clause 6.3.2.1 and clause 6.3.3.1 of TS 33.246 [102].

The MBSF generates the MSK and its key ID for a MBS session. Afterwards, the MBSF distributes the MSK with MBS session ID and its key ID to the MB-SMF and MBSTF. The MBSF shall also 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 and its key ID after protecting it using the MSK as specified in TS 33.246 [102]. The MBSTF shall also provide the new MTK and its key ID 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 with MBS session ID and its key ID 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 [103]. The MSK with MBS session ID and the corresponding key ID are delivered to the UEs that has joined the multicast session. The MBSF shall also send the new MSK with MBS session ID and its key ID 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 MBSTF. The key update request message shall include the MBS session ID. If the MBSTF has generated a new MTK, the MBSTF 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 [102]. 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.

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

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

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 W.4.1.3 of present document.

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