**3GPP TSG-SA3 Meeting #106-e *S3-220294-r1***

**e-meeting, 14 - 25 February 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** |  | **Current 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 |  | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** |  | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Samsung | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** |  | | | | |  | ***Date:*** | | | 2022-01-25 |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***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:*** | | There may be MBS sessions which are not protected at the service layer, but at the application layer or may not be protected (for example, Free-To-Air). If security protection to be applied, then MBSF creates and provides MBS security context to the UE via the SMF. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | For CP procedure, if security protection to be applied for a MBS session, then MBSF creates and provides MBS security context to the UE via the SMF, otherwise MBS security context is not created. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Ambiguity exist in the specification without proper information on MBS traffic protection handling. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | W.4.1.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

*\*\*\*\*\*Start of Change\*\*\*\*\**

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 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 [102].

The MBSF determines whether security protection to be applied or not for the MBS session based on locally configured policy or based on the information provided by the AF. If security protection to be applied, then the MBSF creates the multicast session security context by generating 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.

Upon receiving the MSK from the MBSF, 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 [102]. 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 obtain the multicast session security context. Absence of the multicast security context indicates that security protection is not applied for the MBS session. The SMF shall provide the multicast session security context to the UE, if received from the MB-SMF and the UE is authorized to use the required multicast service. The UE uses the received MTK, if available, 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 [103]. 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 [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 Change\*\*\*\*\**