**3GPP TSG-SA3 Meeting #103-e *draft\_S3-211632-r2***

**e-meeting, 17 – 28 May 2021 revision of S3-211632**

**Source: Huawei, HiSilicon**

**Title: Update to the solution 11**

**Document for: Approval**

**Agenda Item: 5.11**

# 1 Decision/action requested

***This pCR proposes update to the solution 11 in TR 33.850.***

# 2 Rationale

The figure and UE identifier are updated to address the editor’s note.

# 3 Detailed proposal

SA3 is kindly requested to agree to the below pCR to TR 33.850.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* First Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 6.11 Solution #11: Update the keys used to protect the MBS traffic

### 6.11.1 Introduction

This solution addresses Key issue #2 to update the keys to protect the MBS traffic. The MBS traffic is protected between MBSF-U and UEs. The basic idea is to use the signalling messages for the key update procedure. The UEs, which belong to a multicast group, acquire the same group keys as in the MBSF-U. The security protection is enabled in service layer.

### 6.11.2 Solution details



Figure 6.11.2 -1: Procedure for MTK update

1. The UE registers to 5GS and establishes a MBS session, during which MBSF-C generates MTK1&KID1 and distributes them to MBSF-U and UEs. MTK1&KID1 are used to protect the MBS traffic. Details can be found in solution 3 or solution 8.

2. MBSF-C subscribes to the UDM/UDR on the changes of the multicast information including the authorization information. The UDM/UDR notifies the MBSF-C when the authorization for a UE to join the multicast service/application is revoked. The MBS Session ID and UE info (i.e. GPSIs, number of UEs) are included in the notification. The MBS Session ID may be a Temporary Mobile Group Identifier (TMGI) or a multicast address. UE info indicates the change of authorization info.

3. MBSF-C triggers the MTK update based on the changes of authorization info or the key lifetime of MTK1. MBSF-C generates MTK2 and KID2 for this MBS session. For example, if the number of UEs whose authorization is revoked reached the threshold, the MBSF-C triggers the MTK update. It’s operator’s choice to decide the policy for different event.

4-5. MBSF-C distributes MTK2, KID2 and MBS Session ID to (MB)-SMF and MBSF-U respectively.

6. (MB)-SMF distributes MTK2, KID2 and MBS Session ID to the authorized UEs in the connected state whose MBS sessions are not released. Confirmation for update notification is responded to (MB)-SMF. With the confirmation info, (MB)-SMF determines to activate MTK2 based on local policy. For UEs in idle or inactive state UEs, the updated key are delivered when UE joins or actives the MBS session.

7. If the procedure to update the key in UE side is finished, (MB)-SMF indicates MBSF-U to activate the MTK2 for the corresponding MBS session.

8. MBSF-U uses MTK2 and KID2 to protect the MBS traffic.

The above text describes the security handling when SMF and MB-SMF are co-located. If SMF and MB-SMF are deployed separately, MBSF-C distributes MTK2, KID2 and MBS Session ID to MB-SMF. Afterwards, MB-SMF distributes MTK2, KID2 and MBS Session ID to the authorized UEs via SMF. MB-SMF indicates MBSF-U to activate the MTK2

### 6.11. 3 Evaluation

This solution addresses Key issue #2 to update the key for protecting the MBS session. The solution protects the MBS traffic between MBSF-U and UEs.

MBSF-C decides to trigger the MTK update procedure based on the changes of authorization info or the key lifetime of MTK. The new MTK and KID are sent to UE and MBSF-U respectively.

The key update procedure by (MB)-SMF to the UEs requires UEs in connected state that joined the MBS session to get an SM NAS message. The signalling overhead are needed for message transmission from (MB)-SMF to the UEs.

This doesn’t require idle or inactive state UEs to transition to the connected state to receive the key update.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of pCR\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*