**3GPP TSG-SA3 Meeting #104e-Ad-hoc draft\_S3-213529-r1**

**e-meeting, 27 - 30 September 2021** *revision of S3-21xxxx*

**Source: Qualcomm Incorporated**

**Title: Update to Solution #12**

**Document for: Approval**

**Agenda Item: 5.3**

# 1 Decision/action requested

***This contribution proposes an update to solution #12***

# 2 References

[1] TR 33.850 v.0.7.0

# 3 Rationale

MBSF-U is changed to MBSTF to make it aligned with the SA2 architecture.

A change in the overview is made to indicate that this solution also addresses the KI #1 based on the UE authentication by the MBSTF.

Other editorial changes are made.

# 4 Detailed proposal

It is proposed that SA3 approve the below pCR for inclusion in the TR 33.850 [1].

**\*\*\*\*\* START OF CHANGES \*\*\*\*\***

## 6.12 Solution #12: Protection of MBS traffic at service layer based on GBA

### 6.12.1 Solution overview

This solution addresses Key Issue 1, 2 and 3 to protect the MBS key and traffic at service-layer. This solution leverages the MBMS security architecture specified in TS 33.246 [3].

### 6.12.2 Solution details

In order to receive an MBS service, the UE establishes a secure connection with the MBS service function and obtains security materials



Figure 6.12.2-1: Message flows for MBS key delivery and MBS traffic protection

0. The UE is registered to 5GS.

1. The UE requests a PDU session establishment or modification to receive an MBS service.

2. The UE establishes a secure connection with MBSTF based on GBA similar to MBMS [3] or AKMA [5]. In both scenarios, MBSTF is considered an AF and UE and MBSF-U communicate using Ua/Ua\* protocol. Both the UE and MBSTF derive Multicast User Key (MUK) from the AF key (e.g., Ks\_(int/ext)\_NAF for GBA or KAF for AKMA). Over the secure connection, the UE and MBSTF performs authentication and key derivation as specified in TS 33.246 [3].

NOTE: The key management function is located in the MBSTF as in BM-SC [3].

3. The UE receives the Multicast Service Key (MSK) from the MBSF-U. The MSK is protected using the MUK and delivered using a unicast message over the secure connection.

4. The UE receives the Multicast Traffic Key (MTK) protected using MSK from the MBSTF. The MTK can be delivered either a unicast or a multicast message. The MTK is used as a root key to derive application/protocol specific keys to protect (e.g., encrypt or integrity protect) MBS service traffic.

5. Using the MTK received in step 4, the UE derives application/protocol specific keys and decrypts or verifies the MBS traffic.

The key hierarchy, rekeying and key usage for MBS traffic protection is illustrated in Figure 6.12.2-2 and Figure 6.12.2-3. The MUK derived either based on GBA or AKMA is used to protect MSKs, and each MSK is used to protect MTKs. MBSF-U decides to trigger the MSK/MTK update procedure based on the changes of authorization info or the key lifetime. MSK rekeying is done over unicast to each UE joined to the MBS PDU session, and MTK rekeying is done over unicast or multicast to UEs joined to the MBS session.

NOTE: When GBA is used, MUK derivation follows as specified in TS 33.303. When AKMA is used, MUK is set to KAF based on AKMA key derivation.

Editor’s Note: Use of AKMA for MUK rekeying requires further explanation

Editor’s Note: When AKMA is used, how MBSTF obtains the authorization information is FFS



**Figure 6.12.2-2 Usage of MSK for a single session or a channel**



**Figure 6.12.2-3 Usage of MSK for multiple sessions or channels**

### 6.12.3 Solution evaluation

This solution reuse the LTE MBMS security architecture, both GBA and AKMA are used to protect the MBS key and traffic at service-layer.

This solution addresses Key issue #2 and 3 to protect the MBS key and traffic at service-layer.

MBSF-U 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 MBSTF respectively. The MSK update procedure by MBSTF to the UEs incurs overhead proportional to the number of UEs in connected state that joined the MBS session. The user plane messages need to be delivered to those UEs when a MTK change happens.

**\*\*\*\*\* END OF CHANGES \*\*\*\*\***