**3GPP TSG-SA3 Meeting #103-e *S3-211812***

**e-meeting, 17 - 28 May 2021** Revision of S3-21xxxx

**Source: Qualcomm Incorporated**

**Title: EN resolution of Solution #12**

**Document for: Approval**

**Agenda Item: 5.11**

# 1 Decision/action requested

***This contribution proposes to address an EN in Solution #12.***

# 2 References

[1] TR 33.850 v0.5.0

# 3 Rationale

This contribution proposes to address an EN in Solution #12.

# 4 Detailed proposal

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

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

### 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 MBSF-U based on GBA similar to MBMS [3] or AKMA [5]. In both scenarios, MBSF-U is considered an AF and UE and MBSF-U communicate using Ua/Ua\* protocol. Both the UE and MBSF-U derive Multicast User Key (MUK) from the AF key (e.g., Ks\_(int/ext)\_NAF for GBA or KAF for AKMA).

Editor’s Note: the details of authentication protocol between UE and MBSF-U is ffs.

Editor’s Note: It is FFS whether the key management function needs to be separated from MBSF-U or not.

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 MBSF-U. 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.

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

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. 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.



**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**

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