**3GPP TSG-SA3 Meeting #103-e *S3-211714r2***

**e-meeting, 17-28 May 2021**

**Source: Apple**

**Title: New solution on key distribution**

**Document for: Approval**

**Agenda Item: 5.11**

1 Decision/action requested

***It is proposed to add a new solution in MBS TR 33.850.***

2 References

[1] 3GPP TR 33.850: " Study on security aspects of enhancements for 5G Multicast-Broadcast Services (MBS)"

3 Rationale

This pCR proposes a new solution on the key delivery in service layer.

4 Detailed proposal

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

6.X Solution #X: Secure key delivery in service layer

6.x.1 Solution overview

This solution addresses Key Issue #3: Security protection of key distribution, which includes the security requirement as “The distribution of the keys for protection of MBS traffic between the key generator and the UE shall be confidentiality, integrity and anti-replay protected.”

As the NAS confidentiality protection between AMF and UE is not mandatory and it is not always enabled. Whenever there is no NAS confidentiality protection, KMBS will be sent in the clear, which is a huge damage for MBS service. That’s the motivation to design this solution. For the case when the NAS confidentiality protection is enabled, the protection in this solution is optional but also no harm to enable.

This solution proposes a method to protect the KMBS used for MBS traffic protection based on KMBS-UE which is derived based on KAUSF. With this solution, KMBS delivery from MB-SMF to UE can be confidentially protected.

6.x.2 Solution details



**Figure 6.x.2-1. The procedure of key delivery of KMBS**

The procedure is described as follows:

Step 0a: UE initiates the Primary Authentication and establishes the KAUSF with AUSF in HPLMN.

Step 0b: Service announcement procedure, following the current Clause 7.1.1 in TS 23.247.

Step 1. MB-SMF generates KMBS and KID for the specific MB service.

Step 2. To join the multicast group, the UE sends the PDU Session Modification Request (MBS Session ID). MBS Session ID indicates the multicast group that UE wants to join.

Step 3.0. AMF sends MBS Key Request to AUSF to ask for the encryption key.

Step 3.1. AUSF generates a KMBS-UE using KAUSF and TMGI.

 Editor’s Note: it's FFS how AUSF knows TMGI

Step 3.2. UE generates a KMBS-UE and using KAUSF and TMGI.

Step 3.3. AUSF send the KMBS-UE to AMF.

Step 4. By using Nsmf\_MBSSession\_Create request (MBS Session ID), SMF interacts with MB SMF to retrieve multicast QoS flow information of the indicated MBS session.

Step 5. MB-SMF sends the KMBS and KID to SMF using Nsmf\_MBSSession\_Create response.

Step 6. SMF responds to AMF through Nsmf\_PDUSession\_UpdateSMContext response(N2 SM information (PDU Session ID, MBS Session ID, MB-SMF ID, multicast QoS flow information, updated PDU Session information, mapping between unicast QoS flow and multicast QoS flow information), N1 SM container (PDU Session Modification Command, KMBS and KID)

Step 7. AMF send the PDU session modification command (EKMBS-UE(KMBS)) to UE, including the encrypted KMBS and KID.

Step 8. UE decrypt the EKMBS-UE(KMBS) and gets the KMBS

KMBS is used for the future protection of the MBS traffic.

 Editor’s Note: It is FFS whether the KMBS will be used as the root key or the session key.

 NOTE: The UE leaving group procedure will be handled separately.

 Editor’s Note: Whether other keys (e.g Kamf) can be used is FFS.

 Editor’s Note: What algorithms should be used is FFS.

6.x.3 Solution evaluation

TBD

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