**3GPP TSG-SA3 Meeting #105-e draft\_S3-214150-r5**

**e-meeting, 8 - 19 November 2021** *revision of S3-21xxxx*

**Source: Qualcomm Incorporated, Huawei, HiSilicon**

**Title: 5G MBS key management**

**Document for: Approval**

**Agenda Item: 4.15**

# 1 Decision/action requested

***This contribution proposes a clause for 5G MBS key management***

# 2 References

[1] 3GPP TS 33.246: " Security of Multimedia Broadcast/Multicast Service (MBMS) "

[2] 3GPP TS 33.501: " Security architecture and procedures for 5G system"

# 3 Rationale

The key for a particular MBS session (or MBS service) that should be delivered to the UE over unicast message is the MSK according to TS 33.246. Based on the MSK, the UE obtains the MTK that is used for multicast traffic protection over multicast, where the MTK is protected using MSK and delivered to the UEs in the multicast group using the MIKEY packet. In control-plane key generation and delivery, the MSK should be generated by the MSFT and delivered to the UE when the UE joins the multicast session. Additionally, the current MTK may also be delivered to the UE along with the MSK. Such MBSF based key generation and delivery is shown in the Figure 1.

It is also described that the MBSTF generates the MTK and distributes the MTK as the MTK should be generated by the entity that processes the traffic and hence should be able to determine the key refresh (i.e., the MTK refresh in this case) depending on the amount of the traffic that has been protected using the MTK. When the MBSTF generates a new MTK, it sends the new MTK to the MBSF so that MBSF can provide the MSK and the current MTK to the UE who joins the MBS session.

With such modification, only Point-to-Multipoint part is executed over the user-plane.

This architecture and procedure would also support the co-existence with the user-plane approach that is specified in TS 33.246 [1].



MBSF

Via NAS

MB-SMF

SMF

AMF

MSK

MTK

{MSK, MTK}

Figure 1. 5G MBS key management for CP and UP co-existence

# 4 Detailed proposal

It is proposed that SA3 approve the below pCR for inclusion in the draft CR to TS 33.501 [2].

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

### X.4.1 Key derivation, management and distribution

For security protection of MBS traffic, control-plane procedure and user-plane procedure are optionally supported in service layer. The multicast security policy between UE and RAN shall be not needed to avoid redundant protection.

#### X.4.1.1 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.

The MBSF generates 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.

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 [xx]. 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 retrieve the multicast session security context. The SMF shall provide the multicast session security context to the UE if the UE is authorized to use the required multicast service. The UE uses the received MTK 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 [yy]. 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 [xx]. 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.

#### X.4.1.2 User-plane procedure

The UE registers to the MBS service and receives the MBS traffic as specified in TS 33.246 [xx] with the following changes.

* MBSTF takes the role of the BM-SC in TS 33.246 [xx].
* The UE authenticates to the MBSTF based on the GBA as in MBMS security (see TS 33.246 [xx]) or based on the AKMA (see TS 33.535 [yy]). When the AKMA is used, the MRK is derived from the KAF as specified in Annex F of TS 33.246 [xx] by replacing the Ks\_NAF for the GBA\_ME run with KAF. Furthermore, when the AKMA is used, the MUK is set to KAF.

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

X.4.2 Protection of the traffic transmission

The actual method of protection may vary depending on the type of data being transmitted, e.g. media streaming application or file download. Clause 6.6.2 and clause 6.6.3 in TS 33.246 [xx] apply to the protection of streaming data and protection of download data, respectively.

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