**3GPP TSG-SA3 Meeting #101-e draft\_S3-202921-r1**

**e-meeting, 9 – 20 November 2020**

**Source: ZTE**

**Title: Update solution#3 in TR 33.850**

**Document for: Approval**

**Agenda Item: 5.11**

# 1 Decision/action requested

***This contribution proposes to update the solution#3 .***

# 2 References

*(Reference - in list form - should be made to previous related SA3/3GPP/etc. documents.)*

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

# 3 Rationale

In the step 2, how to generate MTK and the associated key identifier (KID) for the MBS application. This contribution proposes to add an Editor’s note to the solution#3 and correct some editorial mistakes.

# 4 Detailed proposal

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

## 6.3 Solution #3: MBS Traffic Protection

### 6.3.1 Solution overview

This solution addresses both KI#2 and KI#3.

According to TR 23.757 [2], in the baseline architecture 2, the MBSU (Multicast/Broadcast Service User plane) is defined as a new entity to handle the payload part to cater for the service level functions and management; Similarly, MSF User Plane (MSF-U) in baseline architecture 1 is also defined. Also the MBSF (Multicast/Broadcast Service Function) is defined as a new entity to handle the signalling aspects; similarly, MSF Control Plane (MSF-C) in baseline architecture 1 is also defined.

In this solution, MBS traffic is protected between the MBSU/MSF-U in the operator domain and the UE, and it is transparent to the content provider. MBS Traffic Key (MTK) is generated by MBSF/MSF-C and distributed to the UEs through the control plane. MBSU/MSF-U uses the MTK to protect the MBS traffic before sending them out to the UE.

### 6.3.2 Solution details

In the procedure below, (MB-)SMF is the enhanced SMF that supports MBS.

NOTE X: (MB-)SMF is either the MB-SMF defined in the baseline architecture 2 or the enhanced SMF in the baseline architecture 1, as defined in the TR 23.757 [2] on 5G MBS.



**Figure 6.3.2-1: Authentication and authorization procedure**

1. The AF of the content provider provisions to the MBSF/MSF-C the information on the MBS application including the security policy. The NEF is involved in the provision if the content provider belongs to a 3rd party.
2. If the security policy indicates the MBS application needs security protection, MBSF/MSF-C shall generate a MTK and the associated key identifier (KID) for the MBS application. MBSF/MSF-C provisions the received information on the MBS application and the generated MTK and the KID to the UDM/UDR.

Editor’ Note: How to generate the MTK and KID is FFS

1. UE sends a request to use the MBS application. The request is forwarded to the (MB-)SMF. According to the TR 23.757 [2], there are two ways for step 1, the control plane join and the user plane join. For the control plane join, the UE initiates the request for a PDU session establishment/modification and includes in the requires the identifier for the MBS application. The request is forwarded to the (MB-)SMF through the control plane. For the user plane join, the UE sends an IGMP/MLR message to a UPF including the identifier of the MBS application. The UPF forwards the IGMP/MLR message the (MB)-SMF.

Editor's note:  The identifier for the MBS application is to be aligned with SA2 progress.

1. If the (MB-)SMF does not have the subscription data already, the (MB-)SMF sends a request for the subscription data to the UDM/UDR.
2. The UDM/UDR replies with the requested subscription and the received MTK in step 2.
3. The (MB-)SMF sends the received MTK and the KID to the UE.
4. The MTK and the KID are delivered to the MBSU/MSF-U from the MBSF/MSF-C.
5. When MBS traffic is received at the MBSU/MSF-U, the MBSU/MSF-U uses the received MTK to protect the MBS traffic. The protected MBS traffic along with the KID are sent to the UE.

The UE uses the received MTK in step 6 to process the MBS traffic.

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