**3GPP TSG-SA3 Meeting #102-e draft\_S3-210487-r1**

**e-meeting, 18th - 29th January 2021 Merger of S3-210487 and S3-210289**

**Source: Qualcomm Incorporated, Huawei, Hisilicon**

**Title: Security for MBS traffic during handover**

**Document for: Approval**

**Agenda Item: 5.11**

# 1 Decision/action requested

***Approve this contribution to resolve an EN in the solution #1***

# 2 References

[1]

# 3 Rationale

This contribution provides a security mechansim to handle MBS security at the RAN during the UE mobility, i.e., Xn-based or N2-based handover. Two handover sceanrios addressed in this contribution are (1) the case that the target RAN node has already created the MBS security context for other UEs that have established the MBS PDU session and (2) the case that the target RAN nodes has not crated the MBS security context. For the first case, the target RAN node provides the MBS security context to the UE in the handover procedure. For the second case, the target RAN node configures DRB(s) for the MBS PDU session that the UE has established via the source RAN node, in the handover procedure.

The related Editor’s Note is deleted.

One typo in 6.1.1 is corrected.

# 4 Detailed proposal

\*\*\* BEGINNING OF CHANGES \*\*\*

## 6.1 Solution #1: protect MBS traffic in transport layer

### 6.1.1 Solution overview

This solution addresses Key Issue 2&3 to support the secure MBS traffic delivery from context provider to multiple UEs through 5GS. The keys for protection of MBS traffic are generated in the RAN nodes and distributed to UEs. The UEs, which belong to a multicast group, acquire the same keys in the RAN node. The security protection is enabled in transport layer.

### 6.1.2 Solution details

UE

(MB-) SMF

AMF

RAN

UPF

UDM

Content Provider

2. Multicast announcement

4.Nsmf PDU session update SMcontext

(multicast\_group\_info)

5.Multicast distribution session check

6.NamfcommunicationN1N2messageTransfer

7.N2 session request

（multicast\_group\_info）

1. UE registration and PDU session establishment

8. generate K\_group, and select the security algorithms

9. RRC reconfiguration request

（key\_ID, K\_group\_enc, K\_group\_int, security algorithms）

10. UE recieves and stores the security info

11. continue with the multicast service initiation procedure

3.PDU session modification request

(multicast\_group\_info)

**Figure 6.1.1-1.The procedure to protect MBS traffic in transport layer**

The procedure is described as follows:

1. The UE registers in 5GS and establishes a PDU session.
2. The content provider announces the availability of multicast using higher layers (e.g., application layer).
3. The UE sends the PDU Session Modification Request. Information about multicast group including identifier of the multicast group, which UE wants to join, shall be sent. Multicast\_group\_ID can be multicast address or other identifier.
4. The AMF invokes Nsmf\_PDUSession\_UpdateSMContext, in which information about multicast group is included. The SMF checks whether the UE is authorized to receive the requested multicast service based on the UE’s subscription information.

Editor’s Note: Step 3&4 need to be revised if SA2 agrees to support UE’s multicast session join/leave operation via UP e.g. IGMP Join/Leave.

1. If MBS context is not available in (MB-)SMF, (MB-)SMF interacts with UDM to check whether a multicast context for the multicast group exists in the system.
2. (MB-)SMF requests the AMF to transfer a message to the RAN node using the Namf\_N1N2MessageTransfer service to create a multicast context in the RAN, if it does not exist already. In addition, the SMF sends a security policy for the multicast service to the gNB via AMF.
3. The N2 session modification request is sent to the RAN, in which information about multicast group and the security policy is included.
4. RAN check whether the MBS security context for this multicast group is available. MBS security context, which is used for MBS traffic protection, includes the key\_ID, K\_group\_enc, K\_group\_int, encryption and integrity algorithms. The key\_ID is the key identifier and associated with the K\_group\_enc and K\_group\_int. K\_group\_enc and K\_group\_int are used for encryption and integrity protection of MBS traffic respectively.

If not, RAN generates K\_group and derives the K\_group\_enc and K\_group\_int. The encryption and integrity algorithms are selected. The MBS security context is stored until all the UEs in the multicast group have left the RAN.

1. The MBS security context is distributed from RAN to UE. The RRC config message further contains the current PDCP COUNT value for the K\_group. If the K\_group is newly created, the PDCP COUNT is set to the initial value (e.g., 0).
2. UE receives and stores the MBS security context for the multicast group.
3. Continue with the multicast service initiation procedure. Then, the UE decrypts and/or checks the integrity of PDCP PDUs sent over the K\_group based on the security policy.

Editor’s Note: The message name and flow may be updated to align with the conclusion from SA2 and RAN WGs.

#### 6.1.2.x Security handling in handover

In handover, if a UE has established an MBS PDU session and the corresponding bearer(s) (i.e., MRB(s)) with the source RAN node, the MRB(s) needs to be handed over to the target RAN node. There are two handover scenarios that need to be considered.

* If the target RAN node has already created an MBS security context for the MBS PDU session that the UE has established with the source RAN node, the target RAN node provides the MBS security context to the UE via the source RAN node.

NOTE: It is possible that the target RAN node creates an MBS security context for the MBS PDU session when it has received a Handover request from the source RAN node.

* If the target RAN node has not created the MBS security context associated with the MBS PDU session, the target RAN node configures the DRB(s) for the MBS PDU session for the UE and provides this configuration information to the UE via the source RAN node. The security activation status of DRB(s) is the same with that of the MBS PDU session.

The above security handling of MBS traffic during the handover is applicable to both Xn-based and N2-based Handover procedures.

### 6.1.3 Solution evaluation

TBD

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