**3GPP TSG-SA3 Meeting #102 *S3-210215r2***

**e-meeting, 18-29 January 2021**

**Source: Apple**

**Title: Modification of solution#1**

**Document for: Approval**

**Agenda Item: 5.11**

1 Decision/action requested

***It is proposed to approve this 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 some modification on solution#1 in TR 33.850. Several ENs are added to highlight some unclear issues:

Editor’s Note: It is FFS what is the security policy for the MBS.

Editor’s Note: It is FFS how the security context is updated before all the UEs leave the RAN.

Editor’s Note: It is FFS how those keys in security context are derived.

In step 9, since the generation method of K\_group is not given, so there is no explanation on why to include PDCP COUNT in the RRC config message. Therefore, the sentence “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).” is deleted.

4 Detailed proposal

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

6.1 Solution #1: Protection of 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 follo¥ws:

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 identifiers.
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. Security policy shall indicate whether confidentiality and/or integrity protection needs to be activated or not for all bearers belonging to that MBS service.
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.

NOTE: The K\_group generation method can be left to implementation.

NOTE: A method for key update is required. Such a method is given, e.g., in Solution (draft\_S3-210462-r2)

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).

Editor’s Note: Inclusion of PDCP COUNT in the RRC Reconfig message requires further explanation.

Editor’s Note: The Relationship between K-group update and PDCP COUNT initialization requires further explanation.

1. UE receives and stores the MBS security context for the multicast group.
2. 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.

Editor’s Note: The support for mobility of UEs is FFS.

6.1.3 Solution evaluation

TBD

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