**3GPP TSG-SA3 Meeting #103-e *draft\_S3-211932-r2***

**e-meeting, 17 – 28 May 2021** Revision of S3-211932

**Source: Nokia, Nokia Shanghai Bell**

**Title: Editor note removal for solution secure framework for key distribution in MBS**

**Document for: Approval**

**Agenda Item:** **5.11**

# 1 Decision/action requested

***Editor note removal and minor update of solution #10 secure framework for key distribution in MBS***

# 2 References

[1] 33.850 Study on security aspects of enhancements for 5G Multicast Broadcast Services (MBS)

# 3 Rationale

The following editor’ note has been captured in SA3#102bis-e meeting in solution #10.

**Observations**:

|  |  |
| --- | --- |
| Editor note in solution#10 | comments |
| 1. Editor’s Note: relationship between joining/leaving the group and key update is FFS. | When a UE joins or leaves the MBS session, then there is no key update needed for any UEs within the MBS group.But when a UE leaves the MBS group, then the current MBS group keys are known to the UE is that is leaving, hence to prohibit the key leakage re-keying of MBS group keys are required. So rekeying token is provided for new key generation. |
| 2. Editor’s Note: Why idle state UE should update the key is FFS. | UEs which are part of the MBS group can be in Idle and may be still listening to the broadcast. So when a UE leaves the MBS group, re-keying is needed to prohibit the key leakage. In this case all UEs in the group MBS group, those who are active as well as idle and listening to the MBS broadcast need re-keying. If Idle UEs are left out in re-keying, then after re-keying they will decode only garbage if listening to MBS. Transition from inactive multicast session to active multicast session is via paging as described in TR 23.757. When any other UE leaving the same MBS group, then rekeying token needs to be shared to all UEs belonging to the group, this is considered as “configuration change” of multicast session. Some UEs could be in idle mode and some could be in connected mode. Idle mode UEs will be paged for the purpose of rekeying token. All Idle mode UEs establish a connection and already connected UEs will receive the configuration change (new rekeying token). |
| 3. Editor’s Note: It is FFS whether a key id is needed between the UE and the RAN to avoid any mis-synchronization while using old and new keys. | Rekeying token identifier and rekeying token list are sent to the RAN from SMF. RAN never passes these rekeying token identifiers to the UE.This identifier is just used between the SMF and the RAN to identify the rekeying token list. Since the UE only receives the rekeying token but not the rekeying token identifier from RAN. There can’t be any mis-synchronization possible between UE and RAN with rekeying token id.Note: As an option, rekeying token id and rekeying token list sent during initial configuration from SMF to RAN, can be simplified by reducing the list to single key. This will avoid key management at RAN. |
| 4. Editor’s Note: In case of combination of PTM and PTP delivery methods, whether same security policy is applied for both MRB and DRB bearers is FFS. | MBS bearer can comprise of MRB(PTM) or DRB(PTP) or combination of both. In case of combination of PTM and PTP delivery methods, security policy applied for both MRB and DRB bearer are different.NOTE: In case of PTM, RAN can use the MBS keys. In case of PTP, RAN can use the AS security keys which is already established and it is unique to the UE.  |

**Resolution:**

It is proposed to delete this editor's note in solution.

# 4 Detailed proposal

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

## 6.10 Solution #10: Secure framework for Key distribution in MBS

### 6.10.1 Solution overview

This solution addresses the key issue #2 “security protection of MBS traffic” and Key issue #3 “security protection of key distribution”.

Encryption key for MBS session is generated at RAN and UE from parmeters like TMGI, multicast group token, rekeying token (needed only when rekeying, otherwise by default it is zero for initial key generation),encryption algorithm and algorithm ID. Integrity key for MBS session is generated at RAN and UE from parameters like Temporary Mobile Group Identifier (TMGI), multicast group token, rekeying token (needed only when rekeying, otherwise by default it is zero for initial key generation),integrity algorithm and algorithm ID.

When UE joins the multicast group identified by the TMGI and its session, after the PDU session establishment, SMF shares the multicast group token, TMGI, Rekeying token list , rekeying token ID to RAN via AMF. Rekeying token list contains many pre-generated re-keying token needed for this particular MBS session. Rekeying ID and respective rekeying token list is stored in RAN for future use. RAN and UE generates independently the encryption and integrity keys for this MBS session.MBS traffic is encrypted, and integrity protected at RAN level. Received MBS traffic is decrypted, and integrity check is performed at UE.

When a UE or few UEs leaves the MBS group, then rekeying token from the stored list in RAN is retrieved. Using this rekeying token, new keys are generated at RAN and UEs in the ongoing MBS session and further sessions, till another member leaves the group.

### 6.10.2 Solution details

Multicast key generation and the procedure to distribution of those keys from network to the UEs belonging to a multicast group identified by TMGI and rekeying procedure is described below in detail.

#### 6.10.2.1 MBS key generation



Figure 6.10.2-1 Key generation at UE and RAN

For the multicast broadcast encryption key generation for traffic KMTenc, the parameters like TMGI (Temporary mobile group identifier), multicast group token, re-keying token (if available, otherwise default value “0” is used), encryption algorithm and encryption algorithm ID are used. For the multicast broadcast integrity key generation for traffic KMTint, the parameters like TMGI (Temporary mobile group identifier), multicast group token, re-keying token (if available, otherwise default value “0” is used), integrity algorithm and integrity algorithm ID are used.

NOTE 1: As long as the “Multicast group Token” is not updated, the security of KMTenc and KMTint depends only on the rekeying token.

Figure 6.10.2-1 shows the key generation at UE and RAN.

(RAN node (Base stations) get the parameters for the key generation from the 5G core network nodes MB-SMF/AMF as detailed in TR 23.757).

#### 6.10.2.2 MBS procedure for key generation and traffic protection

Step 1: UE registers in the PLMN (see clause 4.2.2.2 of TS 23.502) and request the establishment of a PDU session (see clause 4.3.2.2 of TS 23.502). The UE also indicates its capability to receive multicast data over the radio. The AMF obtains information from the UDM whether the UE can join multicast sessions as part of the SMF Selection Subscription data. If so, for direct discovery, the AMF selects an SMF capable of handling multicast sessions based on locally configured data or a corresponding SMF capability stored in the NRF and also indicates the UE's capability to receive multicast data over the radio to the SMF.

Step 2: The content provider announces the availability of multicast using higher layers (e.g., application layer). The announcement includes at least the multicast address of a multicast group that UE can join.

Step 3: To join the multicast group session, steps 4 to 9 as described in TR 23.757 are followed.



Figure 6.10.2.2-1 MBS Procedure for key generation and traffic protection

Step 4: SMF requests AMF to transfer a message to RAN node using Namf\_N1N2Message Transfer service with multicast information along with multicast group token, TMGI, Rekeying token list, Rekying token id etc. Rekeying token list contains many pre-generated re-keying token and corresponding ids needed for this particular multicast group mangement.

NOTE 2: As an option, rekeying token id and rekeying token list sent during initial configuration from SMF to RAN, can be simplified by reducing the list to single key. This will avoid key management at RAN.

Step 5: N2 session request is sent to RAN with multicast related information received from SMF.

Step 6: Rekeying token list is stored in RAN for future purposes (in case of re-keying).

Step 7: RAN generates multicast key hierarchy (both encryption key and integrity key) needed for the traffic as shown in Figure 6.10.2.1-1.

Step 8: RAN shares in an integrity protected and encrypted RRC message, the multicast group token and MBS session ID TMGI to the respective UE. The multicast group token which palys the role of a group master key should of sufficient length for e.g.128bits.

Step 9: UE which joins the session will generate the MBS related keys (both encryption KMTenc and integrity keys KMTint).

Step 10: UPF(MB-UPF) receives multicast PDUs, either directly from the content provider or via the MBSF-U that can manipulate the data.

Step 10a: UPF(MB-UPF) sends multicast PDUs in the N3/N9 tunnel associated to the multicast distribution session to the RAN. There is only one tunnel per multicast distribution session and RAN node, i.e., all associated PDU sessions share this tunnel.

Step 10b: RAN performs the encryption of traffic using encryption key KMTenc and integrity protection by KMTint. RAN selects PTM or PTP radio bearers to deliver the multicast PDUs to UEs that joined the multicast group.

Step 11a: RAN performs the transmission using selected bearer.

Step 11b: Receiving multicast UEs which are part of this MBS session (matching the MBS group ID) will decrypt the traffic using encryption keys and also verifies the integrity check of the packets received.

Figure 6.10.2.2-1 shows the MBS procedure for key generation and traffic protection

NOTE 3: Security policies for PTM and PTP needs to be the same. RAN may decide to switch between PTM and PTP for a UE, if the security policies for PTM and PTP is not the same (e.g. PTM is protected but PTP is not protected), then security may be breached.

#### 6.10.2.3 MBS procedure for re-keying



Figure 6.10.2.3-1 MBS procedure for re-keying

Step 1: If a UE in a Multicast broadcast, is leaving the Multicast group, then respective SMF is informed about the UE leaving the Multicast group and the TMGI. If a UE joins a session, then PDU session estabilishment or modification happens with respective SMF.

Step 2: SMF informs the respective RAN via AMF about a UE leaving an MBS group and initiate a new MBS group management procedure. As one or few UEs leaving the group, same keys can not be used for ongoing MBS traffic.

Step 3: It is also possible that few of the UEs are actively listening to the ongoing MBS session while few of the UEs are in idle mode, may or may not be listening to the traffic. In order to update all the UE which belongs to the new (modified) multicast group, AMF pages the UEs which are in Idle state (which belongs to new multicast group), so that they will listen to the page and further connect to the network. The UEs which have left the multicast group are excluded from the to be paged list.

Editor’s Note: Why idle state UE should update the key is FFS.

Step 4: UEs which were in Idle mode establishes connection to the respective base stations. UEs which were active UEs (already in connected mode) are aligned and will be in connected mode with the respective RAN. So, all the UEs in the MBS group identified by the TMGI under the coverage of a given base station are connected to the base station now.

Step 5: RAN selects the rekeying token from the list already received form SMF, as instructed by the SMF. All the RAN nodes have to select the same rekeying token, so to aid the same rekeying token selection, SMF also would have sent the rekeying token id to the RAN node. It is also option to send the rekeying token to the RAN nodes at this step directly without token id , to avoid sending the rekeying token list upfront.

NOTE: An alternative is to use different rekeying tokens per RAN node indicated by SMF. This would result in different multicast keys (both integrity key KMTint and encryption key KMTenc) at every RAN node.

6

Step 7: New multicast keys (both integrity key KMTint and encryption key KMTenc) are generated at RAN and UE using rekeying token (Procedure shown in Figure 6.10.2.1-1).

Editor´s Note: It is FFS when to activate the new keys at UE and RAN, after rekeying token is delivered.

Step 8: Fresh new multicast keys (both integrity key KMTint and encryption key KMTenc) are generated at UEs using rekeying token.

Note: Rekeying token is never delivered to the UE which left the MBS session and so with older MBS keys, the MBS traffic can’t be decrypted, and integrity protection check will fail.



Figure 6.10.2.3-2 MBS procedure for re-keying token delivery for multiple UEs

### 6.10.3 Solution Evaluation

 TBD

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