3GPP TSG-SA3 Meeting #101-e **S3- 202985**
e-meeting, November 9 - 20 2020

Source:	**Philips International B.V**
Title:	**Key Update Requirement and Solution**
Document for:	**Approval**
Agenda Item:	**5.11**

1 Decision/action requested

This pCR proposes a solution for efficient content key update in TR 33.850.

2 Detailed proposal

KI#2 in TR 33.850 requires the 5GS to support confidentiality protection, integrity protection, and anti-replay protection of MBS traffic. KI#3 in TR 23.757 also requires studying: "How can a UE join/leave (including authorised or revoked to access) a multicast communication service?".

Putting into context both key issues, it is possible to encounter risks and threats such as:

- A content key used to protect the 5MBS traffic is used for a long period of time.
- A device in the group leaves and it should be prevented from receiving new content.
- A device joins and it should be prevented from having access to old content.
- A device in the group is malicious and it should be prevented from injecting fake content.

The above risks and threats require:

1. adapting an existing key issue or creating a new one requiring that the 5GS is capable to update the keys used to protect multicast content.
2. An efficient solution to distribute and update keys used to protect the content so that these keys can be distributed and updated in an efficient manner.

We ask SA3 to kindly consider including the additional two changes in TR 33.850.

- The first change sets a requirement on the need for key update.
- The second change describes an efficient and resilient method for key distribution and update. This is done in the context of existing solution #2.

****** START OF CHANGE 1 ******

Key Issue #3: Security protection of key distribution

5.3.1 Key issue details

MBS introduces the concept of a point-to-multipoint service into a 3GPP system. MBS traffic is delivered from application service provider to multiple UEs through 5GS. To securely transmit data to a given set of users, the MBS traffic needs to be protected to mitigate the potential attacks. As the security fundamental basis, the keys for protection of MBS traffic are required.

Compared with UE keys, the keys for protection of MBS traffic are one-to-many keys. When UE joins the MBS session, only authorized users are able to receive the keys delivered from the key generator for protection of MBS traffic. UEs might also leave an MBS session or be compromised.

5.3.2 Security threats

If the keys for protection of MBS traffic are not confidentiality protected, an attacker may use the 3GPP network to gain "free access" of MBS services.

If the keys for protection of MBS traffic are not integrity or anti-replay protected, the authorised users may not be able to acquire the MBS traffic properly.

If the keys for protecting the MBS traffic cannot be updated, then:

- If a device in the group leaves, the device might be able to access the content after leaving,
- If a device joins the group, the device might be able to access previous content,
- If a device in the group is malicious, the device might be able to inject fake content.

5.3.3 Potential security requirements

The distribution of the keys for protection of MBS traffic between the key generator and the UE shall be confidentiality, integrity and anti-replay protected.

The 5GS shall be able to update the keys used to protect the MBS traffic.

**** END OF CHANGE 1 ****

**** START OF CHANGE 2 ****

Solution #2: protect MBS traffic in service layer

6.2.1 Solution overview

This solution addresses Key Issue 2&3 to support the secure MBS traffic delivery from context provider to multiple UEs through 5GS. In the baseline architecture 2 in TR 23.757 [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 in service layer. This solution protects the MBS traffic between the MBSU/MSF-U in the operator domain and the UE. It is independent to the protection in the application layer from the content provider.

The keys for protection of MBS traffic are generated in the SMF. Afterwards, the keys are distributed to UEs and MBSU/MSF-U respectively. The UEs, which belongs to a multicast group, acquire the same keys in the MBSU/MSF-U. The keys can be updated in an efficient way.

6.2.2 Solution details

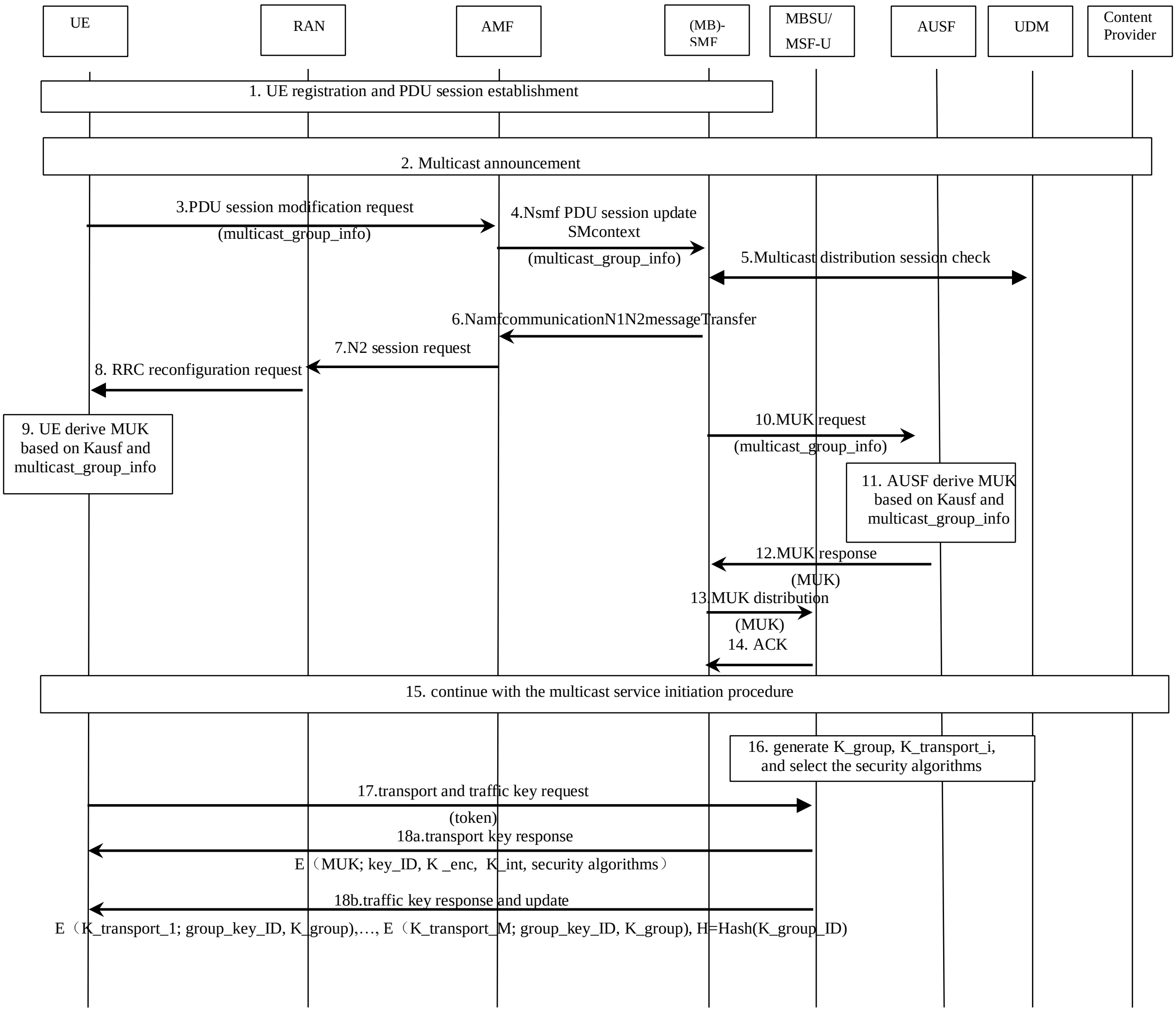
UE
RAN
AMF
(MB)-SMF
MBSU/ MSF-U
AUSF
UDM
Content Provider
1. UE registration and PDU session establishment
2. Multicast announcement
3.PDU session modification request
(multicast_group_info)
4.Nsmf PDU session update SMcontext
(multicast_group_info)
5.Multicast distribution session check
6.NamfcommunicationN1N2messageTransfer
7.N2 session request
8. RRC reconfiguration request
9. UE derive MUK based on Kausf and multicast_group_info
10.MUK request
(multicast_group_info)
11. AUSF derive MUK based on Kausf and multicast_group_info
12.MUK response
(MUK)
13.MUK distribution
(MUK)
14. ACK
15. continue with the multicast service initiation procedure
16. generate K_group, K_transport_i, and select the security algorithms
17.transport and traffic key request
(token)
18a.transport key response
E（MUK; key_ID, K _enc, K_int, security algorithms）
18b.traffic key response and update
E（K_transport_1; group_key_ID, K_group),…, E（K_transport_M; group_key_ID, K_group), H=Hash(K_group_ID)

Figure 6.2.2-1.The procedure to protect MBS traffic in service layer

The procedure is described as follows:

1. The UE registers 5GS and establishs 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 identifer 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.

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.

5. 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.

6. (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. IP address of MBSU/MBS-U may be included if needed for UE to find MBSU/MBS-U,

7. The N2 session modification request is sent to the RAN.

8. RAN sends RRC reconfiguration request message to UE.

9. If UE is allowed to access the MBS service, UE derives Multicast User Key (MUK) from Kasuf and Multicast_group_ID is used as input parameter.

Editor's Note: MUK derivation is FFS.

Editor's Note: Key update procedure after reauthentication is FFS.

10. SMF requests MUK and sends Multicast_group_ID to AUSF.

11. AUSF derives Multicast User Key (MUK) based on Kasuf and Multicast_group_ID.

12. AUSF responds to SMF with MUK.

13. SMF distributes MUK to MBSU/MSF-U.

14. MBSU/MSF-U receives and stores the MUK. Afterwards, ACK is reponded to SMF.

15. Continue with the multicast service initiation procedure.

16. MBSU/MSF-U checks 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 used to indicate which key pair is used. K_group_enc and K_group_int are used for encryption and integrity protection of MBS traffic respectively.

    If not, MBSU/MSF-U generates K_group and derives the K_group_enc and K_group_int. The encryption and integrity algorithms are selected.

17. UE calculates token based on MUK and requests traffic key to MBSU/MSF-U.

Editor's Note: Token construction is FFS.

18. MBSU/MSF-U verifies the token using MUK and distributes the MBS security context to UE if succeeded.

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

Editor's Note: Roaming aspect is FFS.

6.2.2.1 MBS Security content for efficient group key distribution and update

This section explains the logic of step 18a and 18b in Figure 6.2.2.1. using two approaches:

Default approach:

The default version uses key hierarchy:

MUK -> K_group

Step 18a relies on K=K_group, i.e., this message is used to directly update K_group by means of MUK. If K_group needs to be updated and the group size is N, this approach requires the exchanged of N messages.

In Step 18a, E{K1;K2} means authenticated encryption of key K2 with key K1 and is used to indicate the secure delivery of K2.

Communication optimized approach:

Alternatively, a key hierarchy" MUK -> K_transport_i-> K_group" can be used. This alternative is useful to decrease the communication overhead to roughly 2 SQRT(N). In this approach, a multicast group with N members is divided into M disjoint sets S_i of UEs with i={1,…,M}. Each set has roughly L ~ N/M UEs.

Each UE has three keys: a device specific key, MUK; a transport key K_transport_i shared with other L-1 devices in the same set S_i; a group key shared with all N devices and used to protect the MBS traffic. The MUK is used to securely deliver transport keys in a point-to-point connection. The transport keys are used to securely deliver the group key. The key hierarchy is as follows where the arrow indicates protection.

MUK -> K_transport_i -> K_group

The distribution and update of the group key is done by means of two messages:

- Message 18a: in this meassage, K=K_transport_i and is used to provide UE with the key transport for the set it belongs to protected with the UE's MUK.

  Upon reception, a UE first verifies the message authentication code, and if it is correct, it decrypts its transport key. Freshness can be achieved in multiple ways. For instance, an increasing initialization vector can be used that depends on the initial access token exchanged in Step 17.

- Message 18b: the new group key is distributed by protecting it with the transport keys in a point-to-point or in multicast messages. The hash of the new group key H is included in this message.

  Upon reception, a UE first searches the part of the message that is addressed to its set. For instance, if the UE belongs to set z, the UE needs to look for E{K_transport_z; K_group}. Then, the UE verifies the message authentication code, and if it is correct, it decrypts the new group key. Freshness can be achieved by using the same freshness counter as used for the distribution of MBS traffic. Finally, the UE also checks whether the hash of the decrypted key equals the hash H of the group key that is appended at the end of this message.

These two messages 18a and 18b can be combined to address different situations:

1. Initial key distribution to a UE: the UE is provided its transport key and the group key in a same message combining 18a and 18b.

2. Key update triggered by a too long usage of key group: Message 18b is used to distribute a new group key to all UEs.

3. Key update triggered by a new device joining the group: Message 18a is used to deliver the corresponding transport key to the new UE. Then, Message 18b is used to distribute a new group key to all UEs.

4. Key update triggered by a UE leaving/being revoked: If a UE leaves or is revoked, its transport key associated to its set and the group key are compromised. To deal with this situation, Message 18a is sent to the L-1 in its set to update the transport key. Afterwards, message 18b is used to distribute a new group key to all UEs.

This approach is efficient and resilient as follows:

- the update of the group key due to a device leaving the group only requires L – 1 + M messages instead of N that would be required when only point-to-point messages are involved. For instance, if N=1600, M=40, L=40, then the key update only requires 39 point-to-point messages for the update of the transport key associated to the set of the device that is leaving and 40 messages for the group key update. This choice is good since the total number of messages is minimized when L=M=SQRT(N). Another choice might be M=1 so that there is a single transport key or M=N so that there are N transport keys.

- Since M transport keys are used, an attacker that compromises a UE can only try to update the group key and inject fake MBS traffic affecting up to L-1 devices. This limits the impact of such an attack, in particular, compared with a situation in which a single key is used to transport the group key where N-1 would be affected. Furthermore, the hash of the group key is included in Message 18b so that devices in other sets can check the consistency, detect the attack, and inform the 5MBS. In this sense, this solution is resilient as long as the attacker does not manage to capture at least M devices, one per set.

6.2.3 Solution evaluation

TBD

6.X

****** END OF CHANGE 2 ******