3GPP TSG SA WG3 Security — S3#36 **S3-040922**
November 23 - 26, 2004
Shenzhen, China

Source: CCSA/ZTE Cooperation

Title: Efficient Solutions of MSK update

Document for: Discussion and decision

Agenda Item: MBMS

1 Introduction

In SA3#34 meeting, the key management for MBMS is discussed and the update procedures of MSK which are defined in TS 33.246 v 6.0.0 can be described simply as follows. MSKs are encapsulated in MIKEY messages which are protected by MUKs and sent over ptp bearers from BM-SC to UEs. BM-SC use different MUK to create different MIKEY messages for different UEs. For example, in a group including *n* users, BM-SC needs to create n MIKEY messages and do encryption operation for *n* times when BM-SC performs the procedures of MSK update. This contribution discusses two solutions which can reduce the overload of BM-SC when performing the MSK update.

2 Principle of solutions

For the security of MBMS, MSK update should be performed when users leave or join MBMS because the only update of MTK can not address the security requirement R5c that is described in section C.4 of TS 33.246:

R5c: *The UE and MBMS key generator shall support the operator to perform re-keying as frequently as it believes necessary to ensure that:*

- *users that have joined an MBMS User Service multicast service, but then left, shall not gain further access to the MBMS User Service without being charged appropriately*
- *users joining an MBMS User Service shall not gain access to data from previous transmissions in the MBMS User Service without having been charged appropriately*
- *the effect of subscribed users distributing decryption keys to non-subscribed users shall be controllable.*

The events which will trigger MSK update can be classified with three groups: users joining, users leaving, and other events. When MSK update is triggered by users joining, MSK_{old} which is shared by all old users and BM-SC can be used to protect the MIKEY message in which new MSK_{new} is carried from BM-SC to all old users. Meanwhile, the MSK_{new} is sent to the new joining users in

MIKEY message which is protected by MUK shared by new user and BM-SC. By this means, the overload of BM-SC can be reduced when BM-SC performs MSK update which is triggered by users joining. For example, if one user joins a MBMS group which includes n old users, BM-SC needs to perform n+1 encryption operation when using solution in TS 33.246 v 6.0.0. The number of encryption times can be reduced to 2 if the MSK_{old} is used to protect the new MSK_{new}.
In section 3, we will give more details about our solutions.

3 Details of solutions

If the MSK_{old} is used to protect MIKEY message in which MSK_{new} is carried, the MIKEY message can be transmitted over ptp bearers or ptm bearer. In this section, we will introduce the details of these two solutions.

3.1 transmit over ptp bearers

When MSK update procedure will be performed, BM-SC firstly judges the type of the event that triggers the MSK update. If MSK update is not triggered by users joining, BM-SC will perform the procedure defined in the specification TS 33.246. Otherwise, if MSK update is triggered by user joining, BM-SC will operate as follows.
BM-SC creates MIKEY messages that are protected by MSK_{old} for old users and MUK for new users. These MIKEY messages are transmitted over ptp bearers as defined in the specification. The MIKEY messages which are protected by MUK are created in the same way described in the specification, while the MIKEY messages which are protected by MSK_{old} and transmitted by ptp bearers are different from the corresponding MIKEY messages in the specification. Following, some differences are discussed.

1) Extension Payload (EXT)
The IDs of the involved keys are kept in the EXT to enable the UE to look up the identity of the key which was used to protect the message and which key is delivered in the message. So for the MIKEY message which is protected by MSK_{old}, the EXT contains both the ID of the MSK_{old} used to protect the delivery, and the ID of the MSK_{new}.

2) Replay protection
There is already a counter to protect MIKEY message created by MUK. The counter can also be used to perform replay protection for MIKEY message that is created by MSK_{old} and sent over ptp bearers.
BM-SC sets the value of Timestamp Payload according to counter related to per UE for MSK delivery. After receiving the MIKEY messages the Data Type field of the common MIKEY header (HDR) is examined, and if it indicates an MSK delivery protected by MSK_{old}, the MSK_{old} ID is extracted from the Extension Payload. UE must have the ability to get the value of counter associated with MUK which is used to protect MSK_{old}, so that UE could perform replay check.

This solution can efficiently reduce the overload of BM-SC when the BM-SC performs MSK update procedure triggered by user joining. And most changes are resided on BM-SC while few changes are needed on the UE. UE must have the ability to get the counter associated with MUK from MSK_{old} ID and know that the MIKEY message is protected by MSK_{old}.

3.2 transmit over ptm bearers

MIKEY messages created by using MSK_{old} can also be transmitted over ptm bearers. The logical architecture can refer to the MIKEY message in which MTK is carried. MIKEY RAND payload should be added to MIKEY message. One counter should be added to all UEs for MSK ptm delivery protected by MSK_{old}, so that replay protection can be provided.
This solution can reduce not only the overload of BM-SC but also the consumption of network resource.

---

4. Proposal

Two solutions introduced in this paper are efficient to reduce the overload when BM-SC performs MSK update procedure triggered by user joining. We think that the use of these solutions together with solution in the specification is an efficient way to reduce the overload of BM-SC. We propose that SA3 consider the solutions.