3GPP TSG SA WG3 Security — S3#36 **S3-041023**

23 - 26 October 2004

Shenzhen, China

Title: **MBMS MSK management**

Source: **Samsung Electronics.**

Document for: **Discussion and Approval**

Agenda Item: **6.20**

Work Item: **MBMS**

1 Introduction

As defined in current TS33.246 MBMS security, for UE management mechanism of the MSKs received, “if the UE receives an MSK and already contains two other MSKs under the same Network ID and Key Group ID, then the UE shall delete the older of these two MSKs.” This mechanism does not work for MBMS download service. During SA3#35 meeting, one alternative mechanism related to the usage of MTK ID was proposed to support keeping more than 2 MSKs at UE at the same time. This contribution gives more detail analysis about this mechanism compared to current MSK management mechanism. Section 2 describes the limitation of current mechanism, section 3 analyses the increase of MTK ID and its impact to BMSC and UE, Section 4 and 5 describes the 2 different cases to manage the MSK according to proposed mechanism.

2 Limitation of current MSK management mechanism

For MBMS download service, one possible application scenario is that the multiple MSKs may be delivered consecutively after the content is received. Thus, if the UE deals with these multiple keys received according to the above mechanism, it is clear that under the same Network ID and Key Group ID, the UE shall only keep the latest 2 MSKs, and delete all older MSKs even without using them. Thus, the UE shall not be able to use these older MSKs to obtain the corresponding useful MTKs. So, current MSK management mechanism cannot work correctly for MBMS download service.

And even for streaming service, current MSK management mechanism also limits the BMSC operation. Since the UE shall remove the older one of the two MSKs saved when it receives the one new MSK under the same Network ID and Key Group ID, BMSC has to wait to send out the new MSK until the old one of the 2 MSKs saved is no longer used, even though the BMSC may generate this new MSK long time ago and the network finds that it is beneficial to disperse the MSK delivery procedure over this longer period, considering the network resources.

Thus it is concluded that current MSK management mechanism should be changed to support keeping more than 2 MSKs at UE at the same time.

3 Increase of MTK ID

MTK ID is 2 bytes long and it is used to distinguish MTKs that have the same Network ID, Key Group ID and MSK ID. For BMSC transmission, the MTK ID is increased by 1 every time the corresponding key is updated. However, because data loss can always occur, UE may miss some of the MTK updating. Thus, for UE receiving, it is stated that if SEQp (i.e. MTK ID from the newly received MIKEY message) is equal or lower than SEQs (i.e. MTK ID saved) then the MGV-F shall indicate a failure to the ME. And if SEQp is greater than the SEQs, the UE shall carry out the further MAC calculation operation. So, for UE receiving, the corresponding MTK ID is not necessarily increased by 1 every time it received one MTK updating.

So, for the MTK updating initiated by the BMSC, if the BMSC increases the corresponding MTK ID more than 1 compared with the last MTK delivery, there is no any impact to the UE's operation. As for BMSC operation, simply to increase the MTK ID more than 1 seems not to be one big impact to BMSC either.

4 Delete the MSK when it is used

It is quite natural that one MSK should be deleted by the UE when it is already used and shall not be used any longer. Because the only use of MSK is to protect the delivery of MBMS Transport Keys (MTKs), which are then used to secure the MBMS Transport Services, UE should delete one MSK when this MSK cannot be used to protect the MTK delivery any longer. Actually the UE can know whether one MSK can be used to protect the MTK delivery any longer by the use of MSK Key Validity Time. The Key Validity Data subfield, which is present in the KEMAC payload for MSK transmission, defines the Key Validity Time for MSK in terms of sequence number interval (i.e. lower limit of MTK ID and upper limit of MTK ID). So, if the MTK ID of one MTK protected by one MSK reaches the upper limit defined for this MSK, this MSK cannot be used to protect the MTK delivery again and the UE may delete this MSK.

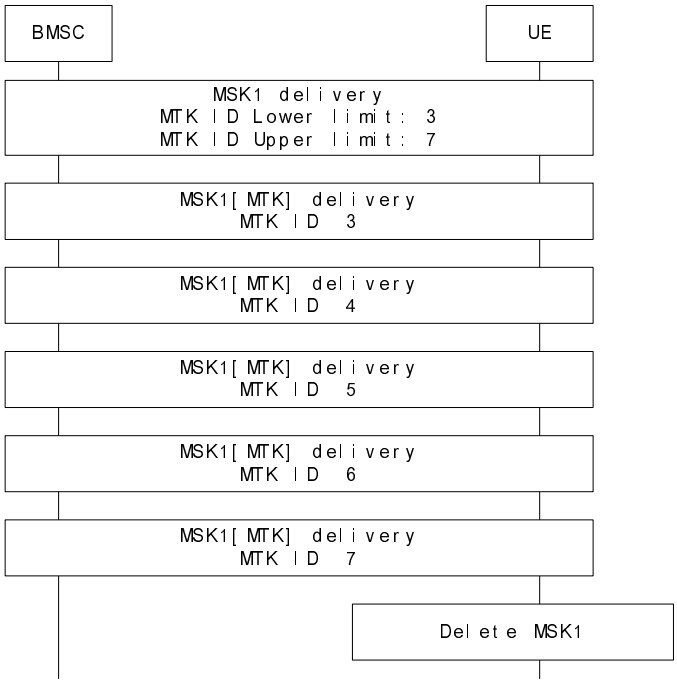

Fig.1

Refer to fig.1, when BMSC delivers MSK1 to UE, it sets the lower limit of MTK ID and upper limit of MTK ID of the MSK1 to 3 and 7. Then BMSC delivers MTKs with the MTK ID from 3 to 7 to UE with the protection of MSK1. When the MTK ID reaches the upper limit 7, UE shall delete the MSK1.

5 Delete the MSK immediately

It is possible that BMSC may wish to stop the use of one MSK immediately even before it is fully used. Since for UE receiving, the MTK ID from the MIKEY message for MTK delivery is not necessarily increased by 1, the BMSC can simply send out the last valuable MTK with the MTK ID increased directly to the upper limit instead of increased by 1.

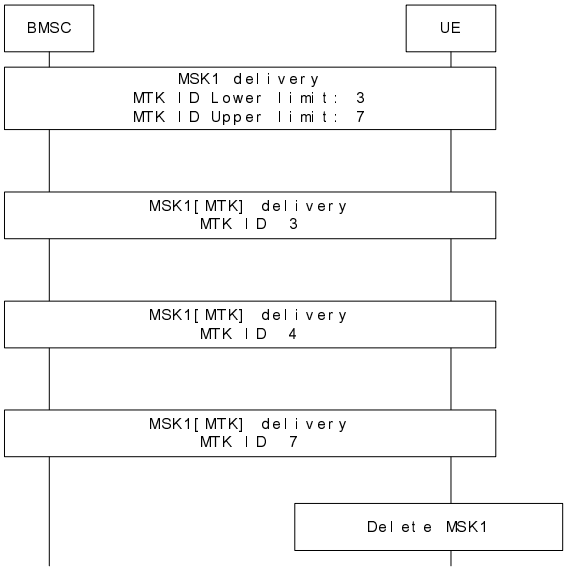

Fig.2

Refer to Fig.2, when BMSC delivers MSK1 to UE, it sets the lower limit of MTK ID and upper limit of MTK ID of the MSK1 to 3 and 7 respectively. Then BMSC delivers MTKs with the MTK ID from 3 to 4 to UE with the protection of MSK1. Then BMSC decides to stop the use of MSk1 immediately. Thus BMSC sends out the last useful MTK with the MTK ID 7. When UE detects the MTK ID reaches the upper limit 7, UE shall delete the MSK1 after obtaining this last MTK. By this method, the BMSC can instruct the UE to delete the MSK immediately.

6 Conclusion and Proposal

It is proposed to agree on the MSK management principles as following:

“The UE shall delete one MSK when the corresponding MTK ID of one MTK whose delivery is protected by this MSK reaches the upper limit defined in the Key Validity Data subfield present in the KEMAC payload when this MSK is distributed. To stop the use of one dedicated MSK immediately, BMSC may set the MTK ID of one MTK to the upper limit when the corresponding MTK is updated.”

The accompanying CR implements the change in the TS.