**3GPP TSG SA WG3 Security — S3#32** **S3-040034**
**09 - 13 February 2004**
**Edinburgh, Scotland, UK**

**Agenda item:** 6.20 MBMS

**Title:** high level key update

**Source:** Huawei Technologies Co., Ltd.

**Document for:** Discussion and Decision

# 1 Introduction

The BM-SC controls when the high level keys used in a multicast service are to be changed, and BM-SC will send a "new key available" message to the UE, if this message is send to all UEs, then all UEs may request the new key at the same time. This contribution suggests a UE requests a new key base on some rules in order to avoid a high number of simultaneous requests.

# 2 Discussion

At the last SA3 meeting ,it was clarified that there are two keys for each multicast services. When the high level keys used in a multicast service are to be changed, the BM-SC send a "new key available" message to UE. If all UEs receive the "new key available" message and determine that they don't have the new key, the UEs will request the new key from BM-SC. If all UEs request the new key simultaneously, the burden of network is huge. The follow suggestion can solve this problem .

When the UE join the multicast service , the BM-SC provides some rules to the UE such that subsequent requests for a new key are made according to the rules. E.g. the BM-SC assign a time interval to the UE, and at the end of each time interval, the UE checks whether it needs to request the new key. If the UE receives a "new key available" message and the time reaches the end of the time interval, the UE requests the new key. The time interval may be same to each UE but because the time that each UE joins is different , the start point of the interval is different , so the simultaneous requests are avoided.

# 3 Conclusion

When a UE joins the multicast service, the BM-SC gives some rules to UE. The UE requests the new high level key base on those rules when it needs the new high level key .

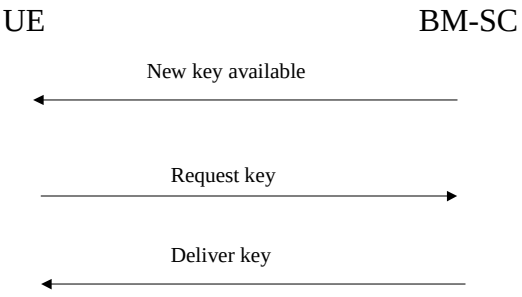
Include the following changes in the TS.

**********Begin of changes**********

## 6.2 Key update procedure

Once a UE has joined a multicast service, the UE should try to get the high level key that will be used to 'protect' the data transmitted as part of this multicast service. If the UE fails to get hold of this key or receives confirmation that no updated key is necessary or available at this time, then, unless the UE has a still-valid, older key, the UE shall leave the MBMS user service. The UE tries to get the high level key using the second message in the below flow.

The BM-SC controls when the high level keys used in a multicast service are to be changed. The below flow describes how the high-level key changes are performed.




The first message is sent out by the BM-SC to indicate that new keys are available. It is an optional message in the flow. If it is sent to all UEs~~, then it needs to be ensured that all the UEs do not request the new key simultaneously.~~, then the BM-SC should provide the rules to UE for subsequent request for the new key when a UE joins a multicast service, to avoid simultaneous requesting from all the UEs. For example, the UE should request the new key base on a time interval provided by the BM-SC.

The second message is used to request a key. This is sent by the UE when it either receives the first message in the flow and does not have the new key, has just joined a multicasts service and does not have a key for that service or a UE has received some protected content which it does key that was used to protect the content. If the UE fails to get hold of the updated key or receive confirmation that no updated key is necessary or available at this time, then, unless the UE has a still valid older key, the UE shall leave the MBMS service.

After receiving the second message the BM-SC should send out the appropriate key to the UE protected by the relevant means. Upon successfully receiving the new key, the UE should store this key for later use.

Editor's note: MIKEY is being considered as the method for carrying keys. Possible optimisations were proposed at the ad-hoc in Antwerp (S3z030010). One identified issue was the possible need to terminate MIKEY in the UICC and/or terminal in the combined method. The use of MIKEY relates to the PTP delivery of a key

**********End of changes**********