3GPP TSG SA WG3 Security — S3#33 **S3-040444**
10 - 14 May 2004
Beijing, China

Title: LS on MBMS MSK key update
Reply to: n/a
Release: Rel-6
Work Item: MBMS

Source: SA3
To: SA4
Cc: SA2

Contact Person:
Name: Huang Yingxin
Tel. Number: +86-10-82882752
E-mail Address: **huangyx@huawei.com**

SA3 has discussed MSK update in the SA3#33 meetings. In the current procedure, an optional message "new key available" is sent to UE. If it is sent regularly and simultaneously to all UEs, using point to multipoint transmission, for efficiency reasons, the BM-SC should provide the rules to the UE for subsequent request for the new MSK when a UE joins a multicast service, to avoid simultaneous requests from all the UEs.

About what rules should be set to UE, there are some discussion in SA3. The key lifetime and the delay time are two potential rules.

1. Key lifetime: associated with key, before the key lifetime is expired the UE need request the new MSK. If the UE request the new key before the key lifetime is expired, there also need the other mechanism to avoid the congestion (e.g. random time spread over the lifetime).

2. Delay time: BM-SC spread the delay time randomly over an acceptable maximal delay interval. When UE join the service, the BM-SC provides the delay time to UE. When UE receive the "New key available" message, the UE request the new MSK according this delay time. The delay time also can be change at any point to point communication between UE and BM-SC.

The common part of the two methods is that a random time interval is necessary for the UE to initiate the MSK request in a congestion avoidable way. There can be 2 different ways for the generation of the random time.

1. Based on information already contained in the UE i.e. delay according to algorithm with a parameter such as the UE id as input

   Delay time generated in the UE: The UE should determine what time it should request the new key and avoid the impact with other UEs, so can not reliably avoid the congestion. The advanced algorithm may help mitigate the problem, but need more complexity and more computing in the UE. The disadvantage is that the operator is not able to ensure that a group of specific customers for a service obtain the key within a defined time period as the actual delay may depend on a parameter not in immediate control of the operator

2. Based on information signalled to the UE from the BM-SC at some previous point to point communication

   Delay time generated in the BM-SC: the main work will be at BM-SC. The BM-SC don't need to manage more additional UE information, only the random delay time should be provide to UE. The BM-SC can control the maximal delay time to ensure the UE with the longer delay time can get new key in time.

According the above analysis, the random time is needed anyway. From the view of operator control, saving the resource and reduce requirements to UE, the random time generate in BM-SC is desirable.

The lifetime of key also reasonable in some case, but it can't use independently for the key update. The proper way out may be the delay time as solution, and the lifetime as complementary if needed.

These solutions avoid congestion at the BM-SC during key update. SA4 and SA2 are kindly asked to comment on the solutions above or to suggest an alternative solution.

2. Actions:

To SA4:

SA4 are kindly asked to comment on the solutions above or to suggest an alternative solution.

3. Date of Next TSG-SA3 Meetings:

SA3#34	July 6-9, 2004	Acapulco, Mexico
SA3#35	October 5-8, 2004	Malta
SA3#36	November 23-26, 2004	Shenzhen, China