3GPP TSG SA WG3 Security — S3#33 **S3-040245**
10 - 14 May 2004
Beijing, China

Agenda item: MBMS

Source: Samsung

Title: MBMS MSK distribution procedure

Document for: Discussion and Decision

1. Introduction

In this contribution, we propose to come to an agreement on the overall MBMS MSK distribution procedure and capture it into current TS.

2. MSK distribution considerations

Con-1: Not explicitly for MBMS but also for other services, for security reason, it is always desirable not to give out the security related key (i.e. MBMS Service Key for MBMS) too early before it is actually used. For MBMS, the network (i.e. BMSC) may prefer to give out the MSK only one period $P_{Distribution}$ (e.g. 6 hours) before it is actually used. This $P_{Distribution}$ may be assigned by the BMSC considering the security issues as well as the time need for MSK updating to all joined UEs.

Con-2: It is assumed that the ptp MSK distribution shall be carried out for each UE with the protection of MUK (MBMS User Key), no matter whether UE requests for the first key or whatever following key updated. And usually this kind of ptp MSK distribution for each UE may consume considerable resources. From the discussions in previous meetings, it was believed that the initial MSK distribution to UE (i.e. first application level joining procedure[1]) can be joined with the UE's bearer level joining procedure to avoid setting up additional ptp bearer for MSK distribution.

Con-3: During last SA3#32 meeting, SA1's LS indicated that from the end user's point of view, it was beneficial if he can join the service at any time after the service announcement. One common joining procedure for all UEs who asks for joining at any time seems give the user good feeling. The period from the time when one UE joins the service at bearer level to the time when service starts may be quite long.

Con-4: For MBMS download service, one example scenario as overnight download news service was discussed over the email reflector, where an operator download using MBMS an audio/video news summary to many customers in the night. If a customer wants to listen to /watch the news summary, they need to fetch all the MSKs needed to decrypt the data from the BM-SC. It is good if the MSK distribution mechanism can support this application scenario.

Con-5: For MSK updating, currently it is assumed that one "New Key Available" message may be need to send to one UE or all the UEs. It should be noted that it shall be quite one big burden to the system if it is sent to each UE in ptp mode and the number of UEs is large. But if this message is sent to all UEs in ptm mode, always there may exist UE who may lost this message due to the ptm transmission characteristics. And, this ptm transmission from BMSC directly to UE may input new requirement to other groups (e.g.SA2), no matter it is transmitted as separate control signaling or as in-band signaling.

Con-6: Simultaneously multiple MSK request should be avoided as far as possible.

3. MSK distribution

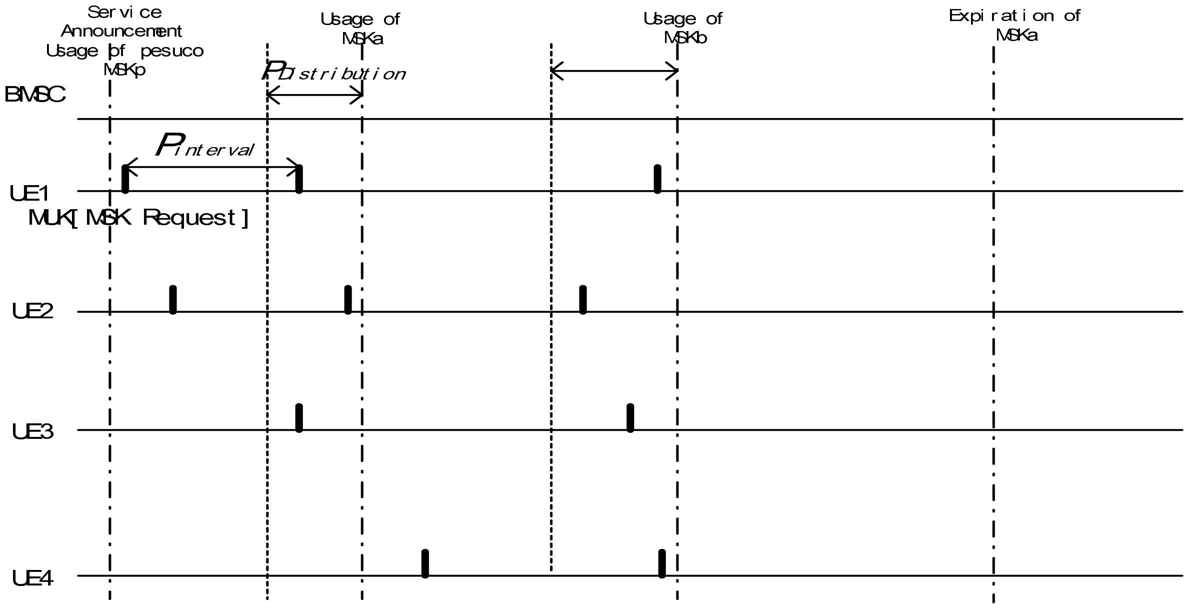

Figure 1 timeline for Service announcement, MSK generation、distribution and implicit expiration

The Figure 1 above gives the timeline for MBMS service announcement, MSK generation、distribution and implicit expiration.

1. Service announcement is first given to users well before service starts.

2. BMSC generates one actual MSK and decides to begin to use it at $T_{MSK\ usage}$. As well, , BMSC decides the period $P_{Distribution}$ ahead of T_{MSK} for this MSK. The BMSC shall not distribution this MSK and thus this MSK is not available for the UE before this $P_{Distribution}$. This $P_{Distribution}$ may be assigned by the BMSC considering the security issues as well as the time need for MSK updating to all joined UEs.[1]

   Before none of the actual MSKs is available, BMSC shall generate and use one pseudo MSK that shall never be actually used indeed (refer to 4). The $P_{Distribution}$ for this pseudo MSK is 0 and its $T_{MSK\ usage}$ is the time when service announcement is made. There's no difference between this pseudo MSK and one actual MSK from UE's point of view[2].

3. After obtaining the Service announcement, the user who is interested in this service may select to join this service at any time as his own will. After bearer level joining is finished[1], UE requests for the MSK at $T_{request}$. [3] This MSK request may be encrypted by MUK for security.

[1] This $P_{Distribution}$ corresponds to the *CON-1*.

[2] This corresponds to the *CON-3*. UE can always obtian keys in the MSK requets procedure after bearer level joining.

[3] This correspond to the *CON-2*. The initial MSK distribution is joined with the UE bearer level joining procedure. No seperate ptp MSK distribution bearer is needed for set up.

4. Receiving the UE's request for MSK, after necessary procedures (i.e. authentication/authorization), the BMSC may decide to distribute one to multiple MSKs[4] together with one request interval $P_{interval}$ to the UE.

   For one specific MSK generated by the BMSC:

   if the $T_{request} >= T_{MSK\ usage}$, this means that this MSK is already in use and the UE asks for this MSK. BMSC may optionally distribute this MSK to the UE if it is not transmitted before;

   If the $T_{MSK\ usage} - P_{Distribution} =< T_{request} < T_{MSK\ usage}$, this means that this MSK shall be used soon and UE asks for this MSK. This MSK shall be distributed to the UE;

   If the $T_{request} < T_{MSK\ usage} - P_{Distribution}$, this means that UE asks for the MSK which should not be distributed at the time $T_{request}$ for security reasons. In this case, this MSK shall not be distributed to the UE. Instead, BMSC shall assign one request interval $P_{interval}$ which makes the $T_{request} + P_{interval} >= T_{MSK\ usage} - P_{Distribution}$. To avoid uplink congestion caused by multiple MSK request simultaneously, the $P_{interval}$ may be different for different UE. Its detail generation mechanism is kept within BMSC, with the principle that that $T_{request} + P_{interval}$ is evenly distributed with the period $P_{Distribution.}$ [5]

   BMSC shall select the minimal $P_{interval}$ of all the $P_{interval}$ values for each MSK and transmit it to the UE.

5. UE performs the next MSK request at the time $T_{request} + P_{interval.}$.[6]

6. BMSC may implicitly make one MSK expired by not using its MSK_ID any longer after a new MSK is used.

4. Conclusion

It is proposed to capture section 3 into current TS as far as is acceptable.

Reference

[1] TD S3-04xxxx Bearer level joining and application level joining for MBMS security, Samsung, SA3#33

[4] This multiple MSK correspond to the *CON-4*.

[5] This different $P_{Interval}$ for different UE corresponds to the *CON-6*.

[6] This $T_{request}$ + $P_{interval}$ corresponds to the *CON-3*. No “New Key Available“ message is needed any more.