3GPP TSG SA WG3 Security — S3#29 **S3-030408**
15 - 18 July 2003
San Francisco, USA

Agenda item: MBMS

Source: Samsung Electronics

Title: Reliable key distribution mechanism

Document for: Discussion and Decision

1 Introduction

One main comment to multicast based key distribution is that UE may miss to receive these keys due to some unpredictable reasons, e.g. poor radio transmission environment. In this case, as one supplemental part to multicast based key distribution, it is proposed that another separate key distribution over the dedicated channel shall be able to be achieved upon the request of this kind of UE.

2 Discussion

During previous meetings, various multicast based key distribution mechanisms have been presented[1][2][3]. One main comment for multicast based key distribution mechanisms is that users may miss the key distribution due to user movement and/or poor radio transmission environment.

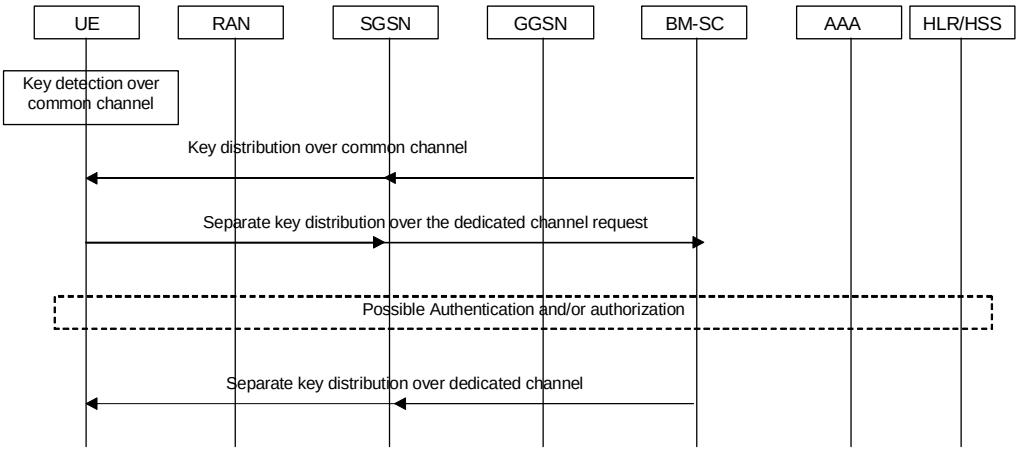
In order to combat these possibilities of key transmission loss, one simple mechanism is that BMSC shall repeat the key multicast transmission for several times. This makes it possible that one user who miss the key distribution at the beginning may catch it at the last chance. However, it is likely that multicast based key distribution shall take use of the common channel as the same way as MBMS traffic data transmission. Thus, this key distribution reparation over the common channel shall bring some extra load to this channel. Also, fast power control, which is one efficient way for combating the poor radio transmission environment, is impossible to be adopted for one common channel. One still user, who may reside in the same spot within poor radio transmission environment for some time, shall not be able to receive the keys even though it is transmitted once more and more .

Another possible mechanism to eliminate the possibilities of key transmission loss is to use dedicated channels for key transmission additionally when needed. The dedicated channel, which can be applied with fast power control, can perfectly adapt to the varying environment and eliminate the possibility of key transmission loss. Those users who cannot detect the keys correctly over the common channel shall ask the BMSC for this dedicated key distribution. After possible authentication and/or authorisation,

BMSC may instruct the network to setup dedicated channels for these users and give out the keys over these dedicated channels.

2.1 Time-triggered key distribution

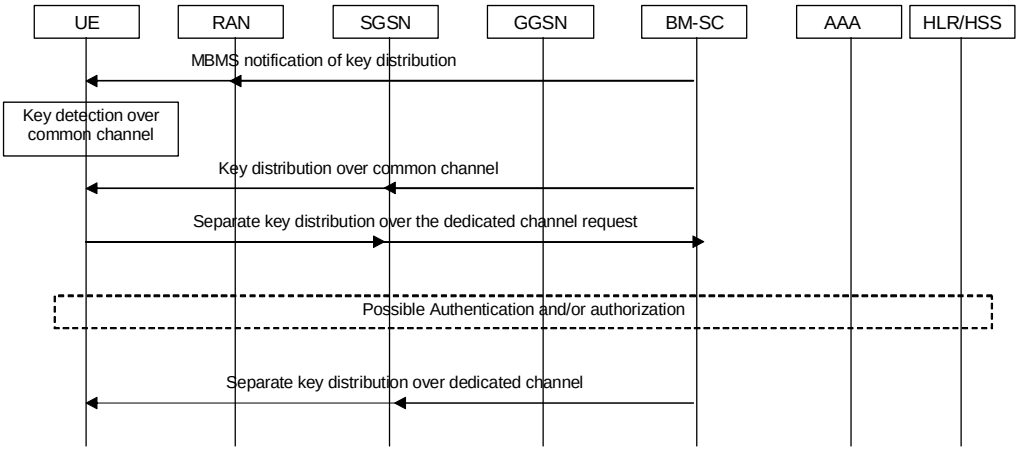
For the time-triggered key distribution, e.g. BMSC shall update the keys and distribute them to the MBMS users every 15 minutes, BMSC and UE shall agree beforehand that key distribution shall be carried out according to some predefined schedules. UE itself shall be able to know when the keys distribution shall likely happen.



1. UE shall listen to the common channel used for key distribution and try to detect the keys according to its estimation of the key-updating interval.
2. According to the predefined schedules, BMSC shall carry out the key distribution over the common channel.
3. If one UE failed to carry out this key reception, it shall notify BMSC to ask for one separate key distribution over the dedicated channel via SGSN.
4. Authentication and/or authorization procedure may be carried out between UE and the network.
5. BMSC shall give the key to this user via the established dedicated channel.

2.2 Event-triggered key distribution

For the event-triggered key distribution, e.g. BMSC shall update the keys and distribute them to the MBMS users whenever one UE joins/leaves the service; it shall be difficult for the other UEs to know when the keys distribution shall likely happen. In this case, some kind of short MBMS notification is needed to paging the UEs about the coming key distribution before it is carried out.



1. Before carrying out the key distribution, BMSC shall notify the UEs about this coming key distribution.
2. UE shall listen to the common channel used for key distribution and try to detect the keys after it gets the MBMS notification in above step.
3. BMSC shall carry out the key distribution over the common channel.
4. If this UE failed to carry out this key reception, it shall notify the BMSC to ask for one separate key distribution over the dedicated channel via SGSN.
5. Authentication and/or authorization procedure may be carried out between UE and the network.
6. BMSC shall give the key to this user via the established dedicated channel.

3 Conclusion

From above analysis, it is proposed that SA3 can agree on the following points and reflect them in the current TS:

- BMSC shall be able to page users for the coming key distribution via MBMS notification;
- UEs who miss the key distribution shall be able to ask for one separate key distribution over one dedicated channel;
- BMSC shall be able to support the point-to-point key distribution as one supplemental mechanism to the multicast based key distribution.

4 Reference

[1] Tdoc S3-030054, Text proposal for MBMS re-keying based on LKH principles, Samsung Electronics

[2] Tdoc S3-030040, MBMS Security Framework, QUALCOMM

[3] Tdoc S3-030257, MBMS PayTV model, Gemplus, Oberthur