3GPP TSG SA WG3 Security — S3#28 **S3-030286**
06 - 09 May 2003
Berlin, Germany

Agenda item: 7.21

Source: Samsung Electronics

Title: Further consideration of LKH for MBMS re-keying

Document for: Discussion

1 Introduction

At the last SA3#27, LKH [1][2] was agreed as one efficient mechanism for MBMS re-keying. However, there is still some dissension [3][4] regarding the use of LKH. This contribution offers some clarification and some further consideration about MBMS LKH for MBMS re-keying.

2 Discussion

The original intention for the introduction of MBMS [5] was to efficiently use the radio/network resources. As stated previously in [1] and [2], the users receiving the same Multicast service within the same area can also be further combined into one (or several subgroups) to make it possible for keys to be given to all users within one subgroup at a time in point-to-multipoint mode. It is commonly understood that LKH is efficient for MBMS re-keying especially with a large number of MBMS users.

2.1 Application Scenarios

According to current MBMS security requirements [6], MBMS re-keying shall be supported to ensure that the MBMS keys are fresh. Basically, the MBMS re-keying can be time-triggered (e.g. these keys shall be periodically updated), or event-triggered (e.g. caused by a user joining/leaving operation), or a combination of these two cases. We agree with Nokia [3] that LKH is efficient in the case of a leaving user/compromised user, i.e. LKH can efficiently serve the event-triggered case.

Furthermore, we believe that LKH can also serve the time-triggered re-keying case. For example when it is time for MBMS Traffic Encryption Key re-keying after a certain time interval and if there is no user leaving/joining operation within one subgroup during this time interval, the MBMS Traffic Encryption Key can be given to all users within this subgroup in point-to-multipoint mode.

Considering the charging issue, it is possible that some high-end users would be authorized by the network operator to utilize the MBMS service continuously, while some others would be authorized for only a certain amount. Thus, the former users consist of one specific subgroup and the updated MBMS Traffic Encryption Key could always be given to all users in this subgroup at the same time in point-to-multipoint mode. In this case, the user-leaving operation would lead to no re-keying in this specific group.

Thus we believe that the efficiency of LKH is more related to the number of MBMS users than to whether MBMS re-keying is event or time-triggered.

2.2 Relationship with charging

In actual fact LKH is an efficient mechanism for MBMS key management and updating. It has no obvious direct relationship with charging. That is to say LKH may be used as long as MBMS key updating is needed.

2.3 LKH Hierarchies and complexity

Compared to point-to-point re-keying, we can see that LKH may have some additional complexity (e.g. definition of additional message formats, some more memory capacity needed both within the UE and BM-SC etc…) whilst offering the benefits of efficiency. As this complexity is closely related to the LKH hierarchies, we can try to simplify the LKH mechanism and eliminate the complexity by reducing the LKH hierarchies to the minimal number needed.

One simplified MBMS re-keying mechanism adopting LKH principles can be illustrated as follows:

As we know, currently in SA2 [7], Temporary Mobile Group Identity (TMGI) is used for group notification purpose. Users belonging to the same group shall share the same TMGI to enjoy the same MBMS service. Point-to-point re-keying shall be adopted within this TMG.

As a working assumption it was implied that there should only be one TMGI for one specific MBMS service. Thus, all MBMS procedures, including BAK framework [4], were related to one specific MBMS service and were accordingly associated with one TMGI.

However, at SA2#31 [8], it was proposed that several different TMGI(s) for one specific MBMS service should be generated to identify different group(s) of MBMS users who share this same MBMS service and accordingly the same MBMS Traffic Encryption Key. Thus, point-to-point re-keying could still be adopted within one TMG without any modification, while the MBMS Traffic Encryption Key can be given to all users who share the same TMGI in point-to-multipoint mode. By these means we believe that, the LHK principles are easily supported with minimal modification to current MBMS procedures that were all associated with the TMGI.

3 Conclusion

It is proposed that SA3 should continue studying applying the LKH principles for MBMB re-keying and also the feasibility of the proposed simplified LKH mechanism for MBMS re-keying.

4 Reference

[1] Tdoc S3-030053, Some consideration about MBMS re-keying across various reference points, Samsung Electronics

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

[3] Tdoc S3-030238, Levels of MBMS key hierarchy, Nokia

[4] Tdoc S3-030197, MBMS re-keying: point-to-point and LKH, QUALCOMM

[5] 3GPP TS22.146, Technical Specification Group Services and System Aspects; Multimedia Broadcast/Multicast Service; Stage 1 (Release 6), version 6.0.0.

[6] 3GPP TS33.246, Technical Specification Group Services and System Aspects; Security; Security of Multimedia Broadcast/Multicast Service; (Release 6), version 0.0.3.

[7] 3GPP TS23.246, Technical Specification Group Services and System Aspects; Multimedia Broadcast/Multicast Service (MBMS); Architecture and Functional Description (Release 6), version 0.4.0.

[8] Tdoc S2-031228, TMGI text proposal, Samsung Electronics