3GPP TSG SA WG3 Security — ad hoc **S3z030019**

3-4 September 2003

Antwerp, Belgium

Source: **Nokia**

Title: **MBMS – Key management requirements comparison**

Document for: **Discussion**

Agenda Item: **6.2**

1. INTRODUCTION

Firstly, this discussion paper provides as an introduction sequence diagrams for different re-keying mechanisms: two-tiered [1], simple point-to-point model [2] and LKH [3]. Different key management requirements [4] are then analyzed concerning these three different mechanisms.

2. RE-KEYING METHODS

2.1 Two-tiered model

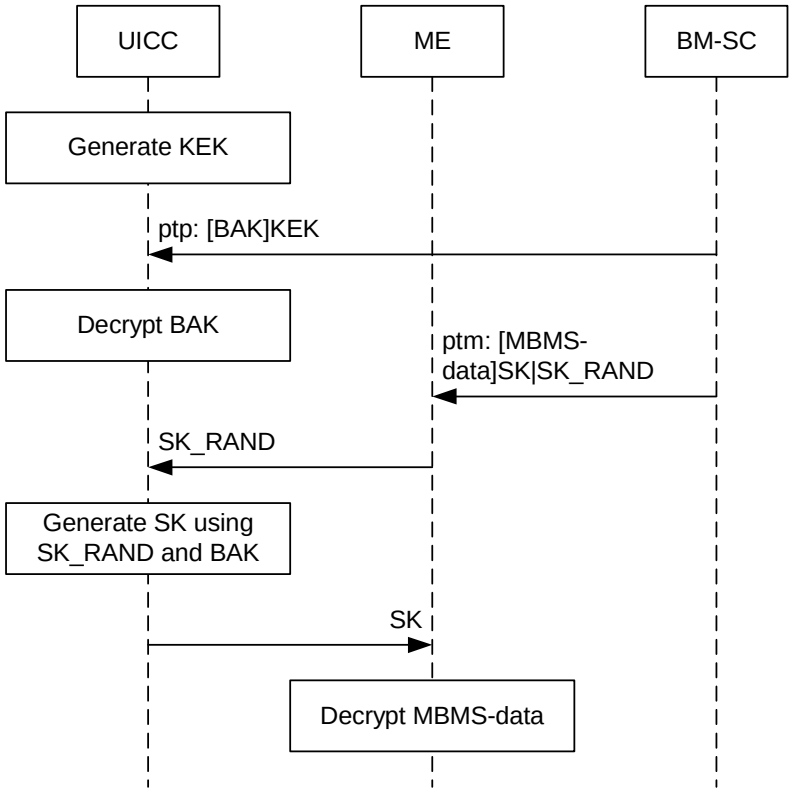

Figure 1 – Two-tiered model sequence diagram

2.2 Simple model

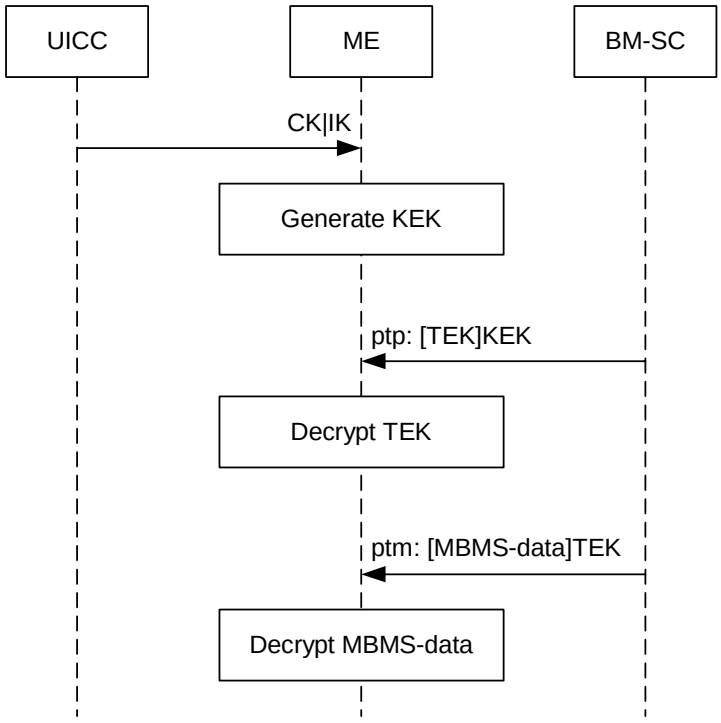

Figure 2 – Simple model sequence diagram

2.3 LKH

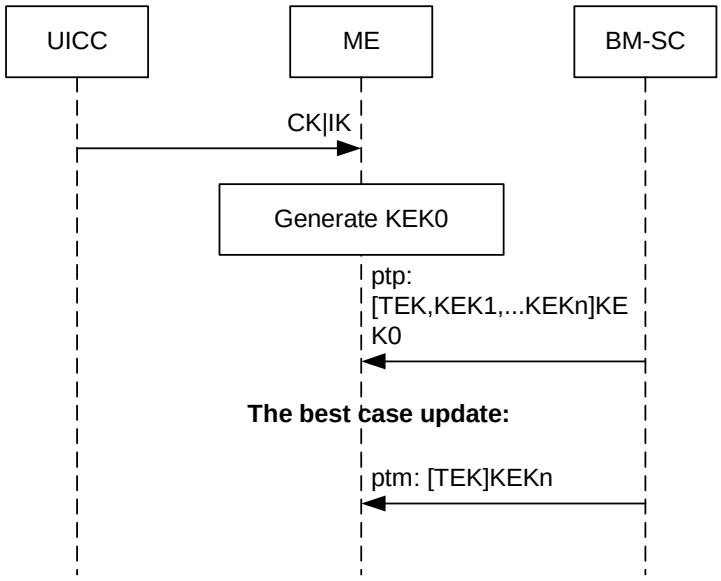

Figure 3 – LKH sequence diagram

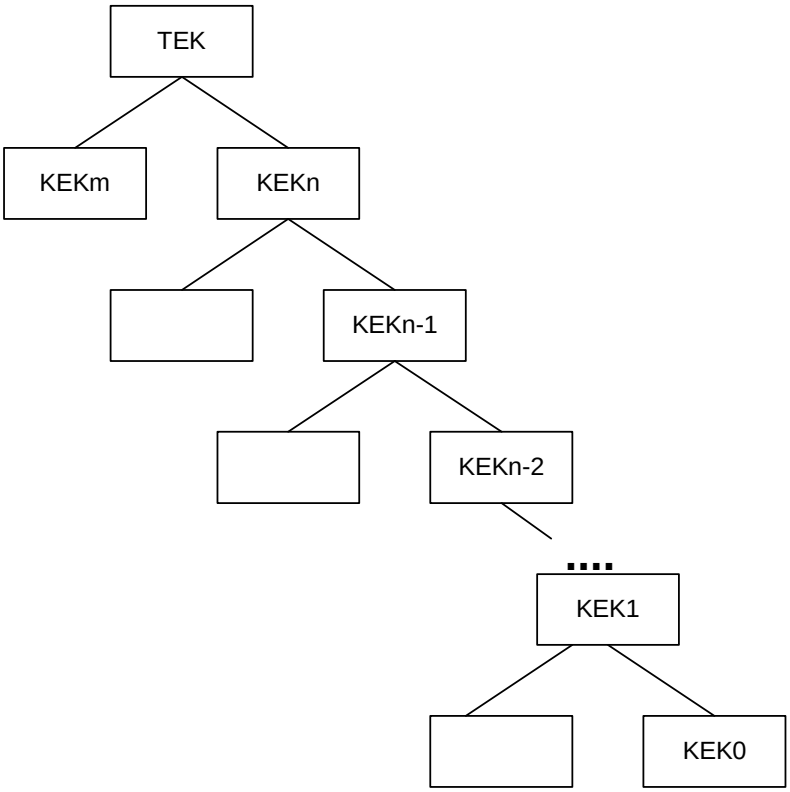

Figure 4 – Levels of key hierarchy in LKH model

3. COMPARISON TABLE

The below table indicates whether these three analyzed models for re-keying satisfy the requirements listed in [4].

Requirement	Two-tiered	Simple	LKH
SA3.1	N/A (bearer encryption is transparent to re-keying)	N/A (bearer encryption is transparent to re-keying)	N/A (bearer encryption is transparent to re-keying)
SA3.2	N/A (bearer integrity protection is transparent to re-keying)	N/A (bearer integrity protection is transparent to re-keying)	N/A (bearer integrity protection is transparent to re-keying)
SA3.3	Yes (it is possible to implement)	Yes (it is possible to implement)	Yes (it is possible to implement)
SA3.4	Yes (ptp for BAK, ptm for SK)	Yes (only ptp)	Yes

SA3.5	Yes (it is possible to implement)	Yes (it is possible to implement)	Yes (it is possible to implement)
SA3.6	Yes (it is possible to implement)	Yes (it is possible to implement)	Yes (it is possible to implement)
SA3.7	Yes (SK_RAND is delivered regulary)	N/A (ptm is not used)	Yes (reliable multicast or repeated multicast messages)
SA3.8	Yes (see also SA3.4)	Yes (see also SA3.4)	Yes (if key leakers can be identified, see also SA3.4)
SA3.9	Yes	Yes	Yes
SA3.10 (Not feasible requirement?)	-	-	-
SA1.1	Yes (it is possible to implement)	Yes (it is possible to implement)	Yes (it is possible to implement)
SA1.2	Yes (it is possible to implement)	Yes (it is possible to implement)	Yes (it is possible to implement)
SA1.3	Yes (it is possible to implement)	Yes (it is possible to implement)	Yes (it is possible to implement)
SA1.4	Yes (key change is not required if someone joins or leaves)	Yes (key change is not required if someone joins or leaves)	Yes (key change is not required if someone joins or leaves)
SA1.5	Yes	No (if very frequent re-keying is needed) or Yes	Yes
SA1.6	Yes (it is possible to implement)	Yes (it is possible to implement)	Yes (it is possible to implement)
SA1.7	Yes (it is possible to implement)	Yes (it is possible to implement)	Yes (it is possible to implement)
SA1.8	Yes (it is possible to implement)	Yes (it is possible to implement)	Yes (it is possible to implement)
SA1.9	Yes (it is possible to implement)	Yes (it is possible to implement)	Yes (it is possible to implement)

4. CONCLUSION

All three alternatives fulfil security requirements. Re-keying method should therefore be decided based on other requirements e.g. implementation cost.

5. REFERENCES

[1] TDoc S3-030360, Levels of Key Hierarchy for MBMS, Qualcomm Europe

[2] TDoc S3-030349, MBMS re-keying: PTP with periodic re-keying, Huawei

[3] TDoc S3-030286, Further consideration of LKH for MBMS re-keying, Samsung

[4] TDoc S3z030002, Key management requirements (results of AP 29/11), Colin Blanchard, BT