3GPP TSG SA WG3 Security – SA3#28 **S3-030238**
6 - 9 May 2003
Berlin, Germany

Title: **Levels of MBMS key hierarchy**

Source: **Nokia**
Agenda item: **7.21**
Document for: **Discussion and decision**

---

1 Introduction

MBMS key hierarchies with many levels have been proposed by various companies for several reasons:
- some keys are user-specific while others are service or even content specific
- it is possible to protect some keys in a better way than other keys
- revocation of keys is easier with deeper hierarchy.

In this contribution we study how valid these reasons are in the MBMS context.

2 Discussion

The nature of the MBMS service (e.g. user occasionally listens in to a multicast transmission) makes it difficult for the network to charge for the exact amount of content that the user has consumed; the network may simply not have any way to find out this data. That is why it is more likely that charging has to be based on a model where the user and the network operator agree beforehand for a certain time unit during which the user is authorized to utilize the MBMS service; the user is paying for this possibility and there is no further counting about how many bits of the content the user actually received. In other words, the flat rate charging is applied at least during the agreed time interval. On the other hand, the time interval may be short, e.g a couple of hours, or it can last longer, e.g. a whole month.

2.1 User leaving service

An important consequence of the above is that there is no point to specify mechanisms that make it possible to renew the keys in case somebody is suddenly leaving the service. This can be handled with dropping the leaving user when the pre-agreed time is at the end. In other words, nobody needs to leave the service: they just do not renew the agreement for the next time unit.

As the main advantage of the Logical Key Hierarchy (LKH) proposed by Samsung (*TDoc S3-030053*) is the more effective management of keys in the case of leaving user/compromised user, this concept does suit well the MBMS case. Indeed, when all the keys need to be renewed anyway, the LKH becomes additional burden to the network (all branches of the "key tree" have to be renewed).

2.2 Key protection level

Another issue is the level of protection of user-specific/service-specific keys: there seems to be no point of maintaining several hierarchies of keys that are similar in both their protection level and their applicability. If we acknowledge the requirement that at least for the first phases of MBMS the service should be available with support from legacy smart cards, there are no MBMS-specific keys in the UICC. This seems to take away the main advantage of the Qualcomm's model (*TDoc S3-030040*). Hence, only the authentication key K and keys derived from that are available for the MBMS. All the rest of the key hierarchy are stored in the ME. This means that no more than three levels of keys are useful in the MBMS context (this conclusion is in-line with Ericsson's proposal, *TDoc S3-030063*):
- user-specific authentication key in the USIM --> K
- user-specific MBMS keys in the terminal (derived from the CK/IK that can leave the USIM) --> KEK
- service-specific MBMS keys in the terminal that are delivered to the user for each time unit that the user agrees to pay for the service --> TEK.

The length of the key validity time interval depends on several factors:
- charging model

- difficulty of leaking out/utilizing the service-specific key
- burden to the system caused by re-keying

but it is important to notice that higher key hierarchy does not have a positive impact on any of these areas.

3 Conclusion

We propose as a working assumption that rekeying is not done in the case that somebody is leaving the service or a key compromise occurs. It is also proposed that a three-level key hierarchy is used.