3GPP TSG SA WG3 Security — S3#29 **S3-030360**
15-18 July 2003
San Francisco, USA

Agenda item:	MBMS Security
Source:	**QUALCOMM Europe**
Title:	Levels of Key Hierarchy for MBMS
Document for:	Discussion

1 Introduction

Security for MBMS relies on a secret key being distributed to many authorized subscribers for the purposes of decrypting MBMS content. This contribution considers whether one or two tiers of symmetric keys are appropriate for content encryption/decryption. Mechanisms for distributing the highest tier of shared key to multiple users are not considered here.

2 Discussion

Ultimately, decryption of the content relies on a common shared-secret key SK being available to terminals of authorized subscribers. Thus, an important issue is to find the balance between updating SK sufficiently frequently (an insecure terminal may publish SK, so this is changed often enough that it is not a cost-effective way for subscribers to access content) while maintaining efficient negotiation of keys with subscribers (to reduce negotiation and overhead on the air interface.)

In 3GPP2, the decision was made to have two levels of decryption keys: the BAK is distributed to authorized UICC in a point-to-point manner. From these BAK and multicasted SK_RAND, short-term keys SK are derived and relayed to the terminal (from the UICC). This provides flexibility to update SK frequently, keeps subscriptions tied to the UICC, and keeps the over-the-air key management costs to a minimum (as BAK need not be changed frequently). The ability to update SK frequently was deemed important because of the likelihood that some terminal may be insecure.

Of course a two-tiered scheme may be deployed in a terminal alone or across the terminal and UICC. Even if MBMS security is initially to be deployed in the terminal only, a two-tiered scheme may be deployed for essentially the same cost than a one-tiered scheme. However, when piracy becomes a concern, operators may begin to issue UICCs supporting this scheme and require them for access to higher value content. Thus the two-tiered scheme affords a future-proof migration path to a secure UICC-based security solution, whereas a one-tiered scheme does not.

The additional cost of the 3GPP2 two-tiered scheme depends on many factors, but we estimate the additional cost to be less than 0.5% of the cost of a one-tiered scheme.

- Unicast key-distribution may take place much less frequently; the BAK keys are sent point-to-point and stored securely on the UICC so that the short term keys may be multicasted.
- There is a small decrease in broadcast bandwidth as random values SK_RAND are transmitted with the encrypted packets, from which SK are derived. The choice of the frequency with which SK_RAND will be sent (eg every packet or every fifth packet) is a trade-off between quality of service and efficiency, but if for example SK_RAND were 4-bytes in length sent every second 512-byte packet, the relative decrease in bandwidth is less than 0.4%.
- There is a small additional processing cost due to frequent generation of decryption keys:
    - Generating the decryption key SK.
    - Initializing the cipher with the new decryption key SK.

3 Conclusion

A two-tiered solution provides the flexibility to change keys SK with whatever granularity is desired, but requiring infrequent over-the-air key management. (The frequency of changes in BAK will depend on how often individual MBMS subscribers will have their subscription to a particular service revoked.) Essentially the two-tiered solution costs little in bandwidth, but saves much of the overhead necessitated by frequent key changes, and allows the option of solutions deployed in terminals alone or based on a UICC.

[1] Broadcast-Multicast Security Framework, 3GPP2 S.P0083 Version 0.5.