3GPP TSG SA WG3 Security — S3#28 **S3-030197**
6-9 May 2003
Berlin, Germany

Title: MBMS re-keying: point-to-point and LKH

Source: **QUALCOMM Europe**

Agenda item: 6.21 MBMS Security

Document for: Discussion

1 Introduction

At S3#27 in Sophia Antipolis a number of proposals were made relating to MBMS security, including those made by QUALCOMM to use the 3GPP2 security framework [5], and Samsung Electronics' proposals [2], [3] to update keys using a Logical Key Hierarchy. This document considers the relationship between these two proposals and provides Qualcomm's view of further work.

2 Discussion

QUALCOMM recently presented the 'BAK' framework adopted by 3GPP2 to provide security for broadcast-multicast services; a component of this solution is the secure point-to-point delivery and update of Broadcast Access Keys between the BM-SC and authorized UE.

At the same meeting Samsung Electronics provided a pair of contributions ([2],[3]) proposing to base MBMS security on a key hierarchy as described in IETF RFC 2627, Key Management for Multicast [4]. Indeed this IETF document describes four strategies for distributing the group keys: Manual (i.e., point-to-point), N Root/Leaf Pair-wise, Complementary Variable, and Hierarchical (or LKH).

In its generality, LKH provides an approach to key provisioning to meet the demands of dynamic, real-time applications, such as 'wargaming, law enforcement, teleconferencing, command and control conferencing, disaster relief, and distributed computing.'

The LKH principles may be applied as a refinement of the BAK security framework, an alternative to distributing the keys in a point-to-point manner.

3 Conclusion

In QUALCOMM's view the LKH proposal is interesting, and it warrants further study. It may have particular application if this security framework is applied to dynamic real-time corporate applications. However LKH will be complex to standardize, while the point-to-point BAK distribution meets the needs of initial consumer applications, such as multicast video.

As there are considerable benefits of harmonization between 3GPP and 3GPP2, and tight timescales required to standardize an MBMS security architecture, SA3 should adopt the point-to-point BAK scheme for Release 6, and later consider such enhancements as LKH functionality if there is a requirement for it.

4 References

[1] 3GPP TS33.246, Technical Specification Group Services and System Aspects; Security; Security of Multimedia Broadcast/Multicast Service; (Release 6), version 0.1.0.

[2] 3GPP S3-030053, Some consideration about MBMS re-keying across various reference points, Samsung Electronics

[3] 3GPP S3-030054, Text proposal for MBMS re-keying based on LKH principles, Samsung Electronics

[4] IETF RFC 2627, Key Management for Multicast: Issues and Architectures, D. Wallner el al.

[5] 3GPP2 S.P0083, Version 0.5, Broadcast-Multicast Service Security Framework

[6] 3GPP S3-030040, Explanation of BAK-based key management, QUAMCOMM