3GPP TSG SA WG3 Security ó SA3#36 **S3-041042**
November 23-26, 2004
Shenzhen, China

Source:	**Ericsson**
Title:	**General comment contribution to MBMS: Feature list to complete MBMS in Release 6**
Document for:	**Discussion and Proposal**
Agenda Item:	**MBMS**

TS 33.246 should be frozen in SA plenary in December 2004. Now when we have seen all the CRs submitted to TS 33.246 it is useful to list the features, which need to be finalised to complete MBMS security in release 6. Some of the listed work may need to be finished within 2005. The list is maybe not exhaustive, and it is proposed that this list is taken as a basis of discussion when deciding if MBMS TS 33.246 should be frozen in SA plenary in December 2004.
Feature list to complete MBMS in Release 6

- Service announcement/discovery
  - SA3 is currently assuming, that service announcement is only send via point-to-point bearers, see Threats in B.1 of TS 33.246. SA4 TS includes possibility to send Service Announcement over MBMS bearer. Protection of Service Announcement over MBMS bearer has not been considered.
  - Confidentiality and integrity protection is indicated today in Service Announcement. It needs to be specified if key management is initiated at all if both confidentiality and integrity protection are turned off.

- GBA bootstrapping
  - GBA bootstrapping initiation request and bootstrapping renegotiation request have not been defined for MBMS application
  - The relations to GBA are missing from MBMS security architecture

- HTTP procedures
  - The contents of HTTP payloads need to be specified
  - Handshake of with SA4 on the security work that needs to be done on stage 3
  - Termination of key management is missing
  - Final decision on the need for SA4 application level joining depends on decision of SA4
  - The protection of post delivery procedures depends on decisions of SA4 (see also LS S3-040907)
  - Possible error cases in HTTP procedures

- MIKEY procedures
  - The handling of MSKs may need some enhancement to cover download services, where the MSK is fetched after the UE has received the encrypted data
  - Possible need for Security policy payload for download
  - Possible error cases in MIKEY procedures
  - Completion of IETF activities for MBMS related MIKEY extensions

- Traffic protection
  - Details of download protection method

- Consistency check security threats ñ> requirements -> functions -> mechanisms
- Editorial check