3GPP TSG SA WG3 Security — SA3#33 **S3-040445**
10-14 May 2004
Beijing, China

Title: **LS on MBMS key Management**
Release: Release 6

Source: SA3
To: SA1, T3, SA4
Cc: -

Attachments: none

Contact Person:

Name: Jorge Abellan Sevilla
Tel. Number: +33 1 46005933
E-mail Address: **jsevilla@axalto.com**

Overall Description

SA3 has analyzed different proposals for MBMS key management. In this context, the following conclusions have been reached:

1) GBA will provide the common security framework for MBMS key management.

This implies that MBMS will require GBA according to TS 33.220 (including the agreed GBA_U functions as available in a CR to TS 33.220 : S3-040413)

GBA secrets will be used in user authentication in MBMS application level procedures (i.e. the application protocols for MBMS User Services joining, leaving and key delivery).

2) It has also been decided that MIKEY protocol with some extensions will be used as the key management protocol for MBMS.

3) It was agreed that the work would continue under the assumption that key management in the UICC and the key management in the ME shall both be supported by the current release.

Based on this, it was agreed that if a terminal supports MBMS, then it shall support both ME and UICC based key management and consequently also the GBA-functions and interfaces required for it (i.e. GBA_ME and GBA_U according to TS 33.220).

However, some companies objected to the keeping of both ME and UICC key management solutions and proposed to have the UICC-based solution only, which was claimed to provide higher security. It was argued that the additional standardization burden that is needed for supporting both solutions was balanced with the benefits of addressing MBMS services to subscribers having pre-Rel6 non-MBMS capable UICCs. It was commented that this decision was not based on security considerations but on service and business requirements.

Actions

Actions to SA1

SA1 are kindly asked to take into account the above considerations and comment whether the assumptions in point 3 are in line with current 3GPP service requirements on MBMS.

Actions to T3

T3 is kindly asked to consider the above agreements and provide the required CRs in the involved T3 specifications to enable GBA_U and MBMS related procedures in the UICC-ME interface.

Actions to SA4

SA4 is kindly asked to consider the above agreements when defining the MBMS service architecture.

Date of Next 3GPP SA3 Meetings

3GPP SA3#34	6 - 9 July 2004	Acapulco, Mexico
3GPP SA3#35	5 - 8 Oct 2004	Malta