
Title: LS on MBMS key Management
Release: Release 6

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

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 (including GBA-U) functions. Based on this, it was agreed that if a terminal is to support MBMS, then the support of GBA-U and related MBMS functionalities is mandated.

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

- 3) GBA is the current working assumption for user authentication and authorization in MBMS application level joining and MBMS application level leaving.

- 4) 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.

However, some companies objected to the keeping of both 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, SA

SA1 and SA are kindly asked to take into account the above considerations and comment whether the assumptions in point 4 are in line with current 3GPP service requirements on MBMS.

Actions to T3

T3 is kindly asked to consider the above resolutions 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 resolutions 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