3GPP TSG SA WG3 Security — S3#33 **S3-040381**
10 - 14 May 2004
Beijing, China

Agenda item: MBMS

Source: Axalto

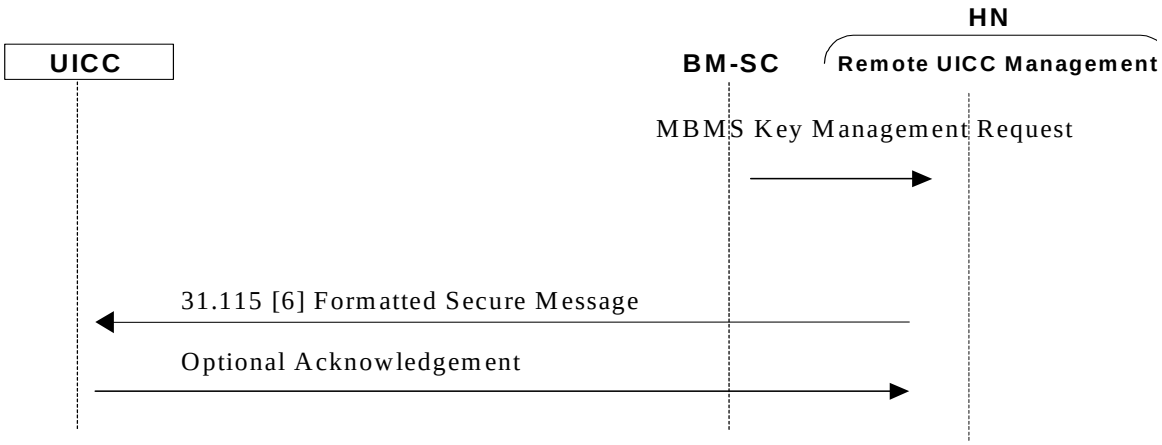
Title: Initial discussion on security requirements in the OTA server interfaces

Document for: Discussion

1. Introduction

At SA3 #32 it was considered that in case OTA solution is chosen for MBMS key Management, "the OTA interface should be standardised (although not necessarily mandated)".

The interface between OTA Servers and the UICC is already standardised in TS 31.116 using security mechanisms defined in TS 31.115 assuring authentication, message integrity, replay detection, sequence integrity and message confidentiality.



The interface between OTA Server and the BMSC should be standardised to assure interoperability between different vendors and an appropriate behaviour in the case where the BMSC is not located in the Home Network.

This interface is used to transfer to the OTA Server the parameters included in a key management request (MBMS identifier, MSK_Id, MSK or $[MSK]_{MUK}$, MTK_SEQ, ...)

It is up to CN4 to define the most appropriate protocol to be run over this interface (e.g. IP & DIAMETER based).

2. Proposal

The following security requirements are proposed as a normative annexe in TS 33.246

Annex C (normative): Security requirements for the interface between the BMSC and the remote UICC management entity (OTA Server) in the home network

This annex contains some security requirements that have identified for the interface between the BMSC and the remote UICC management entity (OTA Server) in the home network.

- Between the BMSC and the OTA Server mutual authentication, confidentiality and integrity shall be provided

NOTE: This requirement may be fulfilled by physical or proprietary security measures if BMSC and remote UICC management entity are located within the same operator's network.

- The MBMS functionality in the OTA Server shall verify that the requesting BMSC is authorised;
- The BMSC shall be able to send a subscriber identification (e.g. IMSI) within the key management request;
- The BMSC shall be able to send the type of key management request (i.e. MSK Update, MSK Deletion, MBMS Subscription, MBMS Un-subscription) within the key management request;
- The BMSC shall be able to send the MBMS keys and associated parameters within the key management request;