3GPP TSG SA WG3 Security — S3#33 **S3-040243**
10 - 14 May 2004
Beijing, China

Source: **Axalto, Gemplus, Oberthur**

Title: **MBMS UICC-based solution**

Document for: **Discussion and decision**

Agenda Item:

Abstract

This contribution describes the MBMS UICC-based only solution.

1. Introduction

At SA3#32 some changes to the UICC-based solution were proposed. This paper describes the new UICC-based solution and presents differences between the UICC-based only solution and the combined solution based on GBA, MIKEY and HTTP_Digest mechanism.

2. Overview of the MBMS UICC-based only solution

2.1. MBMS elements

MBMS Key material: new terminology

At SA3#32 meeting, SA3 agreed to adopt new terminology to have the same key names throughout the different proposals.

- **MTK:** MBMS Traffic Key
  Corresponds to the **SK** (Short-term Key) in previous contributions
  - Session key to encrypt the content to multicast

- **MSK**: MBMS Service Key
  Corresponds to the BAK (Broadcast Access Key) in previous contributions
  - Used to compute/retrieve the MTK
  - Securely stored in the UICC

  MSK and MTK keys are common to all subscribers of an MBMS_Id service.

- **MUK**: MBMS User Key
  Corresponds to the **RK** (Registration Key) in previous contributions
  - An unique key per user

MBMS network entities

To perform the MBMS procedures the following network entities are required:

- **In Home Network**
  - BM-SC
  - MBMS Management Server; this functional entity would be implemented by means of an OTA server.

- **In Visited Network**
  - BM-SC

Interface

- Interface between the BM-SC and the MBMS Management server shall be standardized. This interface is used to transfer data such as the "MBMS Admin data" present in MBMS administrative procedures described further.

MBMS procedures

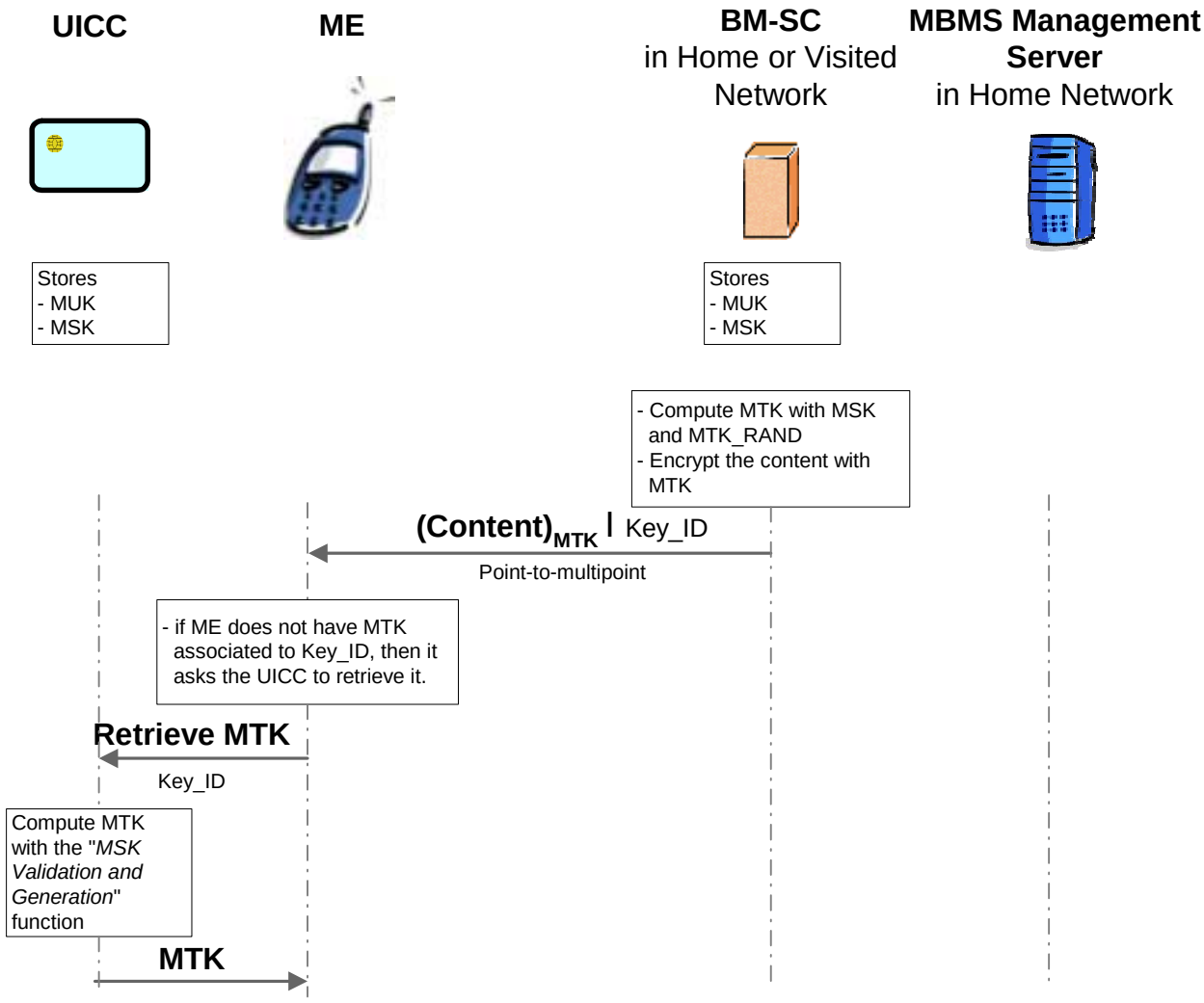
There are 2 types of MBMS procedures:

- The MBMS operating procedure corresponding to the multicast of the content

- The MBMS administrative procedures dealing with MBMS management data.
  They provide the following functionalities:
  - Update MSK
    This function updates a MSK stored on the UICC
  - Subscribe
    This function sets on the UICC the MBMS data associated to a MBMS_Id service
  - Unsubscribe
    This function deletes on the UICC all the MBMS data associated to a MBMS_Id service.
  - Delete MSK
    This function deletes a MSK on the UICC
  - Retrieve MBMS Info
    This function retrieves some MBMS management data stored on the UICC (e.g. MSK_Id, MSK_Expire,…)
  - …

2.2. MBMS service

2.2.1. MBMS OPERATING PROCEDURE



The MBMS Management Server would be implemented by means of an OTA server.

For MBMS operating procedure in the Home Network or in a Visited Network:

- Key_ID uniquely identifies the MSK and contains other information (SEQ, MAC, MBMS_ID) needed to calculate the MTK according to the "MTK Validation and Generation" function described in TS 33.246.
- "Retrieve MTK" function does not require the definition of a new UICC command since an existing UICC command can be slightly modified to achieve it.

2.2.2. MBMS ADMINISTRATIVE PROCEDURE

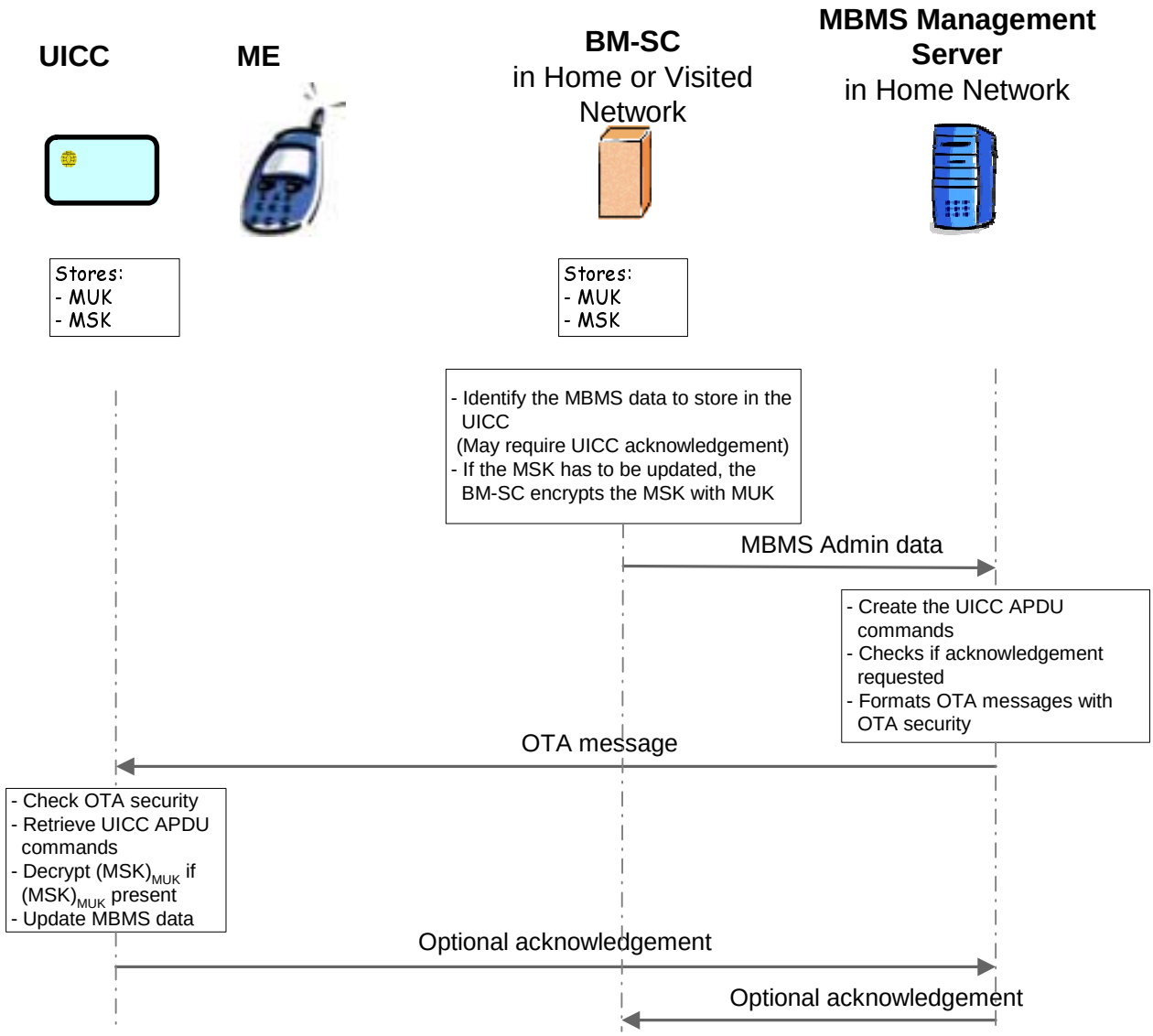


Figure 2: MBMS administrative procedure

The MBMS Management Server would be implemented by means of an OTA server.

<u>According to the MBMS functionality to perform:</u>

- The BM-SC identifies the MBMS data to store on the UICC.
- UICC with OTA mechanisms offers acknowledgement management. So, the BM-SC may use this mechanism and ask the UICC to send back an acknowledgement after execution of the UICC commands present in the OTA message.
- The OTA server defines the set of UICC commands to send to the UICC according to the MBMS Admin data to update in the UICC.
  The OTA security is specified in GSM 03.48 for R97 to R99, in TS 23.048 for Rel-4 and Rel-5, in TS 31.115, TS 31.116, TS 102 225 and TS 102 226 Rel-6. Cf [2].

Those different mechanisms take place both for MBMS service in the Home Network and in a Visited Network.

In case of operators interested in having a roaming agreement where the Visited Network wants to keep secret the MSK values, a solution could be proposed.

2.2.3. STANDARDIZATION PROCESS

The standardization process for MBMS solution concerns the following elements:

Interface:
The interface between the BM-SC and the MBMS Management Server shall be standardized. This specification is not an issue.

UICC:
This solution requires no new UICC command and uses OTA mechanisms, which exist and are already deployed in 3GPP infrastructures. The files required for MBMS were specified at T3 MBMS ad-hoc#101 meeting, the solution is ready for approval in Rel-6 timescale. Cf [2], [3].

The MBMS files specified at T3 ad-hoc#101 meeting are the following:

- $EF_{MBMSList}$ containing the identifiers of the MBM Services and the associated files
- $EF_{MBMSDescription}$ containing the description of one MBMS_Id service

The terminal can read the data of these files if the PIN access right has been granted.

- The MSK keys are stored in a dedicated MBMS key set. The description of the OTA-based MBMS key management is described in S3#33 "OTA for MBMS" contribution [4].

3. UICC-based only solution versus combined solution

At SA3#32 meeting it was agreed that the choice will be between UICC-based only solution and combined solution based on GBA, MIKEY and HTTP-Digest mechanism. This sections aims at comparing the two solutions.

3.1. OTA versus GBA/MIKEY

The two solutions are based on different mechanisms, UICC-based solution relies on OTA and the combined solution relies on GBA, MIKEY and HTTP_Digest. The main differences between OTA and GBA/MIKEY solutions are the following:

Optional mechanism

- GBA is an optional mechanism for Rel-6 and does not exist in previous release. The use of GBA for MBMS will oblige operators to implement GBA while there is no existing infrastructure deployed in the field at the moment.

- OTA is optional but the infrastructure is already deployed in the field. Many operators have an OTA server performing card management; the change to support MBMS consists in an upgrade of the OTA service

Remark: for both solutions there is a need to add a new interface: interface between BM-SC and OTA server for OTA solution, interface between BM-SC and BSF for GBA solution.

UICC modifications

- OTA solution does not require any new command, T3 already studied the UICC modifications to support MBMS

- Combined solution: GBA-U requires the specification of new commands to derive the Ks_int_NAF, Rel-6 timeframe is an issue.

IETF

- Combined solution is based on MIKEY and an enhancement of this protocol is necessary to allow the delivery of MBMS Service Keys to the UEs. Usually such change is performed in IETF scope, but at the moment it is not yet defined if the extensions needed for MBMS will be performed by IETF of will be specified in 3GPP rather than the IETF.

Roaming

- GBA does not envisage for instance the presence of a NAF (BM-SC) in a Visited Network while SA2 specification deals with roaming.

- With OTA solution the Home Operator has a full control of the smart card modification even in case of roaming.

- With the combined solution, the Visited BM-SC is enabled to provide MBMS services to a subscriber and also to modify any MBMS management data stored in the UE. So, the Visited Network gains control of the smart card with the following consequences:
    - The Home network is not more aware of the specific MBMS data contained in the UE (ME and UICC). The subscriber may subsequently need to renew all MBMS related data when returning to the HPLMN.
    - Visited Networks may compete for the same storage in the UE MBMS containers.
    - Solutions to limit the control of the UE MBMS management data by Visited BM-SC are hard to achieve, they need a link to the GBA derived keys with a specific MBMS context to enable the VPLMN to manage a subset of MBMS bearer services and not all of them.

Initiative of MSK delivery

- With OTA, the operator optimizes the key delivery by directly sending the key update messages to the UE (PUSH mechanism). This method decreases the radio traffic and allows the operator to plan the key update in an easy way. Moreover, to perform MBMS key delivery the operator does not require the user to join the MBMS service.

  In case of unexpected event (e.g. videoclip) arousing the interest of many subscribers at the same time while the associated MBMS keys are not provisioned in the smart card, then:
    - The Home Network can give some priority to the OTA server to focus on the corresponding MSK provisioning
    - A “Pay-Per-View” MBMS service may be provisioned within the card to face such unexpected events. Cf Oberthur’s contribution on “MBMS Pay per view charging model” [5].

- With combined solution the initiative to start the re-keying procedure corresponds to the terminal. To perform advanced key updates, the network has to send an additional Point-to-Multipoint “key availability message” to the UEs. Some mechanisms (e.g. Availability Time) have to be specified to prevent congestion due to multiple terminals asking for the keys at the same time, the solution becomes complex.

Key separation

- The MBMS key management of combined solution relies on UMTS authentication key K that plays the role of the MUK since GBA mechanism utilizes K for bootstrapping.

- For MBMS key management, the UICC-based only solution utilizes a dedicated MBSM key as MUK, independent from the UMTS authentication key K. This solution offers a key separation between AKA and MBMS service.

3.2. UICC-based only solution versus combined solution

The use of the UICC is necessary for MBMS high level content. This section identifies the differences between UICC-based only solution and combined solution allowing both UICC-based storage and ME-based storage.

Security

- The UICC provides a higher security level than a ME-based solution since the MBMS management keys are stored in a tamper resistant device. It allows effective MBMS content protection without frequent point-to-point key redistribution.

- In case of combined solution, the MBMS Service Key of a MBMS Service with high value content shall never be stored on the ME. In case of one MSK delivered to a ME then the security level associated to the MBMS_ID service is decreased since the service may be compromised by MSK retrieval on this ME.

Roaming

- With combined solution the roaming case seems more difficult to be taken into account since some Visited Networks may mandate UICC-based solution to protect their MBMS Service Keys.

MBMS parameters storage

- In the combined solution, key storage on the ME is not performed in a standardized way which may difficult the maintenance operations when different proprietary mechanisms are involved. Solutions as Device Management seem difficult to achieve for Rel-6 timeframe.

Secure portability of MBMS keys

- If the MSK are stored on the ME, the link between the MBMS data and the subscription is not assured:
    - The ME should erase MBMS subscription related information when the subscription changes (e.g. the user changes its UICC from one terminal to another one). The ME is not trusted to do that, an a fraudulent user could use the same account to ask for MSK deliveries in different terminal
    - A subscriber who changes his terminal should renew all MSK keys linked to this subscribed MBMS services.

Service Provisioning

- The UICC-based only solution allows immediate availability of the MBMS services on the UE. Operators do not need to update the terminals.

4. Conclusion

The MBMS UICC-based only solution, based on existing 3GPP infrastructure, offers a higher level of security and is ready for Rel-6 timescale.

So, we kindly recommend SA3 to choose the UICC-based solution as unique solution for MBMS service.

5. References

[1] TD S3-030534, Over-The-Air (OTA) technology, Gemplus/Oberthur/Schlumberger

[2] TD T3-040060, Storage of MBMS functionalities on the UICC,

[3] TD T3-040061, MBMS SK retrieving

[4] TD S3-0400xx, S3#33, OTA for MBMS, Axalto, Gemplus, Oberthur

[5] TD S3-0400xx, S3#33, MBMS Pay per view charging model, Oberthur