3GPP TSG SA WG3 Security — S3#32 **S3-040050**
09 - 13 February 2004
Edinburgh, Scotland, UK

Source: **Gemplus, Axalto, Giesecke & Devrient, Oberthur**

Title: **MBMS UICC-based solution**

Document for: **Discussion and decision**

Agenda Item: **6.20**

Abstract

This contribution describes the MBMS UICC-based solution agreed at T3 MBMS ad-hoc#101 meeting.

1. Introduction

The UICC-based solution offers a higher security level for MBMS service and has low impact on network resources. At SA3#31 meeting some companies thought that there was some risk in meeting the Rel-6 timescale. This paper describes the UICC-based solution agreed at T3 MBMS ad-hoc#101 meeting and shows that this solution will be ready for Rel-6 timescale.

2. Overview of the MBMS UICC-based solution

2.1. T3 ad-hoc meeting

At T3 ad-hoc#101 meeting on MBMS issues (13-14 January 2004), the attendees agreed on a complete UICC based solution (architecture and UICC features). This solution is based on 3GPP standards and requires no new UICC command (cf T3 MBMS ad-hoc meeting report [1]). It uses existing key sets management and OTA.

In case of a Visited Network providing the MBMS service, the solution allows two types of roaming agreement:

- Roaming agreement where the Visited Network accepts to reveal its BAK values to the Home Network
- Roaming agreement where the Visited Network wants to keep secret its BAK values

2.2. MBMS elements

MBMS Key material
The UICC-based solution uses the following key material:

- **SK**: Short-term Key
  - Session key to encrypt the content to multicast
- **BAK**: Broadcast Access Key

- Used to compute/retrieve the Session key
- Securely stored in the UICC

BAK and SK keys are common to all subscribers of an MBMS_Id service.

- **RK**: Registration Key
  - An unique key per user

  Remark: In this scheme the presence of the TK (Temporary Key derived from the RK) is no longer necessary since the Home Network performs all the Key Management functionalities.

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 BAK
    This function updates a BAK 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 BAK
    This function deletes a BAK on the UICC
  - Retrieve MBMS Info
    This function retrieves some MBMS management data stored on the UICC (e.g. BAK_Id, BAK_Expire,…)
  - …

MBMS network entities

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

- **In Home Network**
  - BM-SC
  - OTA server

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

- **Trusted Third Party**
  This entity is present to address the case of MBMS roaming agreement where the Visited Network wants to keep secret its BAK values.

Interfaces:

- Interface between the BM-SCs shall be standardized independently of the chosen solution, since it is necessary for MBMS roaming.
  This interface is used to transfer data such as the “MBMS Admin data” present in the MBMS administrative procedures described further.

- The interface between the Home BM-SC and the OTA server is proprietary and operator dependent

2.3. MBMS service in the Home Network

2.3.1. MBMS OPERATING PROCEDURES

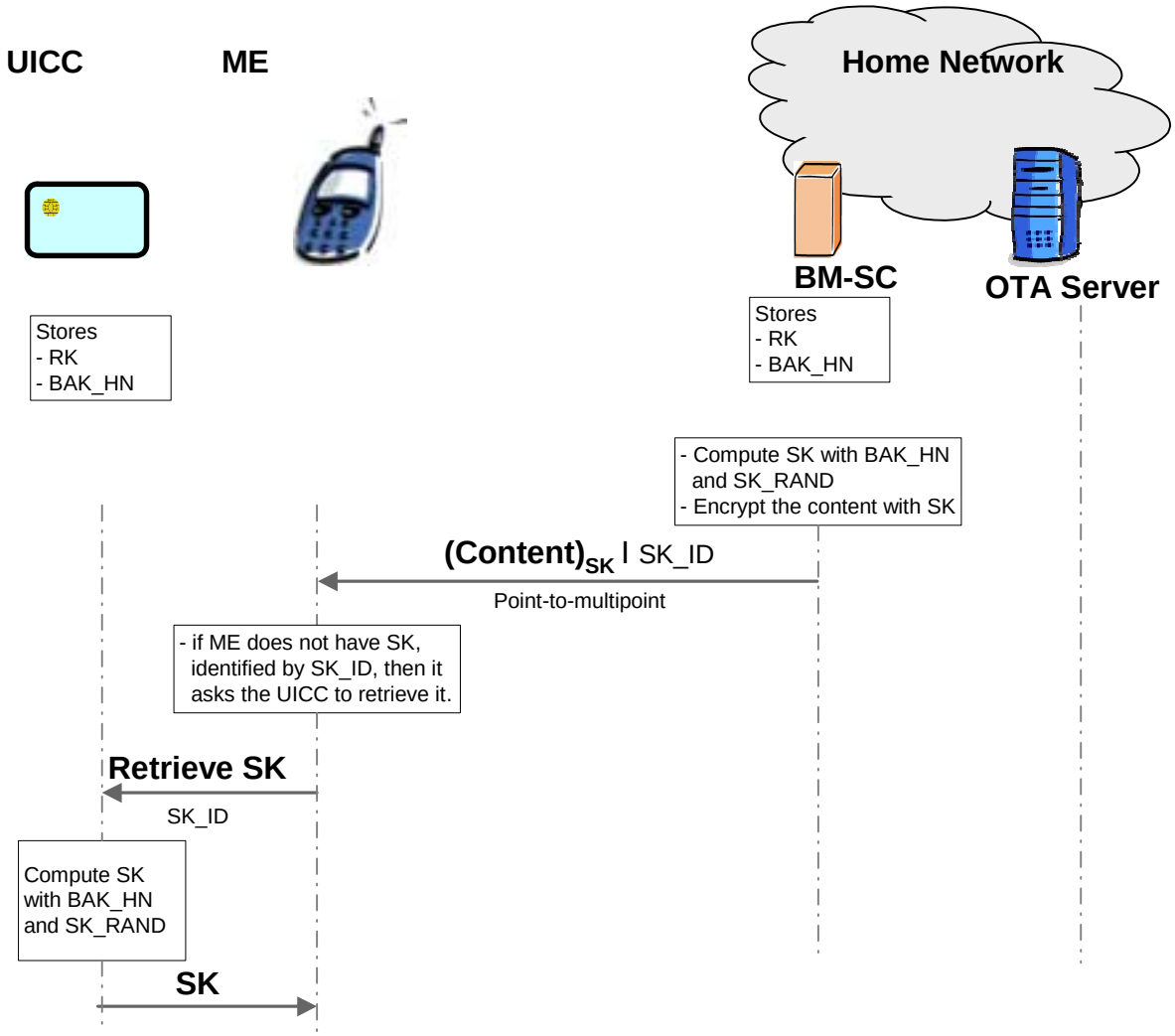

Figure 1: MBMS operating procedure in Home Network

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

- SK_ID uniquely identifies SK and contains other information related to SK computation. SK_ID is composed of the following fields (MBMS_ID| BAK_ID | SK_RAND).

- "Retrieve SK" function does not require the definition of a new UICC command since an existing UICC command can be slightly modified to achieve it.

  The MBMS parameters of the "Retrieve SK" function will have to be specified by SA3 to incorporate the mechanism to guaranty freshness and origin of the session keys, but it will not require the use of a new UICC command.

2.3.2. MBMS ADMINISTRATIVE PROCEDURE

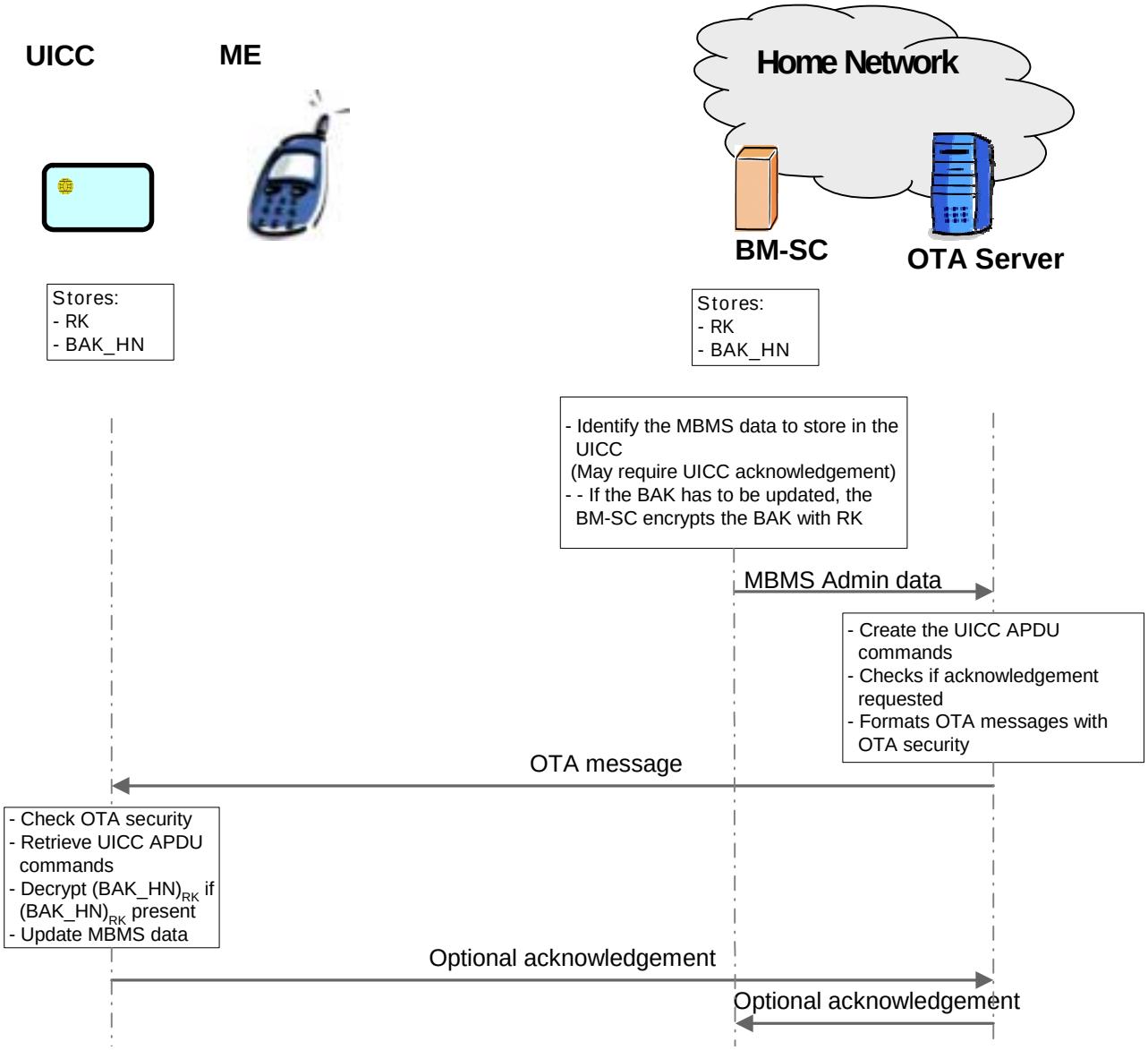

Figure 2: MBMS administrative procedures in Home Network

<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 offer 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.
  This set of commands does not need to be standardized since it is operator dependent.
  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 and TS 31.116 for Rel-6. Cf [2].

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

2.4. MBMS service in a Visited Network

2.4.1. MBMS OPERATING PROCEDURE

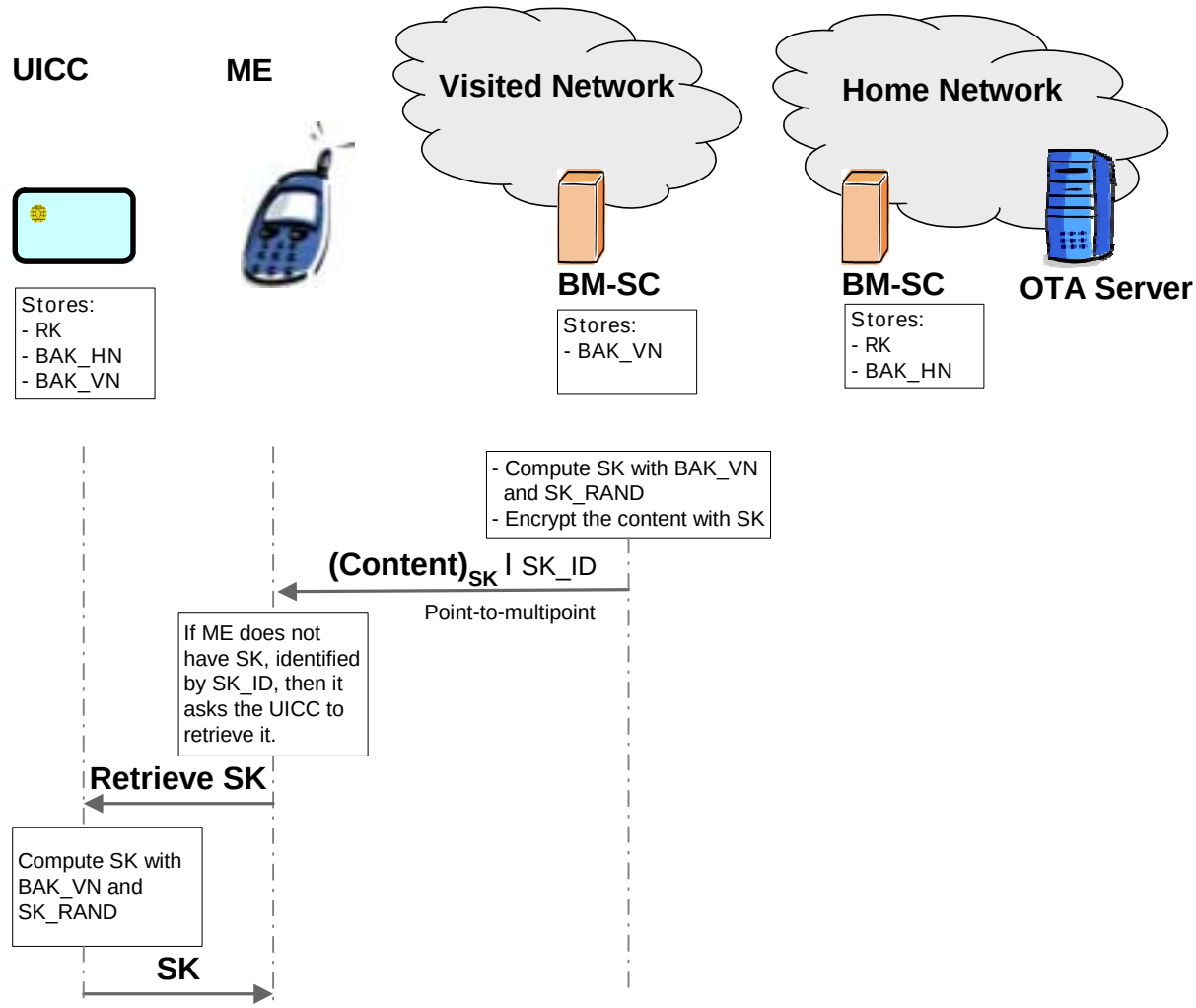

Figure 3: MBMS operating procedure in a Visited Network

2.4.2. MBMS ADMINISTRATIVE PROCEDURES

We distinguish 2 kinds of roaming cases:

Roaming case 1:
Roaming agreement where the Visited Network accepts to reveal its BAK values to the Home Network

Roaming case 2:
Roaming agreement where the Visited Network wants to keep secret its BAK values

Roaming case 1: BAK values of the Visited BM-SC in clear text in the Home Network

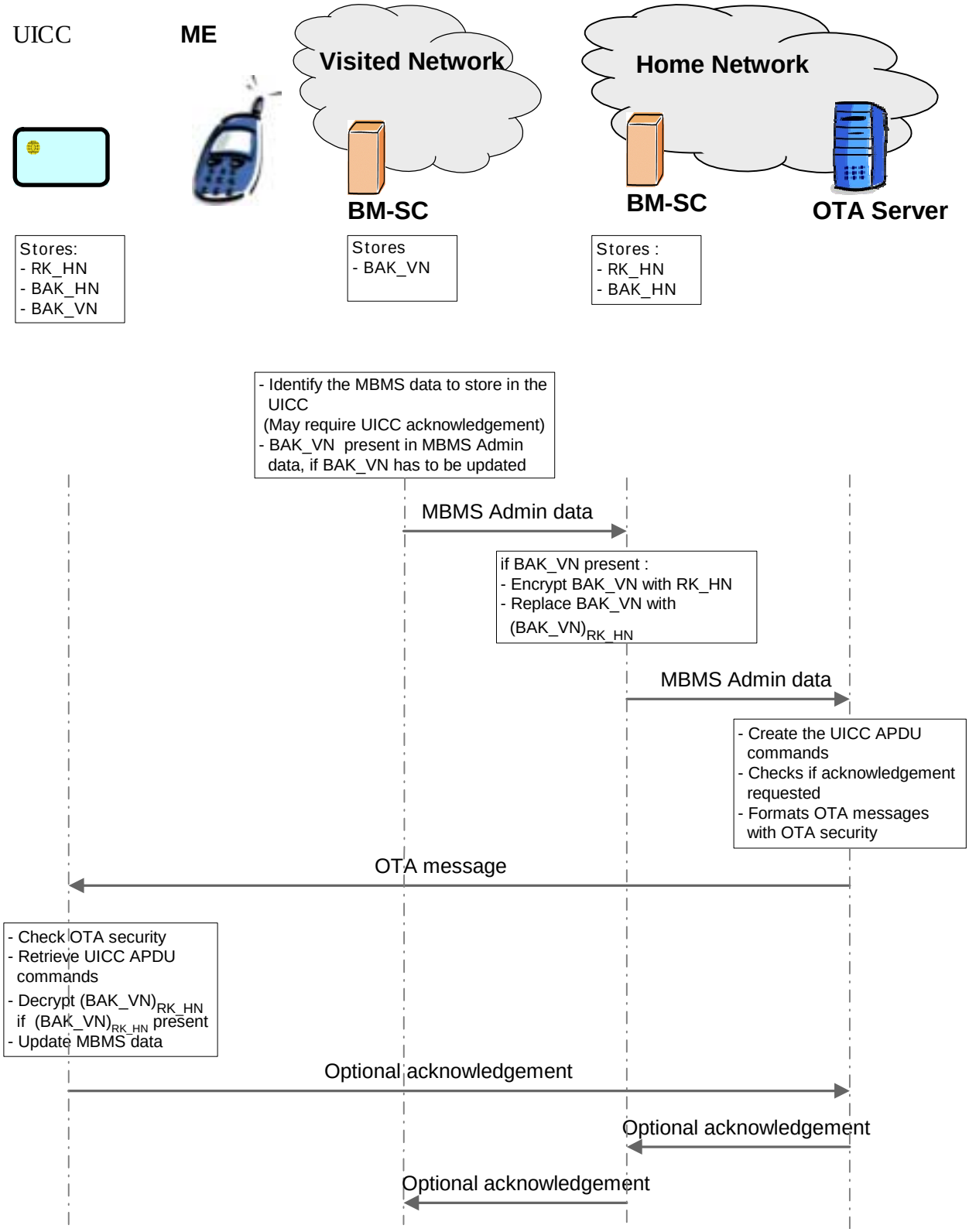

Figure 4: MBMS administrative procedures in a Visited Network – roaming case 1

Roaming case 2: The BAK of the Visited BM-SC are kept secret

This solution needs the presence of a Trusted Third Party. The BAK is transmitted to the Home Network encrypted with a key (RK_VN) provided by the Trusted Third Party.
Only the Trusted Third Party, the Visited Network and the UICC know this RK_VN key. The set up of the RK_VN between the BM-SC and the Trusted Third Party takes place only once per roaming agreement.

This roaming case is more complex than the previous one, but it offers a solution to operators refusing to reveal their BAK values. It is up to the operators to decide if there are interested in this roaming case.

Set up of the RK_VN with the Trusted Third Party

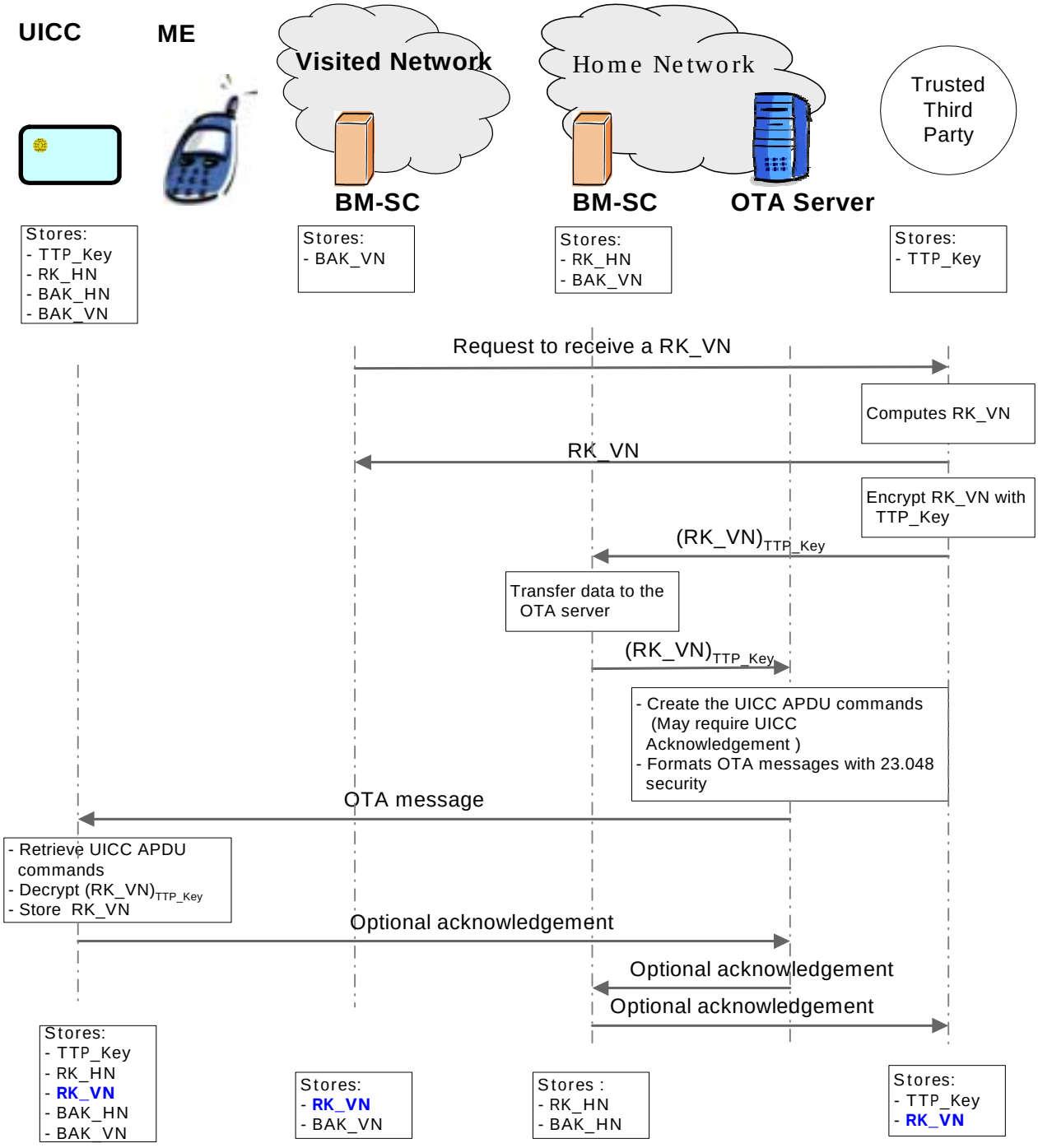

Figure 5: Set-up of the RK_VN key – roaming case 2

MBMS management procedures: for a functionality requiring BAK_VN update

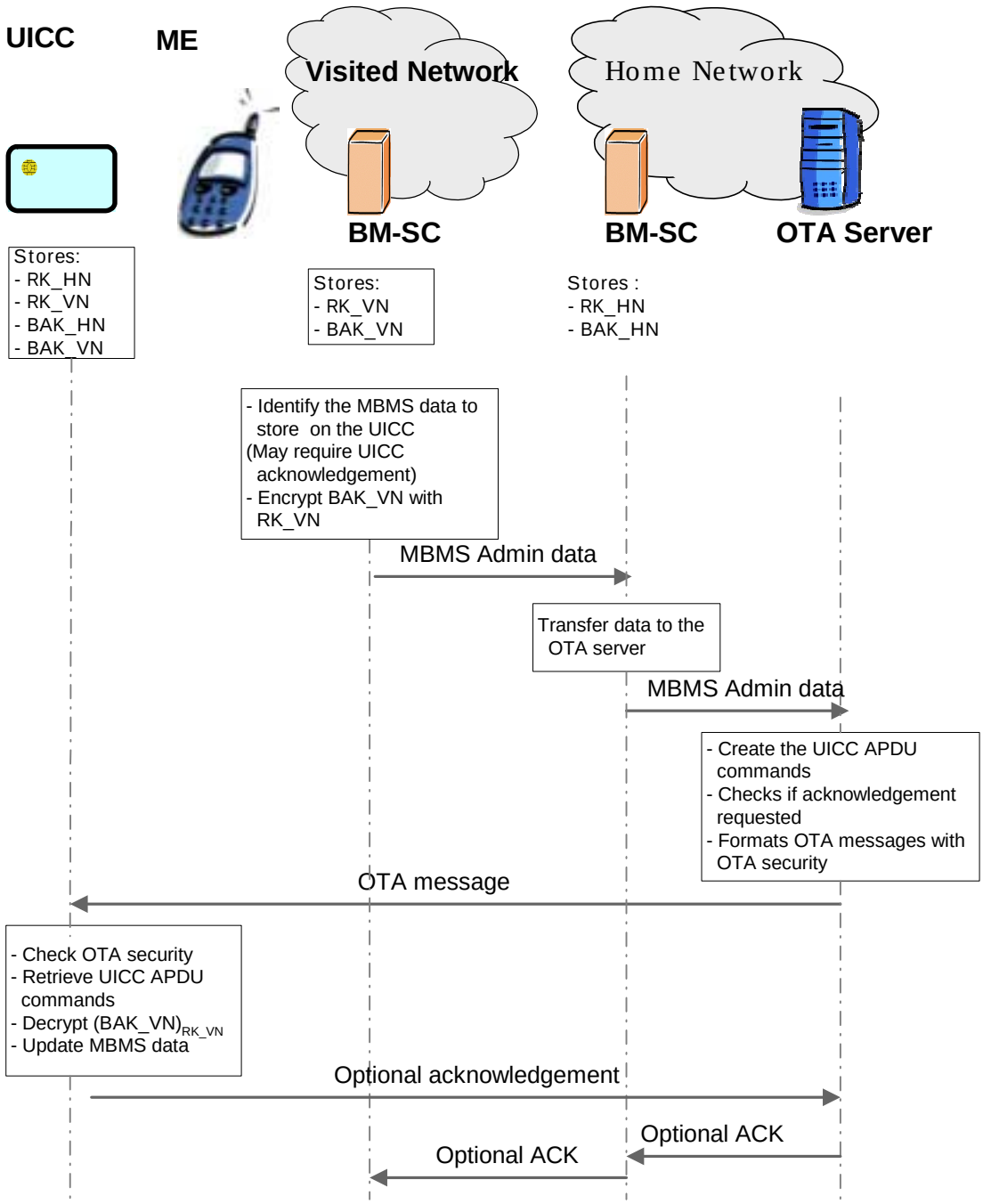

Figure 6: MBMS administrative procedures in a Visited Network – roaming case 2

3. Status of this solution

3.1. Security

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

During MBMS administrative procedures the PLMN gains control of the MBMS management data stored in the UE. By using OTA server, the Home Network is the only entity dealing with the MBMS management data stored on the UE. It avoids the following threats identified in [3]:

- Visited PLMN may modify any MBMS management data stored in the UE.
- Several visited PLMNs may compete for the same storage in the UE MBMS container. It could lead to a denial of service attack.
- The Home Network is not longer aware of the MBMS data present on the UICC. It may need to renew all the MBMS related data in the UE when returning in the HPLMN.

3.2. Standardization process

Interfaces:
The need to standardize the interface between BM-SCs is independent of the chosen solution since it is required for MBMS roaming.

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 ([4], [5]), the solution is ready for approval in Rel-6 timescale.

4. Conclusion

This MBMS UICC solution, based on 3GPP existing infrastructure, offers a higher security level, low impact on the network resources and is ready for Rel-6 timescale.

Moreover, at TSG SA#22 plenary meeting several operators expressed a preference for the UICC-based only solution and TSG SA recommended that options should be kept to a minimum. (Cf TSG SA#22 draft meeting report [6]).

So, we kindly recommend SA3 to choose the UICC-based solution as unique solution for MBMS service. An associated CR is ready for approval [7].

5. References

[1] TD T3z040010, T3 ad-hoc#101 meeting report on MBMS issues

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

[3] TD S3-0400xx, Discussion paper on MBMS key management, Gemplus/Axalto

[4] TD T3z040011, Storage of MBMS functionalities on the UICC,
T3 ad-hoc#101 meeting on MBMS issues

[5] TD T3z040012, MBMS SK retrieving,
T3 ad-hoc#101 meeting on MBMS issues

[6] TSG SA#22 Draft Report meeting

[7] TD S3-0400xx, CR to TS 33.246, Gemplus/Axalto