3GPP TSG SA WG3 #30 **S3-030767**

18-21 November 2003

Munich, Germany

Agenda Item:	6.20 MBMS
Source:	Ericsson
Title:	Impacts on the 3GPP network with a UICC based and a non-UICC based solution in MBMS
Document for:	Discussion and decision

1. Introduction

SA3 is currently discussing several different proposals for key management in MBMS. Some of these proposals are UICC based and some are non-UICC based solutions.

Some of these UICC based solutions, requires a OTA provisioning server in the Home Network in order to be able to upgrade UICC cards with key management and security keys. This paper attempts to in chapter 2.1 summarize the impact on the different nodes and interfaces in the 3GPP network, if such a solution with a OTA-system is required by the operator to upgrade UICC cards.

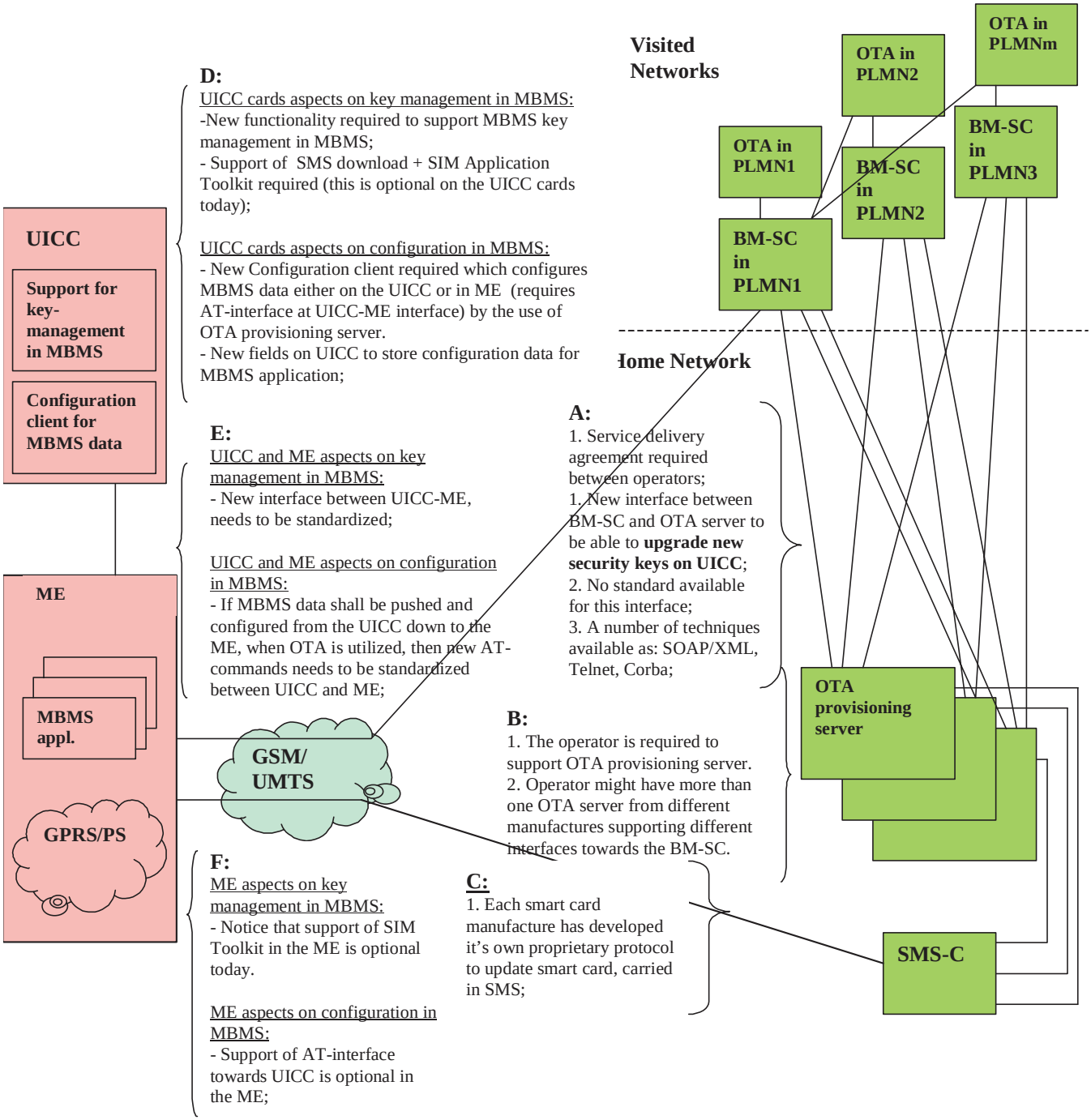
The aspects of upgrading other MBMS data (not security related) in the UE (either on the UICC or in the ME) are also incorporated into the paper. This discussion is not security related but provided just for information to SA3.

If a UICC-based solution for key management in MBMS is selected, then it's very likely that also other MBMS parameters (which are not security related) will be stored in new fields on the UICC, and for that the OTA SMS will most likely be used as well to update UICC cards.
But one should also have in mind that Device Management could be used instead of OTA SMS to configure the terminal instead of the UICC (or even the UICC, but that will be supported in later releases of Device Management), or even a combination of OTA and Device Management could co-exist with a UICC-based solution, as some configuration data might be stored on the UICC and some data will be configured in the terminal itself.

Chapter 2.2 is only provided for information to show an example of network impacts when a non-UICC based solution is used for MBMS.

2. Discussion

2.1 UICC-based solution in MBMS for key management



A:

When the BM-SC is located in a Visited Network, some kind of service delivery agreement with the Home Network is required in order to allow connecting the BM-SC to the OTA provisioning server(s) in the user's Home network.

A new interface between the BM-SC and OTA provisioning server is required. There is no standard available today for this interface. A number of different techniques are available as SOAP/XML, Telnet, Corba. This implies that the BM-SC might have to support several techniques as each operator has there own proprietary protocol towards their OTA provisioning server (and maybe more than one techniques for the same operator, if several OTA provisioning servers are used by this operator from different manufactures).

B:

The operator is required to support OTA provisioning server(s).

The operator might have to support several OTA provision server(s) from different manufactures supporting different interfaces and techniques towards the BM-SC.

C:

Each smart card manufacture has developed it's own proprietary protocol on their smart card to provide the capability to the operator to perform secure updates on the UICC card.

D:

New UICC cards are required with MBMS support. "Fresh" UICC cards could perhaps be re-used as well, if they have the capability to be upgraded via the air with OTA SMS with the necessary functionality in MBMS (e.g. key management, configuration of MBMS data (not security related)).

UICC aspects on key management in MBMS:

In order to update the UICC card, the UICC card needs to support SMS download and SIM Application Toolkit. Notice that support of SIM Toolkit in the UICC is optional today.

UICC aspects on configuration in MBMS:

A new Configuration client is required on the UICC, by which the operator can configure MBMS data specific for this user and the MBMS application running in the ME. The configuration data could be either stored on the UICC or in the ME itself.

For the Configuration client to be able to push down and configure MBMS data in the ME, support of a new AT-interface to the ME is required. This AT–interface needs to be supported by both the UICC and the ME.

New fields on the UICC need to be standardized to store configuration data for the MBMS application;

E:

UICC and ME aspects regarding key management in MBMS:

A new interface between the ME and UICC needs to be standardized for key management in. This interface needs to be supported in both entities.

UICC and ME aspects on configuration in MBMS:

If MBMS data shall be pushed down and configured in the ME by the UICC, then new AT-commands need to be standardized between the UICC and ME;

F:

ME aspects regarding key management in MBMS:

Notice that support of SIM Toolkit in the ME is optional today.

ME aspects on configuration in MBMS:

Support of AT-interface towards the UICC is optional in the ME.

General comments:

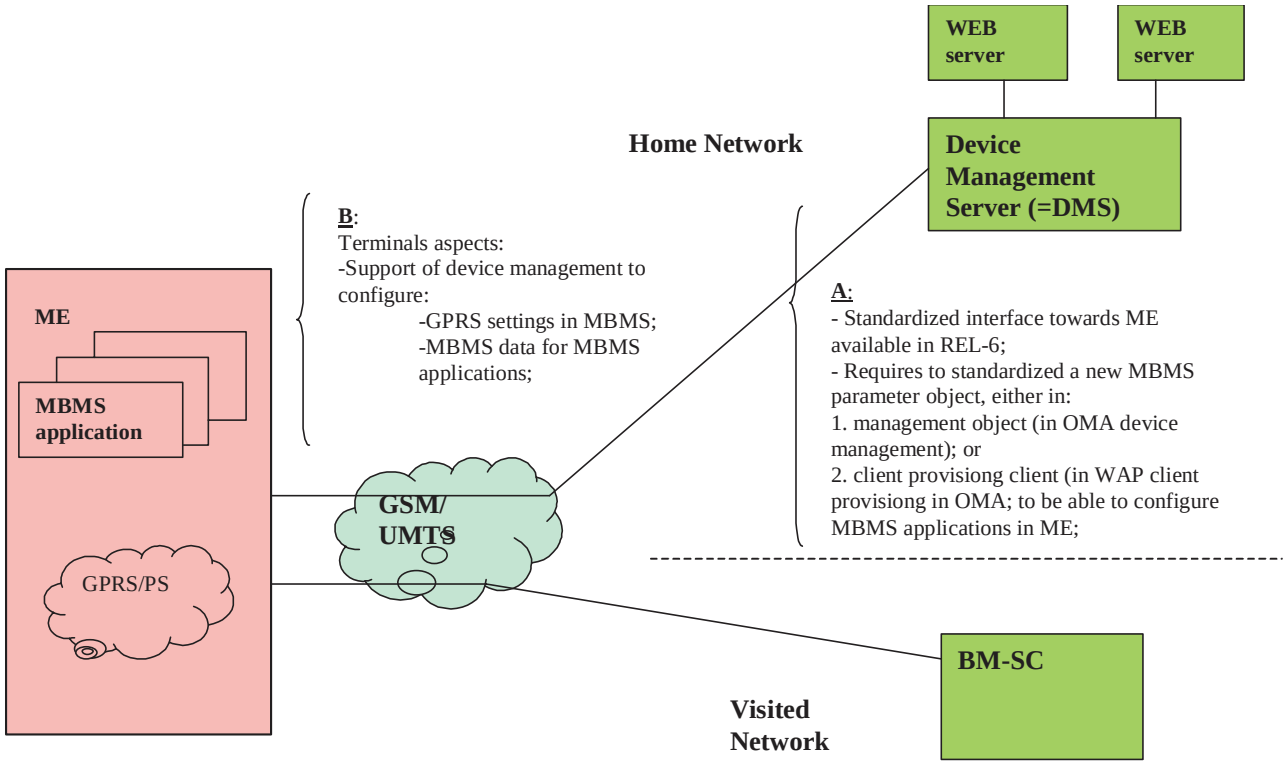
The reliability of when an OTA SMS is delivered to an UE can't be assured. It can take 1 minute or several days. Also when the BM-SC is located in visited networks (MBMS service origins in the visited network), needs to be able to relay on that the home operator can deliver and put priority on the traffic originating from the BM-SC's in visited networks.

2.2 Non-UICC based solution in MBMS for key management

This chapter is not security related, but just provided for information.

The operator may use the Device Management Server in his network to configure GPRS and MMS settings in the terminal. It is foreseen that Device Management will be used for many other services as well in the future.

With a non-UICC based solution in MBMS, a Device Management Server could be used to upgrade the terminals with MBMS data. The purpose is just to show how the OTA provisioning server can be replaced by a Device Management Server in the network, to perform necessary configuration in the terminals. This might imply a less complex network architecture, as new UICC cards and OTA provisioning servers are not any longer involved in MBMS.



A:

The device management interface towards the ME is standardized in OMA. This is expected to be delivered in REL-6. If Device Management shall be used in MBMS, then a new MBMS parameter object needs to be standardized, either as an:
1. management object in OMA device management; or
2. client provisiong client in WAP client provisiong, also in OMA;
to be able to configure MBMS applications in ME.

B:

The terminals are required to support device management in order to be able to configure:
1. GPRS settings in MBMS; and
2. MBMS data for MBMS applications.

3. Conclusion

This paper shows that a UICC based solution in MBMS will have many impacts on the 3GPP network, the UICC and the terminal. For example:

- The operator is required to support of OTA provisioning server(s).

- A new interface between the BM-SC and the OTA provisioning server might need to be standardized in order to avoid support of many techniques as SOAP/XML, Telnet and Corba in the BM-SC.
- The operator might require several OTA provisioning servers, maybe one for each smart card manufacture. Each OTA provisioning server needs to be connected to all BM-SC's in visited networks, which the home operator has roaming agreements with.
- New or fairly fresh UICC cards with support of SMS download and SIM Toolkit are required.
- The reliability of when an OTA SMS can be delivered to an UE can't be assured. It can take 1 minute or several days. For key management in MBMS this might be critical.

4. Proposal

Ericsson proposes that SA3 should send an LS to SA2 and OMA asking whether a new interface between the BM-SC and OTA provisioning server can be standardized.

Ericsson also proposes that SA3 should send an LS to various groups as SA2, OMA, T3 to comment on the issues mentioned in chapter 3 and the architecture with a UICC based solution.

5. References

[1] S3-030583: Key distribution protocol selection, from Siemens.

[2] S3-030534: Over-The-Air (OTA) technology, from Gemplus, Oberthur and Schlumberger.