3GPP TSG SA WG3 Security – S3#30 **S3-030534**

6 - 10 October 2003

Povoa de Varzim, Portugal

Source: **Gemplus, Oberthur, Schlumberger**

Title: **Over-The-Air (OTA) technology**

Document for: **Discussion and decision**

Agenda Item: **T.B.D**

Abstract

This input paper aims at providing an overview of the Over-The-Air technology.

1. Introduction

This contribution provides background about 3GPP's standardized Over The Air (OTA) technology. It is proposed that OTA provides a feasible solution for operators to upgrade the majority of their deployed UICC to support the 3GPP2 key hierarchy for MBMS security, and certainly all cards deployed henceforth may be upgraded when the MBMS standards are complete. Sections 2-4 give background about OTA, and section 5 describes its application to upgrade 'legacy' USIMs to support the 3GPP2 MBMS key management.

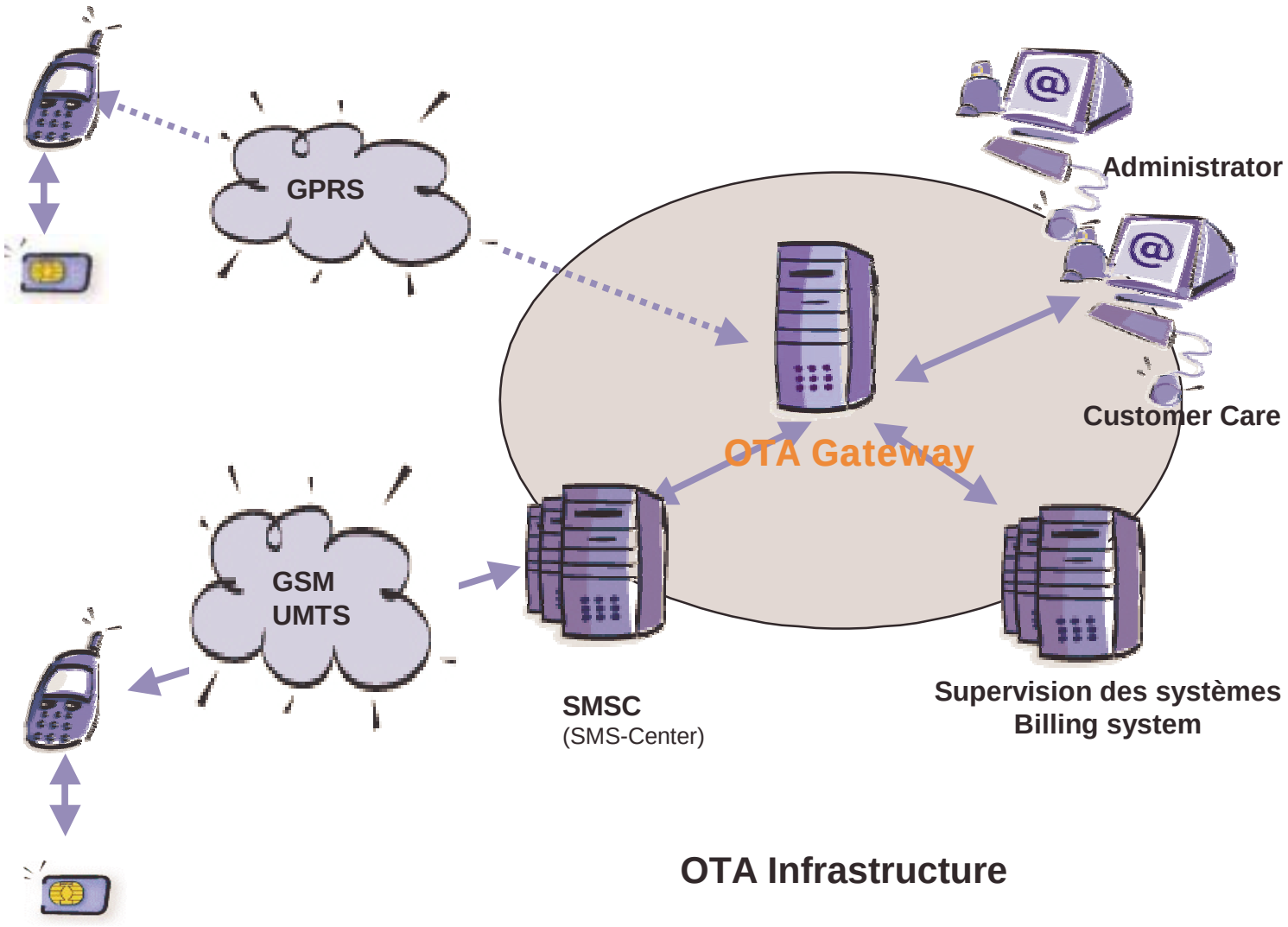
2. OTA overview

Over-The-Air (OTA) is a technology that updates or changes data in smart cards (SIM card or UICC) without having to reissue the cards. OTA enables a network operator to introduce new services or to modify content of smart cards in a rapid and cost-effective way.

OTA is based on a client/user architecture where at one end there is an operator back-end system and at the other end there is the smart card. The operator’s back-end system sends service requests to an OTA Gateway that transforms the requests into Short Messages to be sent to the smart card.

At the moment, the transport bearer is the SMS bearer but in a near future the transport bearer could be CSD or GPRS. To perform OTA with CDS or GPRS bearer, CAT-TP/BIP or J2ME/JSR#177 mechanisms could be used since they are in standardization process.

With SMS bearer:
The OTA Gateway sends the Short Messages onto a Short Message Services Center (SMSC), which transmits them to the smart cards in the field.



OTA Infrastructure

Back-end System

The back-end system can be anything from a customer care operator to a billing system, a content provider or a subscriber web interface. The provisioning system has to be connected to the mobile network. Service requests contain the service requested (activate, deactivate, load, modify…), the subscriber targeted and the data to perform the service. The back-end system then sends out service requests to the OTA gateway.

OTA Gateway

The OTA Gateway receives Service-Requests through a Gateway API that will indicate the actual card to modify/update/activate. In fact, inside the OTA Gateway there is a card database that indicates for each card, the card manufacturer vendor, the card's identification number, the IMSI and the MSISDN.

The second step is to format the service request into a message that can be understood by the recipient card. To achieve this, the OTA Gateway has a set of libraries that contain the formats to use for each brand of smart cards. The OTA Gateway then formats the message differently depending on the recipient card.

The third step consists in sending a formatted message to the SMSC using the right set of parameters as described in GSM 03.48 or TS 23.048. Then the OTA Gateway issues as many SMS as required to fulfil the Service-Request. In this step the OTA Gateway is also responsible for the integrity and security of the process.

SMSC

Services center for short messages (SMS) exchanged between the management system of these messages (OTA Gateway) and the cellular network. A message can be sent to or from a Mobile Phone. If the Mobile Phone is powered off or has left the coverage area, the message is stored and offered back to the subscriber when the mobile is powered on or has re-entered the coverage area of the network.

SMS Channel

The communication between the SIM card and the OTA Gateway can be done by SMS exchange and in this case named the SMS channel.

Mobile Equipment

Regarding OTA services, the mobile equipment has to be SIM Toolkit compliant.

Smart Card (SIM card or UICC)

The messages with protocol identifier set to “SIM data download” are delivered by the ME to the smart card (ENVELOPE or UPDATE RECORD commands, …).

The GSM or 3G application receives those commands and calls the OTA layer.
The OTA layer checks the messages according to the GSM 03.48 or TS 23.048 (Security layer based on cryptographic services). Each secured packet may contain one or more APDUs commands dedicated to Remote File Management or Remote Applet Management or SIMToolKit.

The Remote File Management (RFM) enables to execute EF management commands (SELECT, UDPATE RECORD, DEACTIVATE FILE, VERIFY PIN,…)

The Remote Applet Management (RAM) enable to execute applet management commands (LOAD, INSTALL, DELETE, GET STATUS,…)

3. OTA specifications

3.1. Standardized mechanism

The OTA specification, GSM 03.48 [1], was first created for Release 97 of GSM.

- GSM 03.48 “Security Mechanism for the SIM application toolkit”
  Defines:
  - The structure of the secured packets in SMS-PP (Point-to-Point) and SMS-CB (Cell Broadcast)
  - The set of commands for Remote File Management on the SIM
  - The set of commands used for Remote Applet Management for SIM cards compliant with 03.19 (i.e. JavaCard cards)

GSM 03.48 was renamed 3GPP TS 23.048 [2] for Rel-4 and Rel-5 and is applicable to both GSM and 3G.

For Rel-6 TS 23.048 is split into 4 specifications:

- ETSI TS 102 225 [3]
- ETSI TS 102 226 [4]
- 3GPP TS 31.115 [5]
- 3GPP TS 31.116 [6]

The features applicable to any telecommunication environment are transferred to ETSI SCP (ETSI TS 102 225 and TS 102 226), while the 3GPP specific parts are kept in 3GPP TS 31.115 and TS 31.116.

- ETSI TS 102 225 “Secured packet structure for UICC based applications”
  Defines the secured packet structure.

- ETSI TS 102 226 “Remote APDU Structure for UICC based applications”
  Defines the set of commands to make Remote File Management and Remote Application Management. Those commands are transported in the secured packets as defined in TS 102 225.

- 3GPP TS 31.115 “Secured packet structure for (U)SIM Toolkit applications”
  Is the mapping of the secured packets on SMS.

- 3GPP TS 31.116 “Remote APDU Structure for USIM Toolkit applications”
  Contains the SIM/USIM specific features for remote file management and remote applet management.

The Rel-6 is currently being updated but essentially at the remote applet management level.

4. Requirements for OTA

It is not mandatory for smart cards to support OTA specifications but most cards are supporting the secured packets over SMS for Remote File Management and application download. Only very low cost cards do not support OTA. The Remote Applet Management is generally supported by JavaCards cards only.

The USIM application is mainly present on JavaCard UICCs since the UICC was specified to be multi-applicative and some of the USIM commands are Open Platform commands that require JavaCard.

4.1. Native cards

To be updated via OTA, a native card needs to have an implemented OTA library (23.048 library or a proprietary one (e.g ESMSV2)).

4.2. JavaCard cards

To be updated via OTA a JavaCard card needs to be personalized with an “OTA profile” that enables the UICC to retrieve and execute the OTA command sent by the OTA Gateway. Remote File Management and Remote Applet Management system applet have to be installed into the UICCs. The configuration related to the 23.048 has to be personalized: “KeySet” where OTA keys are stored, “Access Domain” specifying the applets rights on file system, and “Minimum Security Level” specifying minimum security that incoming OTA message has to present.

By default, all the mechanisms required to support OTA operations are present on a JavaCard UICC. It is during the personalization phase that the “OTA profile” is initialized.

The interoperability applies to JavaCard cards only. The Remote Applet Management will be interoperable for Rel-6 UICC. But, this not prevent an operator to perform Remote Applet Management for pre-Rel-6 UICC, since the smart cards manufacturers have implemented some proprietary OTA mechanisms to address this issue.

So, all the JavaCard UICC issued with an initialised “OTA profile” can be upgraded via OTA.

4.3. Card memory size

If the OTA operation consists in adding data in the UICC then the available memory size of the card has to be taken into account. The OTA Gateway is aware of this information during its configuration and provisioning. Furthermore, using Open Platform commands, the OTA Gateway is able to retrieve via OTA SMS the memory left in each card in the field.

4.4. OTA Gateway

To perform OTA, the OTA Gateway shall contain the OTA libraries corresponding to the mechanisms implemented on the smart cards in the field.

When there are smart cards implemented with some proprietary OTA mechanisms, the OTA Gateway needs to have the corresponding libraries to address those smart cards in the field. But, the OTA Gateway of an operator is in line with the smart cards he issues. The platform present in the OTA Gateway knows the card profile of the UICC in the field and is able to format the message to send to the recipient card.

5. OTA and MBMS 3GPP2 solution

The support of MBMS 3GPP2 solution for MBMS security by pre-Rel-6 UICCs may require the addition of an MBMS application on UICCs. Since the USIM application is mainly implemented on JavaCard UICC, the legacy USIMs in the field will need to be upgraded via OTA Remote Applet/File Management to access Multicast service.

So, all the JavaCard UICC in the field issued with an initialised « OTA profile » allowing Remote Applet/File Management and having enough available memory size could be upgraded via OTA to access Multicast service.

The number of USIM application implemented on native cards is very low. The exact number of native cards containing a USIM application and JavaCard UICCs issued without an inadequate OTA profile can only be provided by the operators who issue the cards.

Additionally, the free memory required for this pre-R6 MBMS application is estimated being less than 1 Kbytes, probably fitting in most of the existing UICCs, but again considered as an operator's deployment matter.

The introduction of MBMS service for subscribers will take place in some years. So, if from now all the new issued UICCs are personalized with an "OTA profile" allowing Remote Applet/File Management and have enough available memory size, then the number of UICCs that could not be upgraded via OTA during the introduction of MBSM service will be very low, insignificant.

6. Conclusion

Considering all the advantages of the 3GPP2 solution in term of security, signalling traffic, subscription and charging managements, we recommend to adopt the MBMS 3GPP2 solution for MBMS security. The backward compatibility issues for pre-Rel-6 UICCs may be solved using OTA mechanisms for Remote Applet/File Management in order to properly update the legacy USIMs.

7. References

[1] GSM 03.48: "Security mechanism for the SIM application toolkit"

[2] 3GPP TS 23.048: "Security mechanisms for the (U)SIM application toolkit"

[3] ETSI TS 103 225: "Secured packet structure for UICC based applications"

[4] ETSI TS 102 226: "Remote APDU Structure for UICC based applications"

[5] 3GPP TS 31.115: "Secured packet structure for (U)SIM Toolkit applications"

[6] 3GPP TS 31.116: "Remote APDU Structure for USIM Toolkit applications"