3GPP TSG SA WG3 Security — S3#33 **S3-040356**
10 - 14 May 2004 **Comments to S3-040247**
Beijing, China

Source: **Axalto, Gemplus, Oberthur (commented by Siemens 14/04/2004)**

Gemplus' reply to Siemens comments (29/04/04)

Title: **OTA for MBMS**

Document for: **Discussion and decision**

Agenda Item: **MBMS**

Abstract

This contribution describes the use of OTA for MBMS.

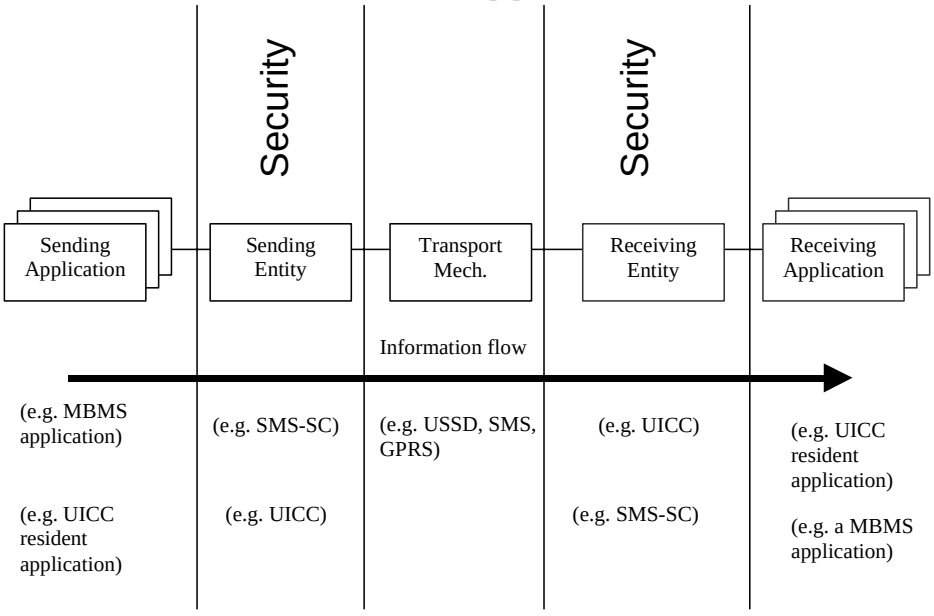
1. Introduction

The MBMS UICC-based only solution relies on OTA mechanisms. This contribution describes OTA mechanisms and the way MBMS makes use of them.

2. OTA security mechanisms - overview

2.1. OTA structure packet structure ETSI TS 102 225

ETSI TS 102 225 defines "Secured packet structure for UICC based applications (Rel-6)", it allows establishment of secure communications [1].



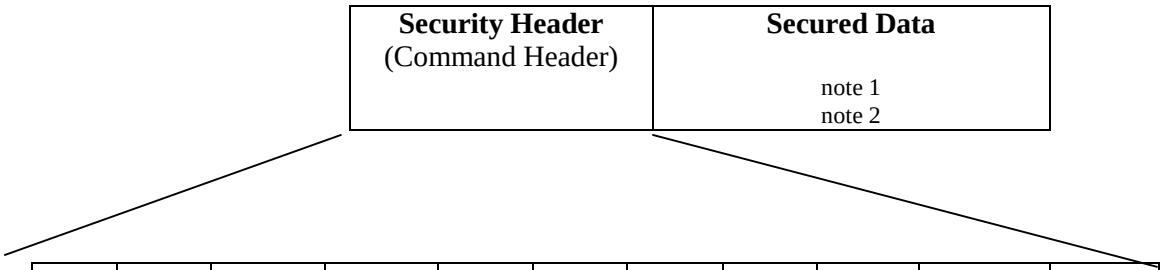
The Sending Entity and the Receiving Entity establish a secure communication by exchanging Secured Packets according to TS 102 225.

Detailed procedure:

- The Sending Application prepares an Application Message and forwards it to the Sending Entity, with an indication of the security to be applied to the message.
- The Sending Entity adds a Security Header (Command Header) to the Application Message and then applies the requested security to part of the Command Header and all of the Application Message (including any padding octets). The resulting structure is referred to as the (secured) Command Packet.
- The Receiving Entity receives the Command Packet and unpacks it according to the security parameters indicated in the Command Header. Additional security conditions may apply (e.g. Minimum Security Level) before unpacking.
- The Receiving Entity forwards the Application Message to the Receiving application indicating to the Receiving Application the security that was applied.
- If so indicated in the Command header, the receiving entity shall create a Secured Response Packet. The Response Packet consists of a Security Header (Response Header) and optionally, application specific data supplied by the Receiving Application. Both, the Response Header and the application specific data are secured using the security mechanisms indicated in the received Command Packet.

Secured Packet consists of a Security Header and Secured Data.

Ex: the Secured Command packet structure



CPI	CPL	CHI	CHL	SPI	KIc	KID	TAR	CNTR	PCNTR	RC/ CC/DS
note 3	note 3	note 3	note 3	note 2	note 2	note 2	note 2	note 1 note 2	note 1 note 2	note 1

NOTE 1: These fields are included in the data to be ciphered if ciphering is indicated in the Security Header.
NOTE 2: These fields are included in the calculation of the RC/CC/DS.
NOTE 3: Part or all of these fields may also be included in the calculation of the RC/CC/DS, depending on implementation (e.g. SMS).

	Element	**Length**	**Comment**
CPI	Command Packet Identifier	1 octet	Identifies that this data block is the secured Command Packet.
CPL	Command Packet Length	variable	This shall indicate the number of octets from and including the Command Header Identifier to the end of the Secured Data, including any padding octets required for ciphering.
CHI	Command Header Identifier	1 octet	Identifies the Command Header.
CHL	Command Header Length	variable	This shall indicate the number of octets from and including the SPI to the end of the RC/CC/DS.
SPI	Security Parameter Indicator	2 octets	see detailed coding in clause 5.1.1 of TS 102 225.
KIc	Ciphering Key Identifier	1 octet	Key and algorithm Identifier for ciphering.
KID	Key Identifier	1 octet	Key and algorithm Identifier for RC/CC/DS.
TAR	Toolkit Application Reference	3 octets	Coding is application dependent as defined in TS 101 220 .
CNTR	Counter (	5 octets	Replay detection and Sequence Integrity counter.
PCNTR	Padding Counter	1 octet	This indicates the number of padding octets used for ciphering at the end of the secured data.
RC CC DS	Redundancy Check Cryptographic Checksum Digital Signature	variable	Length depends on the algorithm. A typical value is 8 octets if used, and for a DS could be 48 or more octets; the minimum should be 4 octets.
Secured data		variable	Contains the Secured Application Message and possibly padding octets used for ciphering.

SPI (Security Parameter indicator) specifies the type of security protection applied to the Secured Packet.

- First octet gives information on the type of integrity (RC or CC, or DS or nothing), the presence or not of ciphering mode, the behavior of the counter.
- Second octet provides information on the type of the Proof of Receipt.

KIc and **KID** in the Security Header:
KIc indicates the key and algorithm for ciphering, KID indicates the key and algorithm for integrity protection. The allowed algorithms are DES (in CBC or ECB), 3DES (in outer-CBC mode using two or three different keys) or proprietary algorithms (e.g. AES).

<G+ answer>
At the moment the coding of KIc and KID specified in TS 102 225 allows the operator to choose between DES, 3DES and proprietary implementations. The proprietary implementation allows the operator to use another algorithm different from the DES and 3DES. So, the AES can be used within OTA security if the operator is interested in.
If SA3 decide to require the use of AES for MBMS, then all Rel-6 UICC cards will support AES and the OTA server will also contain AES algorithm.

OTA key set structure:

	Key Version Number n
	Counter_n
Key Identifier 1	KIc
Key Identifier 2	KID
Key Identifier 3	DEK

- The DEK is called KIK in previous versions of the specification.
- The OTA key version number ranges from ‘01’ to ‘0F’, the value ‘00’ is reserved.

Secured Data: contains secured Application Message and possibly padding octets used for ciphering.

Secured Response Packet

A similar structure applies to Secured Response Packet, which can be protected in confidentiality and integrity according to the required security. Cf TS 102 225.

2.2. Remote Management ETSI TS 102 226

ETIS TS 102 226 defines “Remote APDU structure for UICC based applications (Rel-6)” [2].

A Remote Management application is in the on-card Receiving application that performs either Remote File Management (RFM) or Remote Application Management (RAM).
The Remote Management application takes parameters from the “Secured Data”(containing either a single command or a list of commands) and acts upon the files or applications according to these parameters.

The Remote File Management (RFM) commands are as defined in TS 102 221 [3] and TS 102 222 [4].

The Remote Application Management (RAM) is under the control of a Security Domain and its commands follow GlobalPlatform Card Specification unless they are specially defined as not applicable or optional in TS 102 226. One of the RAM commands is the PUT KEY command dealing with key management.

A Minimum Security Level (MSL) is associated to any Receiving Application (e.g RFM or RAM); it specifies the minimum security to be applied to Secured Packets sent to the Receiving Entity. The Receiving Entity shall check the MSL before processing the security of the Command Packet.

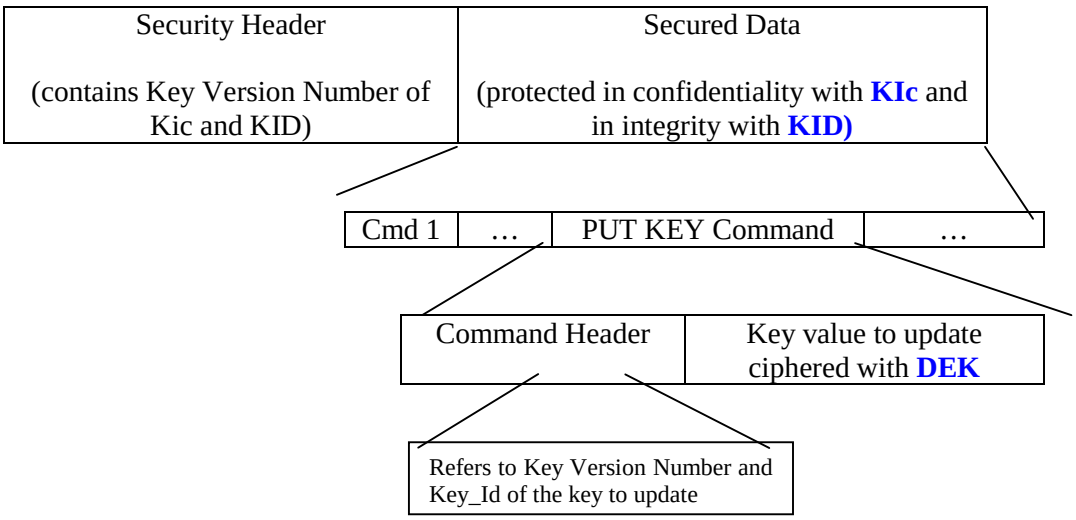
PUT KEY command

This command is used to replace or add key(s) within a key set, create a key set or update the key version number of a key set.

The key used for ciphering the key value of the PUT KEY command is the DEK (Data Encryption Key) of the OTA key set used to secure the Application Message.

The PUT KEY command is transmitted to the Remote Application Management by means of a Secured Packet.

- When replacing or adding a key within a key set, the DEK to be used corresponds to the key version number specified in the PUT KEY command header
- When creating a new key set, the DEK to be used corresponds to the key version number specified in the Command Packet containing the PUT KEY command.



3. OTA applied to MBMS

In MBMS context the Sending Entity is the MBMS Management Server implemented by means of an OTA server.

3.1. Overview of the MBMS Administrative Management

The MBMS UICC-based solution takes advantages of the existing OTA infrastructure and standardized commands to manage the MBMS Administrative data. Cf contribution on UICC-based solution [5].

According to the administrative procedure to realize, the BM-SC identifies the Administrative data to update on the UICC and send them to the OTA server.
After receiving the Admin data from the BM-SC, the OTA server identifies the Remote Management application to target (RAM or RFM), builds the Remote Management commands and formats them as Secured Packets to send to the UICC. It can ask the UICC to send back an acknowledgement, in which case the UICC formats a Secured Packet Response.

3.2. MBMS key set

At the T3 ad-hoc#101 meeting on MBMS issues, attendees agreed on the use of key set structure to store the MBMS Service Keys allowing the update of the MBMS Services Keys by means of the PUT KEY command.

The MBMS key set will have the following structure in order to apply the PUT KEY command to the MBMS key set.

MBMS key set

	Key Version Number n
	Counter_n
Key Identifier 1	RFU
Key Identifier 2	RFU
Key Identifier 3	MUK
Key Identifier 4	MSK_1
Key Identifier x	MSK_y

- The MUK has the role of the DEK and is used to update or create keys in this MBMS key set
- The MSKs can not be used to secure OTA messages

<Gemplus' answer>
RFU means Reserved For Future Use.

3.3. Other MBMS files

Two others types of files (record file) have been identified to deal with the OTA MBMS (cf T3#30 contributions [6]).

During an administrative procedure some fields of these files are updated by means of Remote File Management commands (e.g. Update Record,..) sent by the OTA in Secured Packet commands.

4. Security impacts

At SA3#32 meeting, Siemens presented a list of potential security impacts of the implied increased use of the OTA server. It was agreed that the protocols used need to be carefully studied.

Issue identified by Siemens:

> *"OTA mechanisms will become an interesting point of attack and a security hole will not only affect MBMS but also the other OTA users (e.g. the application download). From that point of view it would be good to used different security mechanisms/protocols for MBMS-key management and OTA, or as a minimum not rely on the same keys for transporting MBMS data and other application data towards the UICC".*

4.1. Protection of MBMS administrative data

For MBMS key management transport the UICC-based solution offers two levels of protection:

1. The OTA keys KIc and KID, can be used to protect in confidentiality and integrity the Application Message containing the Remote Management commands, e.g the PUT KEY command.

2. In the PUT KEY command the MBMS key value to update is encrypted with the DEK (Data Encryption Key) contained in the MBMS key set which is independent from the OTA key set.

So, the MBMS key management benefits from a dedicated encryption mechanism independent from the OTA mechanism.

<Gemplus' answer>

The PUT KEY command follows GlobalPlatform Card Specification. The algorithm to encrypt the key value depends on the choice of the operator; it could be 3DES or AES.

If MBMS requires the use of a specific algorithm, then all the PUT KEY commands used in the scope of MBMS will encrypt the key value with the chosen algorithm.

The MSK encryption with MUK could be performed either within the BM-SC or the OTA server. In case of MBMS service provided by the Home Network or roaming case where the Visited Network agrees the HN to know his MBMS Service Key, the best solution consists in performing the encryption within the OTA server.

MSL value:

The MSL (Minimum Security Level) associated to the Remote Application Management in charge of the MBMS key management is configurable (type of integrity check, the presence or not of ciphering, the behavior of the counter).

We recommend the operators to personalize MSL value with the higher level of protection (integrity and ciphering activated).

Algorithms (KIc and KID)

The KIc and KID fields in the Security Header specify the type of algorithm to use for ciphering (KIc) and integrity (KID). The use of 3DES shall be mandated for KIc and KID personalisation. The TS 33.246 already indicates that OTA shall not use DES in CBC for MBMS purposes.

Additional protection:
The UICC allows the creation of different OTA key sets. So, operators can create a dedicated OTA key (MBMS OTA key set) to transport the MBMS Secured Packets, the transport of other application data being protected with other OTA key sets.

<Gemplus' answer>
The creation of an OTA key set can be done over the air for all Rel-6-UICCs. For pre-Rel-6 UICCs, the creation of a dedicated OTA key set has to be performed during the personalization phase.

4.2. Security analysis

MBMS key management benefits from two independent security protections. To retrieve or modify MBMS Service Keys, an attacker will have to defeat the OTA security and the PUT KEY security.

The Minimum Security Level (MSL) to be applied to OTA messages is securely stored in the UICC, so it is not possible to decrease the level of protection of the OTA messages transporting the MBMS key management commands. The best level of protection consists in a MSL value personalized with ciphering and integrity activation.
<Gemplus' answer>
The MSL is assigned to each Receiving Application during the installation of this application on the UICC. The operator has the possibility to update Over The Air the MSL value; this update can only consist in increasing the security level required by the MSL.

The use of 3DES algorithm to protect in integrity and confidentiality the OTA messages will avoid retrieving the keys of the OTA key set since there is no applicative known attack on 3DES.

The transport of MBMS Service Key can be protected with a dedicated OTA key set. This MBMS OTA key set and the MBMS key set can also be stored in an independent Security Domain containing no other OTA key set.

5. Conclusion

The use of OTA mechanisms for MBMS does not lead to security hole.

6. References

[1] ETSI TS 102 225, "Secured Packet structure for UICC based applications", Rel-6 v6.0.6

[2] ETSI TS 102 226, "Remote APDU Structure for UICC based applications", Rel-6 v6.0.3

[3] ETSI TS 102 221, Smart Cards; UICC-Terminal interface; Physical and logical characteristics

[4] ETSI TS 102 222, Integrated Circuit Cards (ICC); Administrative commands for telecommunication applications

[5] TD S3-040xxx, S3#33, MBMS UICC-based solution, Axalto, Gemplus, Oberthur

[6] TD T3-030060 and TD T3-030061