Source: **Schlumberger, QUALCOMM, GEMPLUS, OCS**

Title: **3GPP Over the Air (OTA) procedures applied to BAK Distribution and MBMS Subscription management**

Document for: **Discussion and Decision**

Agenda Item: **MBMS**

1. Introduction

This contribution explains how existing 3GPP OTA mechanisms may easily be applied to BAK distribution and the other MBMS management operations that have been identified in the BAK scheme [6]. 3GPP OTA techniques provide a secure, simple, efficient and straightforward solution to MBMS key distribution and subscription management.

2. Contents

3. MBMS Management Operations

The APDU MBMSManagementOperation has been defined in the context of the BAK scheme for MBMS key management procedures [4] and do not require significant standardization efforts for Rel-6 USIMs. This new command is used in order to perform the following tasks

-UPDATE_BAK
-DELETE BAK
-SUBSCRIBE
-UNSUBSCRIBE
-UPDATE_SK_COUNTER
-RETRIEVE_SUBSCRIPTION_INFO

The following table summarizes what are the message data content of this APDU command.

Input: MBMSManagementRequest	TK_RAND, OP_Digest, (OP_Code, OP_Counter, OP_Body)*
Output: None | MBMSManagementResponse	TK_RAND, RES_Digest, (RES_Code, RES_Counter, RES_Body)*

*Encrypted with TK

A first estimation of the APDU length is depicted below. It uses OP_Code = UPDATE_BAK and its corresponding fields in OP_Body.

		Length (bytes)
APDU Header (CLA, INS, P1, P2, P3)		5
TK_RAND		8
OP_Digest		16
OP_Code		2
OP_Counter		2
OP_Body		~36
MBMS_ID	2 +2*	
BAK_ID	4 +2*	
BAK_VALUE	16 +2*	
BAK_Expire	6 + 2*	
Others + Padding		~11
TOTAL		~82

*corresponds to the Length & Value fields in the TLV objects

More details about this command can be found in [4].

4. Over The Air (OTA) mechanisms

3GPP OTA mechanisms enable an operator to remotely manage (U)SIM card updates including applet downloads, file management and other value added services in a rapid and cost effective way.

3GPP TS 31.115 [5] defines a “generalised secured packet structure” and the way that these secured packets can be delivered in both single or concatenated Point to Point Short Message (SMS-PP).

Short messages with protocol identifier set to “SIM data download” are delivered transparently by the ME to the UICC using the ENVELOPE (SMS-PP DATA DOWNLOAD) command. This procedure is described in 3GPP TS 23.040 [9] and TS 31.111 [10]

Each secured packet may contain one or more APDUs of those defined for file management or applet management as defined in TS 31.116 [12] For instance, the following file management input commands may be included as defined in [12]:

SELECT, UPDATE BINARY, UPDATE RECORD, SEARCH RECORD, INCREASE, VERIFY PIN, CHANGE PIN, DISABLE PIN, ENABLE PIN, UNBLOCK PIN, DEACTIVATE FILE

Note: OTA architecture uses SMS as a bearer. In the near future it will also be possible to use CSD or GPRS

4.1. Using OTA for MBMS Management Operation

OTA mechanisms can be considered as a good candidate for MBMS BAK distribution and related management operations. They provide a reliable point-to-point mechanism between the UICC and the operator’s network.

Moreover, as the existing 3GPP point-to-point mechanisms to communicate with the USIM will be used, changes in 3GPP specifications are reduced to:

- The new MBMSManagementOperation in the USIM for R6
- The inclusion of MBMSManagementOperation in the list of OTA commands for R6.

Furthermore, relying on the TS 31.115 security, OTA mechanisms for BAK distribution provides proven authentication, message integrity, replay detection, sequence integrity and message confidentiality mechanisms.

Using 3GPP OTA features for MBMS enables a maximum re-usage of the existing 3GPP infrastructure, as is depicted below:

- The BM-SC to send/receive requests. (MBMSManagmentOperation)
- An OTA gateway to process the request.
- An SMSC to send/receive requests to/from the wireless subscriber.
- Mobile equipment to receive the request and transmit it to/from the USIM card.
- A USIM card to receive and execute the request and delivers the response.

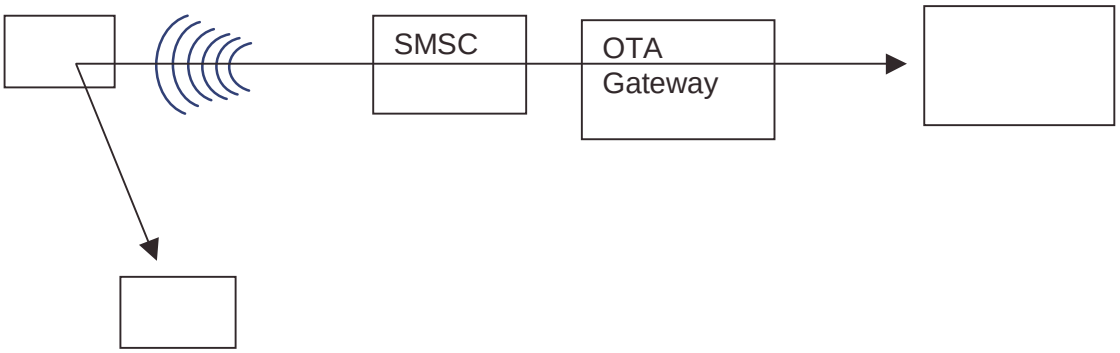

Fig 2: OTA in MBMS BAKManagement

This procedure is inline with the BAK distribution scheme proposed in the MBMS BAK key management scheme [4] as shown in the following figure.

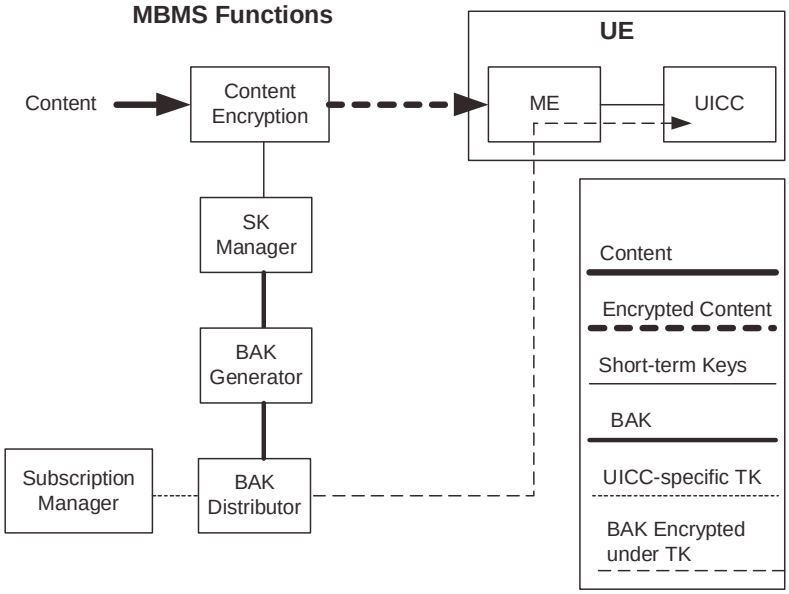

Fig 3: MBMS BAK/SK Management

4.2. Comparison with other point-to-point distribution schemes.

This section briefly compares the OTA mechanisms for BAK distribution with other point-to-point key distribution schemes that could be also applied for BAK delivery to the UICC.

An example of these other point-to-point mechanisms for key distribution was presented in the September 2003 GAA-MBMS ad-hoc meeting. This is shown in the following figure extracted from this document [11].

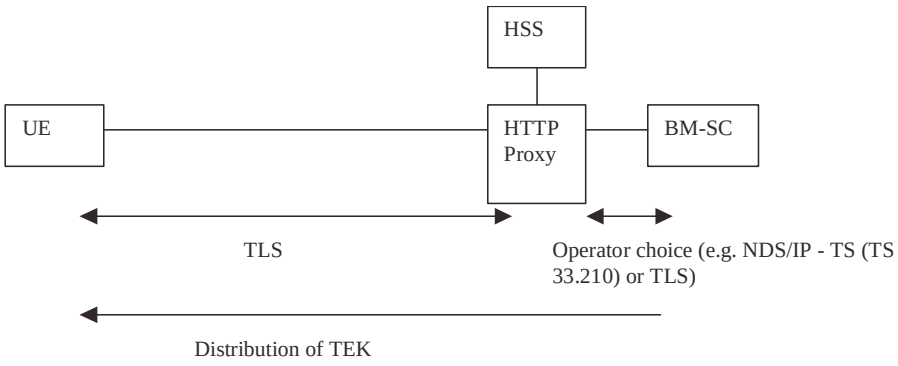

Figure 4: TEK distribution in GAA

Basically, this point-to-point scheme applies the Generic Authentication Architecture (GAA) in order to obtain shared keys to be used in the exchange between the BM-SC and the ME. Subsequently, the ME may perform the protected http requests/responses exchange with the BM-SC to get the TEK/BAK keys and other relevant parameters (e.g. keys id, expiration dates). It was also proposed to use the IETF draft MIKEY as key management scheme.

This approach retains major drawbacks when applied for TEK/BAK distribution: it is complex in terms of the new network entities involved and requires the usage of new IETF protocols (some of them yet a draft version) not especially adapted to the 3GPP BAK distribution needs.

For instance, this scheme necessarily ends in the ME, and some major points about the way that the BAK is delivered to the UICC are not defined (e.g. Does MIKEY enable the transmission of TK_RAND and encrypted BAK to the UICC?)

Moreover, this approach does not enable other MBMS Management operations (e.g. delete BAK, Update_SK_Counter...), which are only possible if the end-point of the encrypted data is the UICC.

Compared with this point-to-point key distribution scheme, MBMSManagement command by OTA offers major advantages:

-MBMSManagementOperation command can be performed in a single TS 31.115 secured packet, properly fitting in two short messages (one for the command packet and one for the response packet).

-Enables all the MBMS Management procedures (UPDATE_BAK, DELETE BAK, SUBSCRIBE, UNSUBSCRIBE, UPDATE_SK_COUNTER, RETRIEVE_SUBSCRIPTION_INFO)

-Reuses 3GPP standards and existing infrastructure (including the TS 31.115 security apparatus and the ME-to-UICC delivery mechanism).

5. Conclusion

OTA mechanisms are the existing 3GPP standard way for point-to-point communication between the UICC and the network and provide all the functionality required for efficient, secure MBMS key management. It is proposed to reuse these existing 3GPP mechanisms for BAK distribution and MBMS management operations instead of reinventing new ones.

6. References

[1] 3GPP TS 22.146: "Multimedia Broadcast/Multicast Service; Stage 1".

[2] 3GPP TR 23.846: " Multimedia Broadcast/Multicast Service; Architecture and Functional Description".

[3] 3GPP TS 33.246, Technical Specification Group Services and System Aspects; Security; Security of Multimedia Broadcast/Multicast Service;

[4] USIM Enhancements for MBMS Support, S3z030009.

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

[6] S3z030007 Pseudo-CR to 33.246: MBMS Security Architecture.

[7] ETSI TS 102 221. Physical and logical characteristics

[8] 3GPP TS 31.102. Characteristics of the USIM Application

[9] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)".

[10] 3GPP TS 31.111: "USIM Application Toolkit (USAT)".

[11] S3z030027 Introducing MIKEY in TS 33.246

[12] 3GPP TS 31.116: “Remote APDU Structure for (U)SIM Toolkit applications”