3GPP TSG SA WG3 Security — S3#32 **S3-040098**
9-13 February 2004
Edinburgh, UK

Source: **Siemens**

Title: **MBMS: OTA security considerations**

Document for: **Discussion and decision**

Agenda Item: **6.20 (MBMS)**

1 Introduction

This contribution investigates the OTA-security mechanisms as available in ETSI TS 102 224/5/6 ([1], [2], [3]) in more detail. Some recommendations are derived from it.

2 OTA security considerations

Issue-1: The OTA mechanisms for transporting keys to the UICC still allow the use of DES.

ETSI TS 102 225 v6.2.0 [2] on secure packet structure for UICC based applications specifies a key hierarchy in annex A of [2] and algorithms use within section 5 of [2]. DES, 3DES or proprietary algorithms can be used. Triple-DES is secure but the use of DES shall be abandoned. No security statement can be given about 'proprietary' algorithms but using them shall not be encouraged.

Annex A of the specification [2] actually describes a multi-level key hierarchy which is applicable only to cards conformant to the GlobalPlatform Specification[1]. The key set version 0[2] serves as the fixed root key that is used for transporting the second level key KIK[3] n for key set version n to the UICC. This key KIK n then is used to transport keys KIc n, and KiD n securely to the UICC. If the above understanding is correct then one of the available key set versions n would be used to transport the MBMS master key to the UICC. It is unknown what security mechanisms are used for cards not conforming to the Global Platform Specification.

Issue-2: Different subscribers shall use different keys for key set version 0

The specification [2] is unclear about whether the key set version 0 is subscriber specific, shared by a group of subscribers or subscriber specific. Clearly from an MBMS point of view, a subscriber specific assignment would be desirable as otherwise an algorithm weakness on the top level key distribution (e.g. by using a weakened algorithm like DES) or a successful physical attack on one card will affect all applications and many users relying on the security of the OTA mechanism.

If the OTA-mechanism would be used for MBMS then following recommendations are proposed for TS 33.246:

---

1 It should be noted that there exist also non globalplatform/proprietary cards on the market. It was mentioned via the SCP2 posed questions that key set version 0 handling behaviour is likely to be different for these card.

2 It was mentioned on the SCP2 mailing list that for some cards, Key set version 0 is not available.

3 Called also DEK (data encryption key) within the Global platform card specification 2.1.1

REC-1: 'OTA should not use DES in CBC mode for transporting new key set versions to the UICC'.

REC-2: 'The used keys for any key set version shall not be shared among subscribers'.

While the conforming to REC-2 is desirable from a security point of view, it may have an undesirable effect in the Home Network. It creates a database of permanent longer-term secrets that have to be managed by the Home Operator. The level of security that has to be provided for the key version number 0 keys (and key version n keys), which have to be stored in the HN, has to be at the same security level as the long term UMTS key K that is stored at the AuC. If pre-Rel6 UICC-cards are not in accordance with the proposed REC-2 then they would have to *be re-provisioned*, even if they would be OTA-capable.

If the understanding of the Annex A mechanism was correct, then a UICC that was not pre-provisioned with key set version 0 for use with OTA (A Pre-Rel-6 card) cannot update key set versions n KIKs over the Air [2].

It was mentioned on the SCP2-mailing list that most operators use card individual keys, and as such need a database for all of these keys. Other operators use one Master key, and use some extra data (e.g. ICCID) to derive card individual keys from it.

Issue-3: Limiting the effects of security breaches.

An important security design issue is to limit the effects of security breaches of one protocol spreading over to other domains.

The use of MBMS will generate a lot more key update and key management messages towards the UICC. Therefore attackers will have much more information available to attack the OTA-messages in order to reveal the keys. OTA is currently used to transport applications and many other data settings to the UICC. Consequently the OTA mechanism 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 (1) it would be good to use different security mechanisms/protocols for MBMS-key management and OTA, or as a minimum (2) not to rely on the same keys for transporting MBMS data and other application data towards the UICC.***[4] SA3 should decide whether to follow approach (1) or (2). A possibility to realize the latter might be to bootstrap a key to the UICC and use this key for MBMS-OTA messages exclusively. GBA_U is described within a companion Siemens contribution to this meeting.

3 Conclusion

This contribution derived several security recommendations when using OTA for MBMS key management. It is proposed (under the assumption that OTA would be selected)

- to incorporate these recommendations into TS 33.246.
- that SA3 decides on the best strategy in fulfilling Issue-3 and document it within the technical Specification. The contribution mentioned two possible approaches.

[4] The Globalplatform specification allows the use of separate security domains ***(http://www.globalplatform.org). But not all cards follow the global platform specification***

Annex A: Relevant information from ETSI TS 102 225 v6.2.0

A.1 Key set version - counter association within a Security Domain

A separate and different counter shall be associated to each key set version as described in table A.1.

Table A.1

	Key Set Version 0	**Key Set Version 1**	....	**Key Set Version n (maximum 'F')**
	Reserved	**Counter 1**		**Counter n**
Key Index 1	Reserved	KIc 1		KIc n
Key Index 2	Reserved	KID 1		KID n
Key Index 3	Reserved	KIK 1		KIK n

A.2 Security keys KIc, KID

The indication of the key to be used in the KIc and KID fields shall refer to an GlobalPlatform key set version number.
The algorithm to be used with the key shall be the algorithm associated with the key (as described in the Open Platform Card specification [6]).
The key set version number indicated in the KIc and KID fields shall be identical when different from 0. If the key set version numbers are different (and both different from 0) then the message shall be rejected with the "Unidentified security error" Response Status Code.

Section 5.1.2 Coding of the KIc

The KIc is coded as below.
b2 b1
00: Algorithm known implicitly by both entities
01: DES
10: Reserved
11: proprietary Implementations
If b2 b1 = 01 (DES), b4 b3 shall be coded as follows:
00: DES in CBC mode
01: Triple DES in outer-CBC mode using two different keys
10: Triple DES in outer-CBC mode using three different keys
11: DES in ECB mode
If b2 b1 = 10, b4 and b3 coding is reserved.
indication of Keys to be used
(keys implicitly agreed between both entities)

DES is the algorithm specified as DEA in ISO 8731-1 [3]. DES in CBC mode is described in ISO/IEC 10116 [4]. Triple DES in outer-CBC mode is described in clause 15.2 of [7]. DES in ECB mode is described in ISO/IEC 10116 [4].

The initial chaining value for CBC modes shall be zero.

Similarly also the key KID is used with DES, triple DES or proprietary algorithm.

Annex B: References

[1] ETSI TS 102 226 v6.4.0 Smart Cards; Remote APDU structure for UICC based applications (Release 6).

[2] ETSI TS 102 225 v6.2.0 Smart Cards; Secured packet structure for UICC based applications (Release 6).

[3] ETSI TS 102 224 v6.0.0 Smart cards; Security mechanisms for UICC based application: functional requirements (Release 6).