3GPP TSG SA WG3 Security — S3#34 **S3-040xxx**
6 - 9 July 2004
Acapulco, Mexico

Source: **AXALTO, GEMPLUS, OBERTHUR**

Title: **UICC-ME interface for MBMS**

Document for: **Discussion and decision**

Agenda Item: **GBA**

1 Introduction

At SA3 #33 it was agreed that the GBA was to be used for MBMS Security for both MSK management and MTK derivation.

The description of the message needed in the ME-UICC for both procedures is not yet included in the current version of the 33.246. It is proposed to include a description of the involved exchanges in TS 33.246 annexe. This is presented in section 2 as a pseudo CR.

Some open issues are discussed in section 3. The solution for them may involve changes in the proposed pseudoCR before being finalised and approved.

Taking into account the schedule constraints for Rel-6, it is also suitable to inform the involved working groups of the final result of this interface description.

2 PSEUDO CR

Annex D (normative): UICC-ME interface

D.1. MSK Update Procedure

This procedure is part of the MSK update procedure as described in 6.3

The ME has previously performed a GBA_U bootstrapping procedure as described in 33.220 [1]. The UICC stores the corresponding Ks_int_NAF together the transaction identifier, Key Life Time and the NAF_Id associated with this particular bootstrapping procedure.

The ME receives a MIKEY message containing an MSK update procedure. After performing some validity checks, the ME sends the whole message to the UICC. The ME also includes in this request NAF_Id to identify the stored Ks_int_NAF.

The UICC then uses Ks_int_NAF as the MUK value for MGV-S as described in chapter 6.3

After successful MSK Update procedure the UICC stores the Service_ID, MSK_ID, MSK, MSK Validity Time and SEQs.

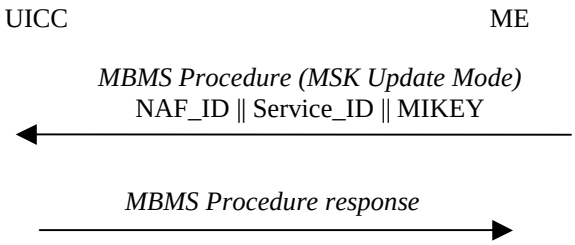

Figure x: MSK Update Procedure

Format of MSK Update procedure data:

- NAF_ID: arbitrary-length bit-stream
- Service_ID: arbitrary-length bit-stream
- MIKEY message: tbd
- SEQs: 16-bit

…

D.2. MTK generation and validation

This procedure is part of the MTK generation and validation function as described in 6.4

The ME receives the MIKEY message (Header, Time stamp, MSK ID, MTK ID = SEQp, MGK[MTK] and MAC). After performing some validity checks, the ME sends the whole message to the UICC. The ME also includes in this request the Service ID.

The UICC computes the MGV-F function as described in section 6.4. After successful MGV-F procedure the UICC returns the MTK.

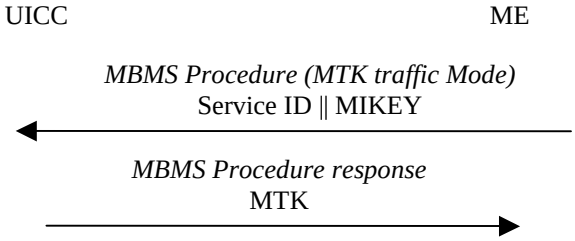

Figure x: MTK Generation and Validation

Format of MTK generation and validation data:

- Service ID: tbd
- MIKEY message (Heater, Time stamp, MSK ID, MTK_ID, MGK[MTK], MAC):
- MTK: 128-bit key
- SEQs: 16-bit
- SEQp: 16-bit
-

3 OPEN ISSUES

Some details of the MBMS key management procedures are still missing in current TS 33.246. Here is a list of open issues:

1- Exact format of MIKEY message for MSK update procedure:

The proposal in S3-040258 was considered to be the guide for further MIKEY adaptations for MSK update and this needs to be included in TS and further detailed:

a. S3-040258 mentions the use of MUK_A and MUK_E: the TS should describe the way these keys are derived and used for MSK transport.

b. The size of the different fields has to be defined.

c. Acknowledge generation in the UICC is not included in TS but described in S3-040258. This has to be defined, if needed.

d. Is Service ID included in clear text in MIKEY message or concatenated to MIKEY message in the input data of the MSK Update procedure?

2- Exact format of MIKEY message for MTK generation and validation is included in TS:

Example from section 6.4 of TS *"MIKEY message (including e.g.Header, Time stamp, MSK ID, MTK ID = SEQp, MGK[MTK], MAC)"*

a. Content of MIKEY message need to be further described.

b. Is Service Id included in MIKEY?

c. Acknowledge generation in the UICC is not included in TS but described in S3-040258. This need to be defined, if needed.

d. Are Ff, Fg, Ft, Fm of MGV-F operator dependent functions or specified by ETSI SAGE group?

3- TD S3-040259 proposed a Key Deletion function. Details of this procedure are not yet included in TS.

4 Conclusion

Taking into account the schedule constraints for Rel-6, we kindly ask SA3 to complete SA3 CR at SA3#34 meeting and inform involved working groups of the final result of the ME-UICC interface for MBMS.

5 References

[1] 3GPP TS 33.220 v6.1.0 (2004-06) "Generic bootstrapping architecture (Rel-6)"