3GPP TSG SA WG3 Security — S3#34 **S3-040499**

July 6 - 9, 2004

Acapulco, Mexico

Source: **AXALTO, GEMPLUS**

Title: **UICC-ME interface for GBA-U**

Document for: **Discussion and decision**

Agenda Item: **GBA**

1 Introduction

At SA3#33 the concept of GBA_U was approved and introduced in TS 33.220 [TD S3-040413] .

The description of the message needed in the ME-UICC for GBA_U is not yet included in the current version of the TS. It is proposed to include a description of the involved exchanges in TS 33.220 annexe. This is included in section 2 as a draft CR.

Some open issued are discussed in section 3. The solution for them may involve changes in the CR before being finalised and approved. A CR for approval could be delivered in SA3#34 based on discussion and resolution on the pending issues.

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 DRAFT CR

Annex D (normative): GBA_U UICC-ME interface

This section describes the UICC-ME interface to be used when a GBA_U aware UICC application is active and the ME is involved in a GBA bootstrapping procedure. When the UICC application is not GBA_U aware, the ME uses AUTHENTICATE command in non-GBA_U security context (i.e. UMTS security context in case of USIM application and IMS security context in case of the ISIM) as defined in 31.102 [ ] and 31.103 [ ].

D.1. GBA_U Bootstrapping procedure

This procedure is part of the Bootstrapping procedure as described in section 5.3.2

The ME sends RAND and AUTN to the UICC and performs the Ks_ext and Ks_int derivation as described in 5.3.2.

The UICC then stores Ks_ext and Ks_int. The UICC also stores the used RAND to identify the current bootstrapped values. RAND value in the UICC shall be further accessible by the ME.

Editor’s note: The storage of Ks_ext on the UICC depends on SA3 decision.

The ME then, finalizes the Bootstrapping procedure and stores in the UICC the Transaction Identifier and Key Life Time associated with the previous bootstrapped keys (i.e. Ks_int and Ks_ext). Transaction Identifier and Key Life Time values in the UICC shall be further accessible by the ME.

At the end of the GBA_U bootstrapping procedure the UICC stores Ks_ext, Ks_int, Transaction Identifier, Key Life Time and the RAND.

A new bootstrapping procedure replaces Ks_ext, Ks_int, TId, Key LifeTime and RAND values of the previous bootstrapping procedure.

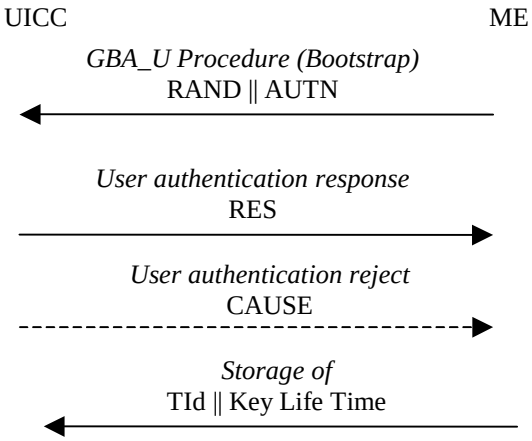

Figure x: GBA_U Bootstrap Procedure

Format of GBA_U bootstrapping procedure data:

- RAND: tbd
- AUTN: Cf TS 33.102
- RES: authentication response of AKA procedure (as defined in TS 33.102) followed with flipping of the least significant bit. RES shall have a variable length of 4-16 octets
- User authentication reject CAUSE: tbd
- Ks_ext: 256-bit key
- Ks_int: 256-bit key

D.2. GBA_U NAF Derivation procedure

This procedure is part of the Procedures using bootstrapped Security Association as described in section 5.3.3

The ME sends NAF_ID and IMPI to the UICC. The UICC then performs Ks_ext_NAF and Ks_int_NAF derivation as described in 5.3.2. The UICC uses the RAND, Ks_ext and Ks_int values stored from the previous bootstrapping procedure. The UICC returns Ks_ext_NAF to the ME and stores Ks_int_NAF together with NAF_Id.

Note: A previous GBA_U Bootstrap needs to be undertaken before. If a Ks_int, Ks_ext pair is not available in the UICC, the command will answer with the appropriate error message.

Editor's note: The storage of Ks_ext (either in ME or in the UICC) depends on SA3 decision

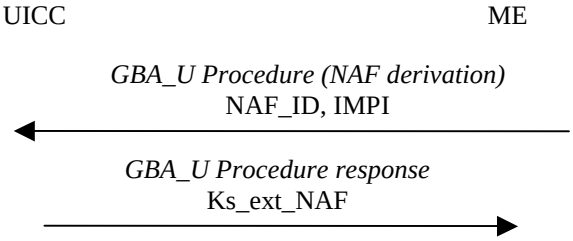

Figure x: GBA_U NAF derivation procedure

Format of GBA_U NAF derivation data:

- NAF_ID: arbitrary-length bit-stream
- IMPI: arbitrary-length bit-stream
- Ks_ext_NAF: 256-bit key

3 OPEN ISSUES

Some details of the GBA_U mechanism are still missing in current TS 33.220. Here is a list of open questions:

1- The structure of GBA_U-AV

2- Input parameters of h1 and h2 functions

3- The size of the data involved in the bootstrapping procedure and the GBA_U NAF derivation procedure has to be defined

4 Conclusion

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