3GPP TSG SA WG3 Security — S3#34 **S3-040576**

July 6 - 9, 2004 **comment to S3-040491**

Acapulco, Mexico

Source: **Siemens [commented by AXALTO]**

Title: **GBA: The support of GBA features within a Rel-6 ME**

Document for: **Discussion and decision**

Agenda Item: **GBA**

1 Introduction

In SA3#33 Gemplus did provide a commented contribution S3-040350 (comments to the contribution S3-040218 and S3-030217 on GBA) stating that a GBA-aware ME shall support both GBA_U and GBA_ME. This paper analyses the rationale for and the consequences of this requirement, taking into account the arguments that were exchanged during SA3#33 discussions. The discussion in this paper has intentionally not been related to MBMS as for MBMS there has been agreement that an MBMS ME has to support both GBA-variants.

2 Summarizing the known issues

From S3-040350: *"GBA is a Rel-6 feature without legacy issue. So, we propose that a GBA-aware ME shall support both GBA_ME and GBA_U interface procedure in order to avoid security issues."*

Response from Siemens in S3-040346*: "Modularity in terminal feature implementation could be a reason to allow Rel-6 terminals not to implement GBA_U interfaces".*

Arguments included within the SA3#33 meeting report (S3-040451)*: "TD S3-040350 GBA_U: comments to S3-040217 and S3-040218. This was introduced by Gemplus and proposed that as GBA is a Rel-6 feature without legacy issue, that a GBA-aware ME shall support both GBA_ME and GBA_U interface procedure in order to avoid security issues. Siemens commented that "in order to avoid security issues" was confusing, as this requirement was not a security issue. Gemplus stated that having GBA_U on the ME would allow flexibility for future applications and provide a minimum level of Security for the applications. After some discussion it was decided that this requires further study and will be addressed at the next meeting."*

3 Looking at the ME-UICC interaction

This section start with first giving an overview on the features that can use GBA in a Rel-6 ME. Thereafter, a closer look is taken at the different steps an ME has to take to generate and use Ks_xx_NAF keys. Finally we relate the findings towards the Rel-6 features.

A Rel-6 ME and GBA:

1) It should be possible to bring lower-cost mobiles on the market that have dedicated limited functionality e.g. a Rel-6 ME that is manufactured for VGCS (ciphering) or GSM-only ME shall not be obliged to implement GBA.

2) Following functions of Rel-6 features currently are designed to make use of GBA-secrets (described from ME point of view)

a) Administration via Ut-reference point (Protocols PSK-TLS, http digest authentication); The ME acts as endpoint.

b) MBMS key management (used within MIKEY); Both ME and the UICC can be the security endpoint.

c) MBMS http communication (http digest authentication); The ME acts as endpoint.

d) Subscriber Certificates Enrolment towards the ME (http digest authentication or PSK-TLS); The ME acts as endpoint.

The different steps an ME has to take to generate and use Ks_xx_NAF keys:

Figure 1 describes the steps that are involved within a GBA_U bootstrapping. Three steps can be distinguished. Step-1 includes the known AUTHENTICATE call to the UICC. Step-2 would be needed for Ks_int_NAF-key derivation (and storage) on the UICC. A subsequent step-3 would involve the use of an application on the UICC (E.g. for MBMS this is the MSK key management). When only Ks_ext_NAF would be needed, a step-2 call is not necessary from a functional point of view.

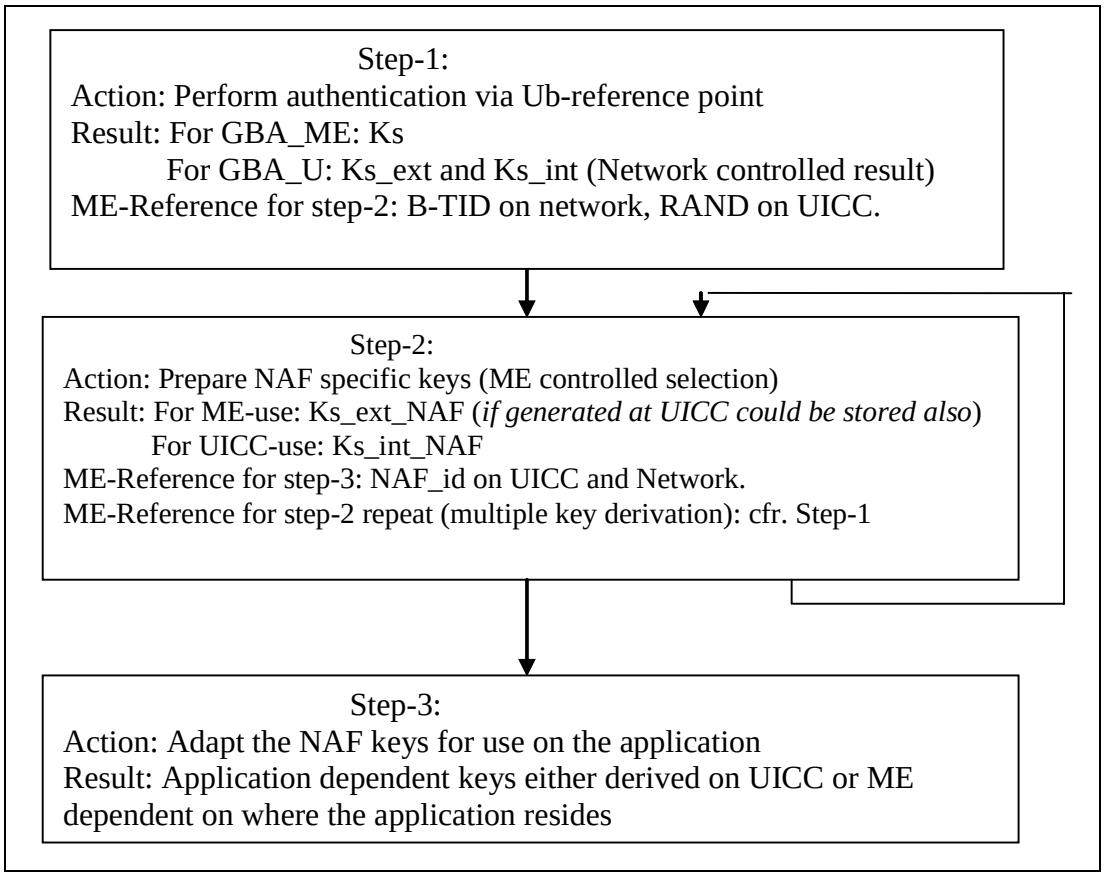

Figure 1: Different steps involved for setting up and using GBA_U secrets

Let us now try to clarify what is meant by '*GBA_ME and GBA_U interface procedure'*.

An ME that supports only GBA_ME needs only to support step-1 (as a minimal) above and therefore needs to support the AUTHENTICATE command to the UICC in UMTS security context. In addition, this ME needs to support the key derivation functions on the ME (TS 33.220 Clause 4) in order to derive Ks_NAF. If a GBA aware UICC is put into the ME, this ME can still behave the same. If this ME would support step-2 procedures (but no step-3 procedures), any generated Ks_int_NAF would be of no use. The UICC could generate the key Ks_ext_NAF on behalf of the ME and store it. The execution of a step-2 call to

the UICC does have the disadvantage of adding an additional processing delay (calling a UICC function) for the Ua-interface.

As can be seen from the Figure 1, the additional procedure that is needed for GBA_U, is the step-2 interface procedure. An **ME that supports GBA_U** shall support both step-1and step-2 procedures. But steps 2 and 3 may be executed by /combined with calling one or more applications. The more steps are combined, the more specific the application is. Steps 2 and 3 for UICC-use would return no Ks_xx_NAF values to the ME. Only if the UICC would function as a storage for Ks_ext_(NAF), the Ks_ext_NAF could be returned within a step 2.

From this there are several possibilities for the realization of the step 2 and 3:

The ME calls an application-specific function on the UICC. This is the only case we will have in Rel-6. The example is MBMS where the ME sends (amongst other input parameters) the encrypted MTK and the NAF_Id to the UICC and retrieves the MTK.

The ME calls a generic function on the UICC, e.g. a generic encryption function, which may include NAF specific key derivation (step-2). This will not be specified in Rel-6 and more discussion is needed on the requirements for the generic functions.

The Rel-6 Features and support for GBA_U interface procedures:

For the cases a, c and d, the mandatory implementation of GBA_U procedures on the ME will **not enhance security** if either the UICC or the ME do not support the security applications that provide the inputs to the protocols that have their endpoints at the ME. Such UICC applications are not planned with Rel-6 timeframe (exception: MBMS MSK/MTK decryption).

This leads to following conclusion:

Even if we do mandate that a Rel-6 ME supports step-2 interfaces procedures separately, **GBA_U support on the ME will not be useful until there is an UICC application that can make use of it** and the ME supports these application interface functions. At that time even the decision can be taken to integrate Step-2 and Step-3 procedures. So the logic for deciding whether the ME shall support Step-2 interface procedures seems to be the following. **If the ME has to work together with an UICC-application that makes use of Ks_int_NAF then the ME has to support the GBA_U interfaces towards the UICC in addition to the application interfaces to the UICC if they would be specified and used separately**.

4 Conclusions

In order for the UE to take advantage of the GBA_U key Ks_int_NAF, the UE needs to have an application that uses the Ks_int_NAF. For the mentioned Rel-6 applications in section 3 this may mean the availability of some generic cryptographic functions on the UICC that can make use of the Ks_int_NAF. These UICC functions are not yet available for Rel-6 and it is probably too late to start standardization on this. In the absence of such UICC-applications the support of ME-UICC interfaces procedures (step-2) at the ME for these functions has no added value as Ks_ext_NAF has to be used anyhow. Furthermore it was indicated that second separate UICC call adds an additional processing delay at Ua-reference point which can be avoided.

Therefore it is proposed that Rel-6 ME that does not support MBMS, need not support any GBA_U interface procedures.

A CR to TS 33.220 is available in a companion contribution to SA3#34.

References

[1] S3-040350: SA3#33, Gemplus, GBA_U: comments to S3-040217 and S3-040218

[2] S3-040218: SA3#33, Siemens and Ericsson: GBA_U: Bootstrapping secrets to the UICC