3GPP TSG SA WG3 Security — S3#33 **S3-040350**
10 - 14 May 2004
Beijing, China

Source: **Gemplus**

Title: **GBA_U: comments to S3-040217 and S3-040218**

Document for: **Discussion and decision**

Agenda Item:

Abstract

This contribution proposes some improvements to GBA_U proposal.

1. Introduction

In the scope of GBA work item, SA3 agreed as a working assumption that the GBA_U is added as a generic mechanism, it is for further study to decide if it could be used for MBMS. Contributions S3-040217 [1] and S3-040218 [2] propose a GBA_U concept description. This contribution provides some security enhancements to the GBA_U proposal.

2. GBA-U concept description

Initial statements were:

- GBA_ME: the ME receives CK and IK from the UICC and concatenates these keys to form Ks. This and all further key derivation functions are implemented within the ME.

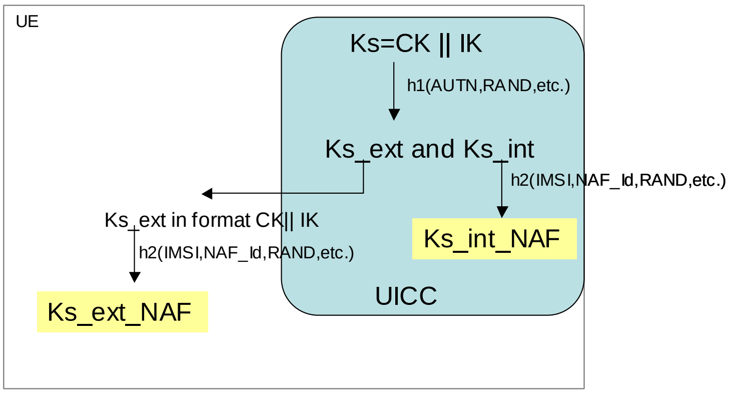
- GBA_U: the key Ks shall never leave the UICC. For some application (ME security services) a key Ks_ext_NAF is needed within the ME. For other applications (UICC security services) a key Ks_int_NAF shall not be made available to the ME. A GBA_aware UICC shall be able to supply keys to both types of services.

S3-040218 [2] propose solutions, S3-040217 [1] is a CR to TS 33.246 corresponding to this proposal.

S3-040218 proposal:
The contribution provides the following description:

UICC derives both Ks_int and Ks_ext, whereby Ks_ext is given to the ME and whereby the key Ks_int is kept secret within the UICC. When the

- *When the ME wants to use Ks_ext for ME security service then it performs a key derivation step that is implemented on the ME to obtain Ks_ext_NAF.*
- *When the UICC wants to use Ks_int for UICC security service then it performs a key derivation step to obtain Ks_int_NAF. This key derivation is implemented on the UICC. The derivation of keys Ks_int and Ks_ext can done by the UICC as a result of one call to the UICC (very similar to Rel99 authentication), and the derivation of Ks_int_NAF from Ks_int is then done as a result of a second call to the UICC which includes the key derivation parameters (NAF id etc).*



In this proposal the GBA_aware UICC sends Ks_ext to the ME which performs the Ks_ext_NAF derivations. This description does not correspond to initial proposal S3-040095 presented at SA3#32 saying that Ks=CK|| IK did not leave the UICC and the Ks_ext_NAF computation took place on the UICC.

In the current GBA_U concept, Ks_ext is stored on the ME used to derive the Ks_ext_NAF keys, the retrieval of Ks_ext on the ME allows to deduce all the NAF-specific keys. The level of security associated to Ks_ext is the same as for GBA_ME case.
The storage of Ks_ext on the UICC avoids deducing Ks_ext_NAF value from key derivation parameters (IMSI, NAF_Id, RAND, etc). Moreover, the lifetime of Ks_ext could be longer if Ks_ext were stored on the UICC. So, the security level associated to Ks_ext is higher if this key is stored on the UICC. The GBA-aware UICC would send Ks_ext_NAF as a second call to the UICC which includes the key derivation parameters (IMSI, NAF_Id, RAND, etc).

3. GBA-aware ME

S3-040218, section 2.4, tries to solve the case of a GBA-aware UICC inserted into a ME that does not support the GBA_U procedure to derive Ks_int_NAF from Ks_int on the UICC. The contribution provides two solutions:

- The first solution proposes that the NAF could rely on the fact that the NAF-application has knowledge of the UE feature support of that application. The way that the NAF obtains UE required feature knowledge is out of scope of the GBA_U scope and would be addressed in the respective application
- The second solution proposes the use of a GBA_U request flag on the Ub-Interface with the following interpretation: *"An ME supporting GBA_U UICC interface procedures will set the flag on Ub"*. .
  This solution is not the preferred one since there are no advantages seen in using a GBA_U request flag on the Ub-interface.

Here are some issues related to the 2 proposed solutions:

GBA_U usage depending on ME information
The use of GBA_U shall not depend on information coming from the ME since the ME could be a fraudulent device. A possible attack consists in having a ME that claims that it does not support GBA_U, then the NAF has not longer choice between GBA_U and GBA_ME, it will continue the process with the lower level of security or will not provide the required service. E.g. in MBMS context the user is a potential attacker so the attack on the ME is feasible, it would oblige the delivery of low value content only and there would be roaming issues in case of Visited Network mandating UICC-based only solution to protect its MBMS Service Keys.

NAF obtains UE required feature knowledge
In the previous paragraph we show that information coming from the ME cannot be trusted. Moreover, the network has not information on the GBA_U capability of the ME of the user's UE, the Home Network does not store information related to the UE features of a user since the UICC is a portable device. So, it seems difficult to provide the NAF with trusted information on the GBA_U capability of the ME.

Proposal:
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.

4. Conclusion

The security level offers by GBA_U is increased if Ks_ext does not leave the UICC and if all GBA-aware ME support both GBA_ME and GBA_U interface procedures

So, we kindly ask SA3 to adopt these proposals for the definition of GBA_U concept as generic mechanism.

5. References

[1] TD S3-040217, "Introduction of a UICC-based Generic Bootstrapping Architecture", Siemens

[2] TD S3-040218, "GBA_U: Bootstrapping secrets to the UICC", Siemens Ericsson