3GPP TSG SA WG3 Security — S3#34 **S3-040498**

July 6 - 9, 2004

Acapulco, Mexico

Source: **Gemplus, Axalto, Oberthur**

Title: **GBA: GBA_U derivations**

Document for: **Discussion and decision**

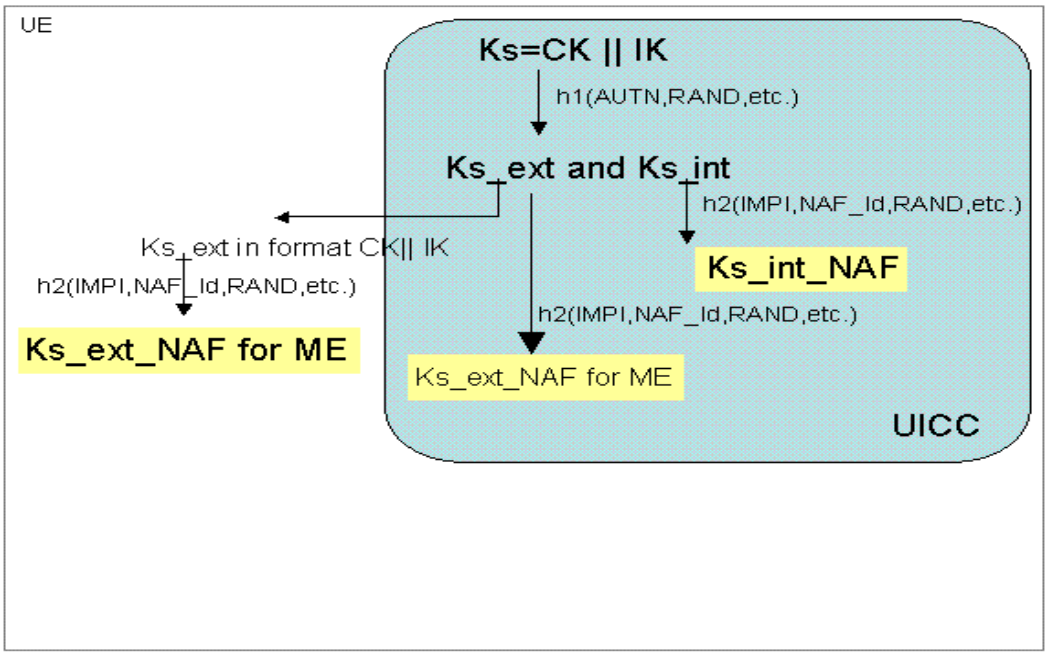
Agenda Item: **GBA**

1. Introduction

The current version of TS 33.220 "Generic Bootstrapping Architecture" mentions that the location (whether in the UICC or in the ME) of the storage of Ks_ext is for further study. This contribution proposes some elements of comparison in order to select the location of Ks_ext storage.

2. Current status of GBA-U key derivation

The current TS 33.220 [1] proposes the following key derivations for GBA-U:



The TS states that:

- The location (whether in the UICC or in the ME) of the storage of Ks_ext is for further study.

- When the UE is powered down, or when the UICC is removed, any GBA_U keys shall be deleted from storage in the ME. There is no need to delete the keys Ks_int and Ks_int_NAF from storage in the UICC.

3. Elements of comparison

During SA3#33 meeting some elements of comparison were provided in order to select the location of the storage of Ks_ext for GBA-U.

Ks_ext key lifetime:

- Scenario 1: Ks_ext stored on the ME
  Ks_ext shall be deleted when the UE is powered down or when the UICC is removed.

- Scenario 2: Ks_ext stored on the UICC
  There is no need to delete Ks_int and Ks_ext from the UICC in case of UE power down or UICC removal. Only, the Ks_ext_NAF key stored on the ME shall be deleted.

  So, the key lifetime of Ks_ext is longer with K_ext storage on the UICC, this leads to:
  - Decrease the frequency of bootstrapping procedures
  - Decrease the consumption of authentication vectors

Ks_ext availability

Ks_ext_NAF are derived from Ks_ext, they are computed as Ks_ext_NAF = h2 (Ks_ext, h2-key derivation parameters) where the h2-key derivation parameters include IMPI, NAF_Id and RAND.

- Scenario 1: Ks_ext stored on the ME
  Attacks on ME are possible, so the retrieval of Ks_ext, Ks_ext_NAF keys, IMPI and RAND is possible. The same value of IMPI and RAND is used as h2-key derivation parameters for all Ks_ext_NAF computation. So, an attacker, who accesses one time Ks_ext, IMPI and RAND on the ME during the key lifetime of Ks_ext, is able to compute/deduce Ks_ext_NAF of any NAF since he only requires the NAF_ID value to perform h2(Ks_ext, IMPI, NAF_ID, RAND). The attacker could use these Ks_ext_NAFs to send authenticated application requests to new NAFs.

  Moreover, the level of security of Ks_ext_NAF with GBA_U is the same than the security level of Ks_NAF with GBA-ME.

- Scenario 2: Ks_ext stored on the UICC
  Attacks on ME allow retrieving the IMPI and RAND values used as h2-key derivation parameters and all the Ks_ext_NAF keys available on the ME. But, an attacker cannot compute/deduce the value of a Ks_ext_NAF corresponding to a new NAF, since the attacker does not know Ks_ext. So, he cannot send an authenticated application request to new NAFs.

  So, the security level is higher in case of Ks_ext storage on the UICC.

ME not implementing GBA-U

- Scenario 1: Ks_ext stored on the ME
  A GBA-aware UICC gives Ks_ext to the ME. This scenario allows handling the situation where an ME (with only GBA_ME function implemented) does not know that a GBA-aware UICC has been inserted.

- Scenario 2: Ks_ext stored on the UICC
  A GBA-U aware UICC does not provide Ks_ext to the ME and sends Ks_ext_NAF during the second run of the bootstrapping procedure. A ME, which does not support GBA_U capabitlities, could not derive the correct Ks_ext_NAF.

  This issue only exists in case of Rel-6 GBA-capable MEs not supporting GBA-U. But this scenario is not yet decided and depends on SA3 decision, a SA3#34 contribution on "GBA_U in Rel 6 MEs » [2] is proposed for discussion. So, if SA3 decide that Rel-6 GBA-capable MEs shall support both GBA-ME and GBA-U, the issue described in previous paragraph is not longer relevant.

4. Conclusion

In case of Rel-6 ME supporting both GBA_U and GBA_ME, the location of Ks_ext storage in the UICC provides a higher level of security for Ks_ext_NAF usage and extends the key life time of Ks_ext.

So, we kindly recommend SA3 to require the storage of Ks_ext on the UICC for GBA_U.
A CR [3] implements this proposal.

5. References

[1] TS 33.220, v6.1.0

[2] TD S3-040xxx, "GBA_U in Rel 6 Mes", Axalto, Gemplus, SA3#34

[3] TD S3-040xxx, "CR to TS 33.220, GBA: GBA_U derivations: ", Axalto, Gemplus, SA3#34