3GPP TSG SA WG3 Security — SA3#34 **S3-040655**
6-9 July, 2004
Acapulco, Mexico

Source:	Session Chairman
Title:	GBA_U Evening session report (Thursday, July 8th)
Agenda item:	7.9.2
Document for:	Information

Summary of discussions

The GBA_U related contributions were discussed in an evening session, and below are the results of these discussions:

1. *Mechanism to trigger the bootstrapping run*: In offline discussions before the evening session, Siemens, Axalto, and Gemplus had agreed on the way forward with using the MAC indication method with some additional changes, and not to pursue the special RAND approach. There were no objections against the proposal in general. Nokia reserved the right to further comment on the proposal during the SA3 plenary. *S3-040654 contains an updated CR that is based on S3-040476.*

2. *ME capabilities and GBA_U support*: Discussions on whether it should be mandated that Release-6 MEs should support GBA_U, were not conclusive. Axalto and Gemplus were driving that the support for GBA_U in Release-6 MEs should be mandatory. The main arguments were that having the ME supporting GBA_U is a minor issue because the ME-UICC interface does not need to be extended much. Also, the potential new applications on the UE that could use GBA_U was used as an argument. Nokia, Siemens, and Ericsson stated that GBA_U should not be made mandatory, especially as "low-end" terminals in Release-6 would probably not use GBA_U. Nokia and Siemens also wanted to know what are the potential applications that would use GBA_U and how it would work in general with UICC applications. The CRs weren't looked at as companies could not reach an agreement. *There was no consensus on this matter and a way forward needs to be decided by the SA3 plenary.*

3. *Detailed UICC-ME interface for GBA_U*: Axalto presented the ME-UICC interface for GBA_U in S3-040499. It was commented that parts of the interface details depend on whether the Ks_ext is given to the ME or not, and whether MEs are mandated to support GBA_U. *In order to further progress the work, it was agreed that Axalto will provide a CR to the SA3 plenary that is based on S3-040499 and add an editor's note stating that the storage of the Ks_ext is open.*

4. *Storage of Ks_ext*: Axalto and Gemplus were driving that the Ks_ext should be stored on the UICC. They stated that reasons for doing this was that this approach provides higher level of security. 3 expressed slight preference for storing the Ks_ext on the UICC. Nokia, Ericsson, and Siemens were questioning the necessity to store the key to the UICC. It was noted that for requiring the Ks_ext to be stored on the UICC complicates the implementation of the ME, as it must support for both GBA_U aware and unaware UICCs, i.e., the NAF specific key may be derived in the UICC or in the ME. It was also noted that this issue depends on the issue 2: if GBA_U unaware MEs are allowed then Ks_ext must be given to the ME. The CRs weren't looked at as companies could not reach an agreement. *There was no consensus on this matter and a way forward needs to be decided by the SA3 plenary. Note that the way forward also depends on the decision that is made on regarding ME capabilities and GBA_U support (bullet 2).*

5. *Key derivation*: *Key derivation contributions were not discussed as this also depends on the bullets 2 and 4 above.*

6. *Others*: S3-040540 was introduced by Nokia. It was commented that it was unclear if such generic encrypt/decrypt functions are really necessary. *It was agreed to recommend to the SA3 plenary to reject the CR.*

   S3-040564 was introduced by Gemplus. It was agreed to recommend to the SA3 plenary that the CR is approved with clarifying example that specific NAF mandate the use of usage of the specific key, or it can be negotiated by the NAF and the UE. Also, additional CR to TS 33.222 should be generated stating that the in GBA_U context, the Ks_ext_NAF shall be used by default. *An update of the 564 and a new CR to TS 33.222 will be provided by Gemplus to the SA3 plenary.*

Annex A: GBA_U discussions list

A) Mechanism to trigger the bootstrapping run

Discussion Papers:

TD S3-040475 Alternative to Special Random or AMF indication for GBA_U: MAC indication; Axalto

TD S3-040580 Comments to S3-040475 (Alternative to Special Random or AMF indication for GBA_U: MAC indication); Siemens

TD S3-040585 Comments to S3-040580; Axalto

CR'sv:

TD S3-040490 CR: Introducing the Special-RAND mechanism for GBA_U; Siemens

TD S3-040476 CR: Introduction of GBA_U AUTN generation in the BSF; Axalto

B) ME capabilities and GBA_U support

Discussion Papers:

TD S3-040477 GBA_U Scenarios and Rel 6 MEs capabilities; Axalto, Gemplus, OCS

TD S3-040491 GBA: The support of GBA features within a Rel-6 ME; Siemens

TD S3-040576 GBA: The support of GBA features within a Rel-6 ME; Axalto comments to S3-040491

CR's:

TD S3-040478 CR: Requirement on ME capabilities for GBA_U; Axalto, Gemplus, OCS

TD S3-040488 CR: Unaware GBA_U MEs, which are GBA_ME aware only shall be allowed; Siemens

C) Detailed UICC-ME interface for GBA_U

TD S3-040499 UICC-ME interface for GBA-U; Axalto, Gemplus

D) Storage of Ks_ext

TD S3-040515 Clarification of Ks_ext; Huawei (Discussion paper including CR)

TD S3-040498 GBA: GBA_U derivations; Gemplus, Axalto, Oberthur (Discussion Paper)

TD S3-040533 CR: GBA_U: storage of Ks_ext in the UICC; Axalto, Gemplus, Oberthur

TD S3-040537 CR: GBA_U: Ks_ext not stored on UICC; Nokia, Siemens

E) Key derivation

TD S3-040536 CR: GBA_U: key derivation procedure modified; Nokia, Siemens (CR+ppt-slides).

TD S3-040575 GBA_ME/GBA_U scenarios in UE att S3-040536 COMMENTED/REVISED BY AXALTO; Axalto comments to S3-040536

F) Others

TD S3-040540 CR: GBA_U: generic functions for Ks_int_NAF usage; Nokia

TD S3-040564 Removal of the definition of a default type of NAF-specific key; Gemplus