3GPP TSG SA WG3 Security — SA3#35 **S3-040710**
October 5-8, 2004
St Paul's Bay, Malta

3GPP TSG T WG3 Meeting #32 ***T3-040562***
New York, USA, 10th - 13th August 2004

Title: LS on USAT initiated GBA_U Bootstrap
Release: Release 6
Work Item: SEC1-SC
Attachment: T3-040486

Source: **T3**
To: SA3

Contact Person:
Name: Christophe Dubois
Tel. Number: +34 91 7829311
E-mail Address: cdubois@axalto.com

Attachment: T3-040486

1. Overall Description:

T3 has discussed the attached contribution that proposes a procedure to enable UICC applications to initiate a GBA_U Bootstrapping procedure.

The following security use cases have been identified justifying this new procedure:

-A UICC application may wish to establish a security association with a Network Application Function in a moment where there are no available GBA bootstrapped keys or whenever the bootstrapped keys are no more valid. In that case the UICC application may need to ask the ME to perform a bootstrapping procedure.

-A Network operator may wish to initiate bootstrapping procedures (e.g. for renewing GBA Bootstrapped keys) using the available push and triggering mechanisms to the UICC. In that case the UICC application may, as requested by the Network Operator, initiate the bootstrapping procedure.

Related to the first of the use cases, it has been also acknowledged that in most cases the existing solution (ME initiated) may be enough to have GBA keys available for usage by any UICC application. This is acceptable as far as Bootstrapping procedure is linked to an initialisation procedure or performed frequently enough to limit the moments where valid bootstrapped keys are not available. However, T3 is not aware of any of those assumptions and then the attached contribution may be then required.

Some additional comments mentioned that it could also be possible to initiate the bootstrapping procedures using the available data channels between the UICC and the network (e.g. BIP/GPRS). However it was also pointed out that the requested protocols needed on Ub reference point (i.e. HTTP Digest AKA) might be out of the computing capabilities of some Rel-6 UICCs.

2. Actions:

To SA3. T3 would like SA3 to comment on the security requirements and considerations about this T3 proposal and come back to T3 in order to further progress on this issue.

3. Date of Next TSG-T3 Meetings:

3GPP TSG-T3#32
Ney York, USA, 10-13 August 2004

Tdoc ⌘ T3-040486

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.111** **CR** ⌘ **rev** **-** ⌘ Current version: **6.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	UICC initiated GBAU Bootstrapp
Source:	⌘	Axalto
Work item code:	⌘	SEC1-SC
Date:	⌘	28/07/2004
Category:	⌘	**B**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	GBA with UICC-based enhancements (GBA_U) may be used to establish security associations between any UE application and a Network Application Function (NAF). In the case of a USAT application, a mechanism for initiating a bootstrapping procedure is needed in case that bootstrapped keys are not available.
Summary of change:	⌘	The following changes are included: - Inclusion of specific requirements to perform GBA bootstrapp procedure initiatiate by a REFRESH command on EF_{GBABP}
Consequences if not approved:	⌘	USAT applications will not be able to use GBA_U when a bootstrapp procedure has not been performed by the ME.

Clauses affected:	⌘	6.4.7.2 (new)
Other specs affected:	⌘	Y / N [ ] / [X] Other core specifications [ ] / [ ] Test specifications [ ] / [ ] O&M Specifications
Other comments:	⌘	

6 Proactive UICC

6.4.7 REFRESH

See TS 102 223 [32].

6.4.7.1 EF_{IMSI} changing procedure

When an EF_{IMSI} is changed via Data Download or a USAT application and a REFRESH command is issued by the UICC the following rules apply to the UICC and ME:

- USIM Initialization. This command shall not be used if an EF_{IMSI} is changed, as the behaviour of the UE is unpredictable;
- File Change Notification. This command shall not be used if an EF_{IMSI} is changed, as the behaviour of the UE is unpredictable;
- USIM Initialization and File Change Notification. This command shall not be used if an EF_{IMSI} is changed, as the behaviour of the UE is unpredictable;
- USIM Initialization and Full File Change Notification. This command shall not be used if an EF_{IMSI} is changed, as the behaviour of the UE is unpredictable;
- UICC Reset. Normal UICC Reset procedure is carried out;
- USIM Application Reset. Normal USIM Application Reset procedure is carried out;
- 3G Session Reset. Normal 3G Session Reset procedure is carried out.

If an EF_{IMSI} is to be updated, neither EF_{IMSI} nor EF_{LOCI} shall be updated in the UICC before the 3G session termination procedure has been completed by the ME.

6.4.7.2 Generic Bootstrapping Procedure Request

When the UICC issues a REFRESH command implying a File Change Notification on EF_{GBABP} under ADF USIM (GBA Bootstrapping parameters) the ME shall perform a GBA bootstrapping procedure (as defined in [14]).

This procedure applies to REFRESH command only in the following modes: USIM File Change Notification; USIM Initialization and File Change Notification; and USIM Session Reset.