3GPP TSG SA WG3 Security — S3#34 **S3-040664**
July 6 - 9, 2004
Acapulco, Mexico

Title: LS on Required UICC-ME interface enhancements for GBA_U support.
Release: Rel-6
Work Item: SSC-GBA

Source: SA3
To: T3
Cc:

Contact Person:
Name: **Adrian Escott**
Tel. Number: +44 7782 325254
E-mail Address: adrian.escott@three.co.uk

Attachments: S3-040653

---

1. Overall Description:

SA3 are currently finalising Generic Bootstrapping Architecture (GBA) TS 32.220. In this context, SA3 have discussed the required ME-UICC interface to support the GBA_U specific enhancements of GBA.

So far, two specific GBA_U calls to the corresponding UICC application have been identified. The first one, performs an adapted AKA run in the UICC to produce GBA_U bootstrapping key material (GBA_U Bootstrapping procedure). The second one is used to derive application specific key material from the GBA_U bootstrapped keys (GBA_U NAF Derivation procedure).

SA3 have not yet decided on whether a part or all the key material derived in the first GBA_U call is to be kept inside the UICC application or it should be delivered to the ME. So, it is not yet decided if the second GBA_U call will be applicable only to internal UICC key material or to both, ME and UICC, bootstrapped keys.

The attached proposed CRs implement the two mentioned GBA_U calls in the UICC-ME interface. Three proposals are included:

a) The keys of the first GBA_U call are kept in the UICC (alternative 1)
b) The keys are partially kept in the UICC and partially in the ME (alternative 2)
c) The keys are kept in the UICC and partially in the ME (alternative 3)

Many of the interface definitions are common to the three proposals and the differences between them are considered quite limited. So, it is SA3's assumption that T3 could start working on the implementation of these procedures in the involved Rel 6 TS using the attached information and the available TS 33.220. However, as stated before, SA3 have not yet agreed on any of the detailed attached proposals and they may evolve as a consequence of following SA3 meetings.

SA3 would like to draw T3's attention to the fact that TS 33.220 Rel 6 will likely not be frozen before the SA3 #35 meeting. Since some stage 2 decisions will probably be taken then, it is SA3's opinion that T3 would likely not be able to complete the required GBA_U functionalities before SA3 work completion. However, it is highly desirable that T3 starts working on this Rel 6 feature and liase with SA3 for commenting on T3 CRs if required.

2. Actions:

To T3 group.

ACTION: Please consider the attached documents in order to help T3's work on producing the required Rel 6 TS changes for GBA_U support.

3. Date of Next TSG SA WG 3 Meetings:

TSG-SA3 Meeting #35	5-8 October 2004	Malta
TSG-SA3 Meeting #36	23-26 November 2004	Shenzhen, China

3GPP TSG SA WG3 Security — S3#34 **S3-040653**
6 - 9 July 2004
Acapulco, Mexico

Source: **Axalto**

Title: **GBA_U ME-UICC interface and Ks_ext storage**

Document for: **Discussion and decision**

Agenda Item: **GBA**

1 Introduction

After some discussions on this issue an agreement was not reached. The following alternatives were evoked/discussed during the GBA_U evening session.

1) Storage of Ks_ext and derivation of Ks_ext_NAF in the UICC.

2) Storage of Ks_ext and derivation of Ks_ext_NAF in the ME.

3) Storage of Ks_ext and derivation of Ks_ext_NAF in both the ME & UICC.

Proposed CRs are attached in this contribution for each of the three alternatives.

Comparing the three alternatives, alternative 1 provides enhanced security, portability and extended key life time. Additionally, it will require the support of GBA_U specific functions in the ME.

Alternative 2 will limit the impact in ME to Ks_ext derivation and B-Tid/Key Life Time storage but will not provide any of the above advantages.

Alternative 3 will provide portability an extended key life time enhancements but none of the security improvements. However, it will slightly reduce the implementation needs in the ME.

2 Proposal

As it could be seen in the attached documents the differences on implementing option 1,2,3 are minimal compared with the effort of supporting GBA_ME in the terminal. It is considered that there are not technical issues avoiding that the recognized security/usage enhancements are not supported in all GBA capable MEs if an operator decides to implement this GBAU enhancements in the UICC and the network.

Considering this, it is proposed that SA3 adopts alternative one approving the corresponding attached CR and the CR in S3-040533

It is also proposed to inform T3 about the details of this interface.

CR-Form-v7

CHANGE REQUEST

⌘ **33.220** **CR** ⌘ **rev** **-** ⌘ Current version: **6.1.0** ⌘

*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-ME interface for GBAU support
Source:	⌘	Axalto, Gemplus
Work item code:	⌘	SSC-GBA
Date:	⌘	23/06/2004
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:

2	*(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)*

Reason for change:	⌘	The current version of TS 33.220 does not include a description of the message needed in the UICC-ME interface
Summary of change:	⌘	The description of the UICC-ME interface is added as normative annex.
Consequences if not approved:	⌘	Description of the solution is not complete.

Clauses affected:	⌘	Annex			
Other specs affected:	⌘	Y: X / N:	Other core specifications	⌘	TS 31.102, TS 31.103
		Y: / N: X	Test specifications		
		Y: / N: X	O&M Specifications		
Other comments:	⌘	-			

BEGIN OF CHANGE

Annex D (normative): GBA_U UICC-ME interface

This section describes the UICC-ME interface to be used when a GBA_U aware UICC application is active and the ME is involved in a GBA bootstrapping procedure. When the UICC application is not GBA_U aware, the ME uses AUTHENTICATE command in non-GBA_U security context (i.e. UMTS security context in case of USIM application and IMS security context in case of the ISIM) as defined in 31.102 [ ] and 31.103 [ ].

D.1. GBA_U Bootstrapping procedure

This procedure is part of the Bootstrapping procedure as described in section 5.3.2

The ME sends RAND and AUTN to the UICC and performs the Ks_ext and Ks_int derivation as described in 5.3.2.

The UICC then stores Ks_ext and Ks_int. The UICC also stores the used RAND to identify the current bootstrapped values. RAND value in the UICC shall be further accessible by the ME.

The ME then, finalizes the Bootstrapping procedure and stores in the UICC the Transaction Identifier (B-Tid) and Key Life Time associated with the previous bootstrapped keys (i.e. Ks_int and Ks_ext). Transaction Identifier and Key Life Time values in the UICC shall be further accessible by the ME.

At the end of the GBA_U bootstrapping procedure the UICC stores Ks_ext, Ks_int, Transaction Identifier, Key Life Time and the RAND.

A new bootstrapping procedure replaces Ks_ext, Ks_int, TId, Key LifeTime and RAND values of the previous bootstrapping procedure.

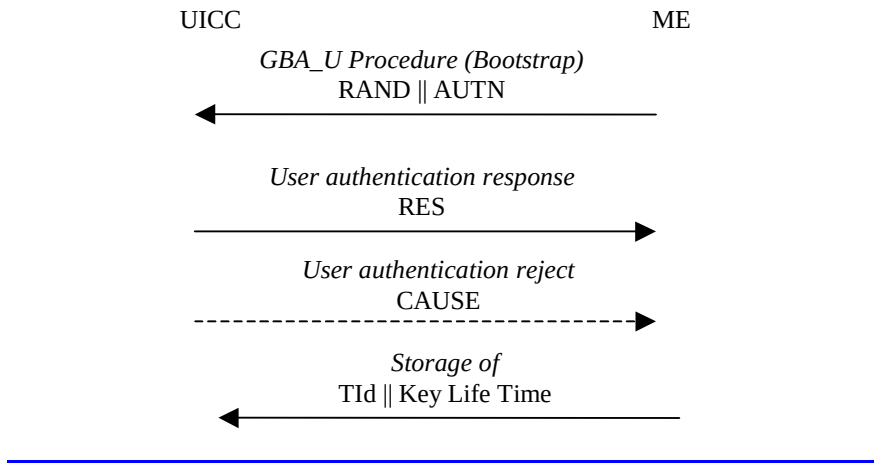

Figure x: GBA_U Bootstrap Procedure

D.2. GBA_U NAF Derivation procedure

This procedure is part of the Procedures using bootstrapped Security Association as described in section 5.3.3

The ME sends NAF_ID and IMPI to the UICC. The UICC then performs Ks_ext_NAF and Ks_int_NAF derivation as described in 5.3.2. The UICC uses the RAND, Ks_ext and Ks_int values stored from the previous bootstrapping procedure. The UICC returns Ks_ext_NAF to the ME and stores Ks_int_NAF together with NAF_Id.

Note: A previous GBA_U Bootstrap needs to be undertaken before. If a Ks_int, Ks_ext pair is not available in the UICC, the command will answer with the appropriate error message.

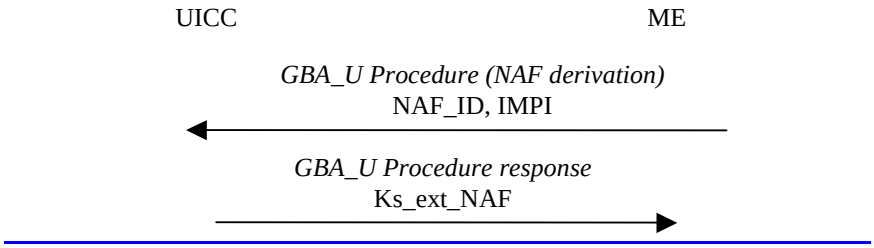

Figure x: GBA_U NAF derivation procedure

CR-Form-v7

CHANGE REQUEST

⌘ **33.220** **CR** ⌘ **rev** **-** ⌘ Current version: **6.1.0** ⌘

*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-ME interface for GBAU support
Source:	⌘	Axalto, Gemplus
Work item code:	⌘	SSC-GBA
Date:	⌘	23/06/2004
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:

2	*(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)*

Reason for change:	⌘	The current version of TS 33.220 does not include a description of the message needed in the UICC-ME interface
Summary of change:	⌘	The description of the UICC-ME interface is added as normative annex.
Consequences if not approved:	⌘	Description of the solution is not complete.

Clauses affected:	⌘	Annex			
Other specs affected:	⌘	**Y**	**N**		
		X		Other core specifications	⌘ TS 31.102, TS 31.103
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘	-			

BEGIN OF CHANGE

Annex D (normative): GBA_U UICC-ME interface

This section describes the UICC-ME interface to be used when a GBA_U aware UICC application is active and the ME is involved in a GBA bootstrapping procedure. When the UICC application is not GBA_U aware, the ME uses AUTHENTICATE command in non-GBA_U security context (i.e. UMTS security context in case of USIM application and IMS security context in case of the ISIM) as defined in 31.102 [ ] and 31.103 [ ].

D.1. GBA_U Bootstrapping procedure

This procedure is part of the Bootstrapping procedure as described in section 5.3.2

The ME sends RAND and AUTN to the UICC and performs the Ks_ext and Ks_int derivation as described in 5.3.2.

The UICC then stores Ks_int. The UICC also stores the used RAND to identify the current bootstrapped values. RAND value in the UICC shall be further accessible by the ME.

The ME then, finalizes the Bootstrapping procedure and stores in the UICC the Transaction Identifier (B-Tid) and Key Life Time associated with the previous bootstrapped keys (i.e. Ks_int and Ks_ext). Transaction Identifier and Key Life Time values in the UICC shall be further accessible by the ME.

At the end of the GBA_U bootstrapping procedure the UICC stores Ks_int, Transaction Identifier, Key Life Time and the RAND.

The UICC sends Ks_ext (in the format of CK'|| IK') and RES to the ME.

A new bootstrapping procedure replaces Ks_int, TId, Key LifeTime and RAND values of the previous bootstrapping procedure.

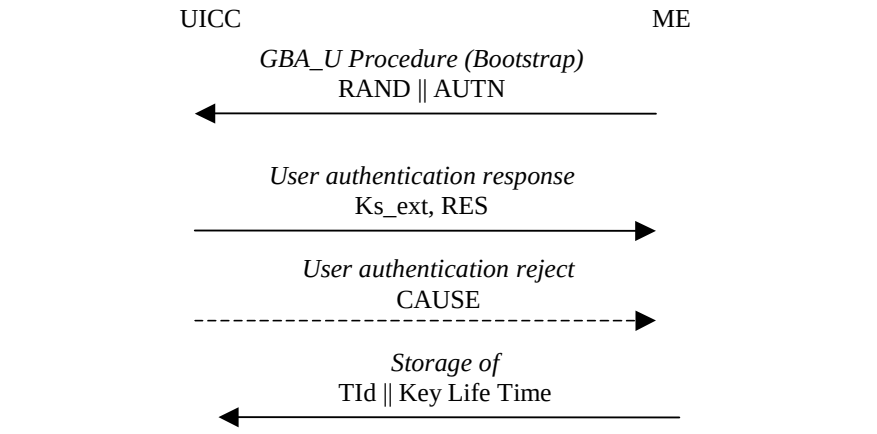

Figure x: GBA_U Bootstrap Procedure

D.2. GBA_U NAF Derivation procedure

This procedure is part of the Procedures using bootstrapped Security Association as described in section 5.3.3

The ME sends NAF_ID and IMPI to the UICC. The UICC then performs Ks_int_NAF derivation as described in 5.3.2. The UICC uses the RAND and Ks_int values stored from the previous bootstrapping procedure. The UICC stores Ks_int_NAF together with NAF_Id.

Note: A previous GBA_U Bootstrap needs to be undertaken before. If Ks_int is not available in the UICC, the command will answer with the appropriate error message.

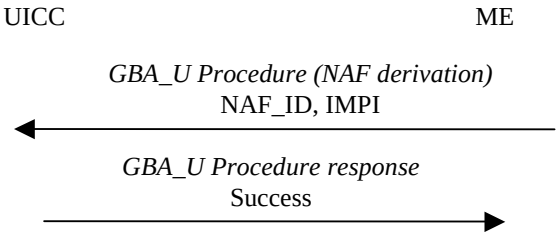

Figure x: GBA_U NAF derivation procedure

CR-Form-v7

CHANGE REQUEST

⌘ **33.220** **CR** ⌘ **rev** **-** ⌘ Current version: **6.1.0** ⌘

*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-ME interface for GBAU support
Source:	⌘	Axalto, Gemplus
Work item code:	⌘	SSC-GBA
Date:	⌘	23/06/2004
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:

2	*(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)*

Reason for change:	⌘	The current version of TS 33.220 does not include a description of the message needed in the UICC-ME interface
Summary of change:	⌘	The description of the UICC-ME interface is added as normative annex.
Consequences if not approved:	⌘	Description of the solution is not complete.

Clauses affected:	⌘	Annex

		Y	N		
Other specs affected:	⌘	X		Other core specifications	⌘ TS 31.102, TS 31.103
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘	-

BEGIN OF CHANGE

Annex D (normative): GBA_U UICC-ME interface

This section describes the UICC-ME interface to be used when a GBA_U aware UICC application is active and the ME is involved in a GBA bootstrapping procedure. When the UICC application is not GBA_U aware, the ME uses AUTHENTICATE command in non-GBA_U security context (i.e. UMTS security context in case of USIM application and IMS security context in case of the ISIM) as defined in 31.102 [ ] and 31.103 [ ].

D.1. GBA_U Bootstrapping procedure

This procedure is part of the Bootstrapping procedure as described in section 5.3.2

The ME sends RAND and AUTN to the UICC and performs the Ks_ext and Ks_int derivation as described in 5.3.2.

The UICC then stores Ks_ext and Ks_int. The UICC also stores the used RAND to identify the current bootstrapped values. RAND value in the UICC shall be further accessible by the ME.

The ME then, finalizes the Bootstrapping procedure and stores in the UICC the Transaction Identifier (B-Tid) and Key Life Time associated with the previous bootstrapped keys (i.e. Ks_int and Ks_ext). Transaction Identifier and Key Life Time values in the UICC shall be further accessible by the ME.

At the end of the GBA_U bootstrapping procedure the UICC stores Ks_ext, Ks_int, Transaction Identifier, Key Life Time and the RAND.

The UICC sends Ks_ext (in the format of CK'|| IK') and RES to the ME.

A new bootstrapping procedure replaces Ks_ext, Ks_int, TId, Key LifeTime and RAND values of the previous bootstrapping procedure.

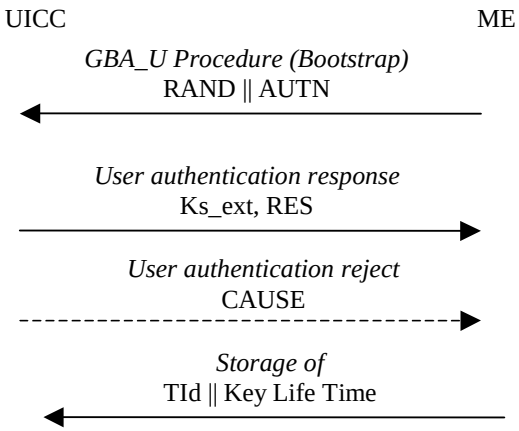

Figure x: GBA_U Bootstrap Procedure

D.2. GBA_U NAF Derivation procedure

This procedure is part of the Procedures using bootstrapped Security Association as described in section 5.3.3

The ME sends NAF_ID and IMPI to the UICC. The UICC then performs Ks_ext_NAF and Ks_int_NAF derivation as described in 5.3.2. The UICC uses the RAND, Ks_ext and Ks_int values stored from the previous bootstrapping procedure. The UICC returns Ks_ext_NAF to the ME and stores Ks_int_NAF together with NAF_Id.

Note: A previous GBA_U Bootstrap needs to be undertaken before. If a Ks_int, Ks_ext pair is not available in the UICC, the command will answer with the appropriate error message.

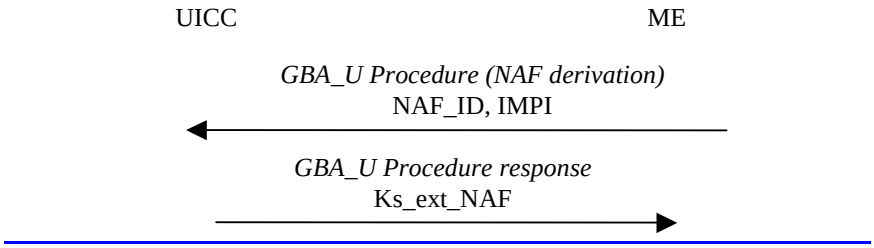

Figure x: GBA_U NAF derivation procedure