3GPP TSG SA WG3 Security — S3#34 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 <u>Introduction</u>

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.

6 - 9 July 2004, Acapulco, Mexico									
CHANGE REQUEST									
	33.220 CR	жre	- # C	urrent versio	6.1.0				
For <u>HELP</u> on using this form, see bottom of this page or look at the pop-up text over the ** symbols.									
Proposed change	affects: UICC ap	pps <mark>⊯ X</mark> ME	X Radio Acc	ess Network	Core Net	work			
Title: #	LUCC ME interfac	ce for GBAU support	•						
Title.	OICC-ME Internac	e for GBAO support	L						
Source:	Axalto, Gemplus								
Work item code: ₩	SSC-GBA			Date: 🕱	23/06/2004				
Category:	В		F	Release: 🕱	Rel-6				
	B (addition of a C (functional n D (editorial mo	is to a correction in an feature), nodification of feature) odification) as of the above catego		2 (0 R96 (F R97 (F R98 (F R99 (F Rel-4 (F Rel-5 (F	e following relea GSM Phase 2) Release 1996) Release 1997) Release 1998) Release 1999) Release 4) Release 5)	ases:			
					·				
Reason for change		rersion of TS 33.220 UICC-ME interface		de a descript	ion of the mes	ssage			
	needed in the	OICC-ME INTERNACE	•						
Summary of chang	ge: <mark>黑 The descripti</mark>	on of the UICC-ME	interface is add	led as norma	tive annex.				
Consequences if not approved:	Example 2 Description of	f the solution is not	complete.						
Clauses affected:	器 Annex								
Other specs affected:	X Test s	core specifications pecifications Specifications	器 TS 31.	.102, TS 31.1	03				
Other comments:	光 -								

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.

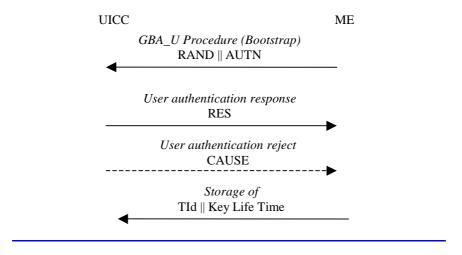


Figure x: GBA U Bootstrap Procedure

D.2. GBA UNAF 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.

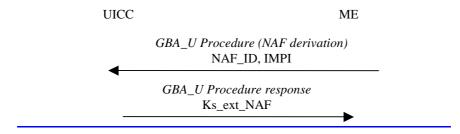


Figure x: GBA_U NAF derivation procedure

6 - 9 July 2004	, Aca	pulco, I	Mexico							
CHANGE REQUEST								CR-Form-vī		
[H]	33	<mark>.220</mark> (CR	≋re	v -	. #	Current v	ersion:	6.1.0	(X)
For <u>HELP</u> on	n using	this form,	see bottom	of this page	or loo	k at th	e pop-up te	ext ove	r the 🛣 sy	mbols.
Proposed chang	e affec	ets: UIC	CC apps <mark>ж</mark> 🗴	ME	X R	adio A	ccess Netv	vork	Core N	etwork
Title:	₩ UIC	CC-ME int	terface for G	BAU suppor	t					
Source:	Ж Ах	alto, Gem	nplus							
Work item code:	₩ SS	C-GBA					Date:	第 23	3/06/2004	
									.,	
Category:	Deta	F (correct A (correct B (addition C (function D (editor ailed expla	e following cate tion) sponds to a coon of feature), onal modification attions of the TR 21.900	rrection in an on of feature n) above catego)		2	of the f (GS (Rei (Rei (Rei (Rei (Rei	el-6 following rei M Phase 2, lease 1996, lease 1997, lease 1998, lease 1999, lease 4) lease 5))))
Reason for chan	ge: <mark></mark> Ж	The currenced	ent version on the UICC-	of TS 33.220 ME interface) does	not in	clude a des	scription	n of the m	essage
Summary of cha	nge: <mark></mark> %	The des	cription of the	e UICC-ME	interfa	ce is a	added as no	ormativ	e annex.	
Consequences in not approved:	f X	Descript	ion of the so	lution is not	compl	ete.				
Clauses affected	l: <mark></mark> #	Ann	ex							
Other specs affected:	æ	X	Other core sp est specifica O&M Specific	tions	æ	TS	31.102, TS	31.103	3	

BEGIN OF CHANGE

Other comments:

光 -

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, Tld, Key LifeTime and RAND values of the previous bootstrapping procedure.

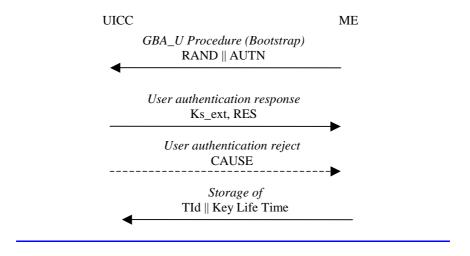


Figure x: GBA_U Bootstrap Procedure

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.

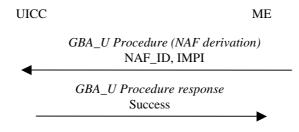


Figure x: GBA_U NAF derivation procedure

6 - 9 July 2004,	Acapulco	, Mexico							
CHANGE REQUEST									
(X)	33.220	CR	жrev	- #	Current versi	on: 6.1.0	 #		
For <u>HELP</u> on u	ısing this for	m, see bottom	of this page or	look at the	e pop-up text	over the <mark>器</mark> sy	mbols.		
Proposed change	affects:	JICC apps <mark>Ж</mark> Х	ME X	Radio A	ccess Networ	k Core N	etwork		
Title: ₩	UICC-ME	interface for G	BAU support						
Source: #	Axalto, G	emplus							
Work item code: <mark></mark> 器	SSC-GBA	4			Date: ₩	23/06/2004			
Reason for change Summary of change Consequences if	Use one of F (con A (cor B (add C (fun D (edi Detailed exp be found in E: # The coneede	ed in the UICC-	orrection in an earlion of feature) n) above categorie 0. of TS 33.220 de ME interface	s can pes not ince	2 e) R96 R97 R98 R99 Rel-4 Rel-5 Rel-6				
not approved:	. Desci	iption of the so	iution is not co	mpiete.					
Clauses affected:	₩ A	nnex							
Other specs affected:	安 X X X	Other core sp Test specifica O&M Specific	itions	æ TS 3	31.102, TS 31	.103			
Other comments:	28 -								

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.

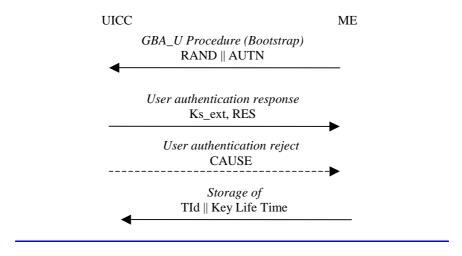


Figure x: GBA_U Bootstrap Procedure

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.

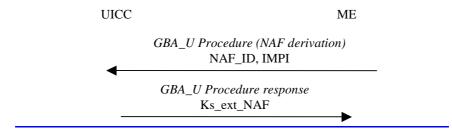


Figure x: GBA_U NAF derivation procedure