3GPP TSG-T (Terminals) Meeting #27
Tokyo, Japan, 9-11 March 2005

TP-050019

Agenda Item: 6.3.3

Source: T3

Title: CRs to TS 31.103

Document for: Approval

This document contains the following change requests that are approved by 3GPP TSG T3 and forwarded to 3GPP TSG T#27 for approval:

Doc-2nd-Level	Spec	CR	Rev	Rel	Subject	Cat	Ver-old	Ver-new	WI
T3-050126	31.103	022		Rel-6	Reservation of file IDs under ADF ISIM	A	6.6.0	6.7.0	TEI5
T3-050163	31.103	023		Rel-5	Reservation of file IDs under ADF ISIM	F	5.8.0	5.9.0	TEI5
T3-050182	31.103	024		Rel-6	Completion of GBA_U-related procedures	F	6.6.0	6.7.0	TEI6
T3-050185	31.103	025		Rel-6	Storage of NAF-keys identifiers in GBA_U	F	6.6.0	6.7.0	TEI6

3GPP TSG-T3 Meeting #34
Barcelona, Spain, 8th – 11th February 2005

Tdoc T3-050126⌘

CR-Form-v7

CHANGE REQUEST

⌘ **31.103** **CR** **022** ⌘**rev** **-** ⌘ Current version: **6.6.0** ⌘

*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 [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Reservation of File IDs under ADFisim
Source:	⌘	T3
Work item code:	⌘	TEI6
Date:	⌘	10/02/2005
Category:	⌘	**A**
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:	⌘	File IDs '6F1X', '5F1X' and '5F2X' under ADFisim have voluntarily been left unused. However, they are not stated as 'reserved' anywhere in the specifications. Action item asked by T3 plenary: AP#1/30, following the approval of an equivalent CR for TS 31.102 in T3-040160 (CR #221).
Summary of change:	⌘	Mention that File IDs '6F1X', '5F1X' and '5F2X' under ADFisim are reserved for administrative use
Consequences if not approved:	⌘	Risk of clash of file-IDs (causing interoperability problems with MEs) if some card issuer choose values that would be used in further versions of the specification.

Clauses affected:	⌘	4.2

Other specs affected: ⌘	Y	N		⌘
		X	Other core specifications	
		X	Test specifications	
		X	O&M Specifications	

Other comments:	⌘	Equivalent Rel-6 CR to the Rel-5 CR in document T3-0500163 (CR #23)

4.2 Contents of files at the ISIM ADF (Application DF) level

The EFs in the ISIM ADF contain service and network related information and are required for UE to operate in an IP Multimedia Subsystem.

The File IDs '6F1X' (for EFs), '5F1X' and '5F2X' (for DFs) with X ranging from '0' to 'F' are reserved under the ISIM ADF for administrative use by the card issuer.

3GPP TSG-T3 Meeting #34
Barcelona, Spain, 8th – 11th February 2005

Tdoc T3-050163⌘

CR-Form-v7

CHANGE REQUEST

⌘ **31.103** **CR** **023** ⌘**rev** **-** ⌘ Current version: **5.8.0** ⌘

*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 [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Reservation of File IDs under ADFisim
Source:	⌘	T3
Work item code:	⌘	TEI5
Date:	⌘	10/02/2005
Category:	⌘	**F**
Release:	⌘	Rel-5

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:	⌘	File IDs '6F1X', '5F1X' and '5F2X' under ADFisim have voluntarily been left unused. However, they are not stated as 'reserved' anywhere in the specifications. Action item asked by T3 plenary: AP#1/30, following the approval of an equivalent CR for TS 31.102 in T3-040160 (CR #221).
Summary of change:	⌘	Mention that File IDs '6F1X', '5F1X' and '5F2X' under ADFisim are reserved for administrative use
Consequences if not approved:	⌘	Risk of clash of file-IDs (causing interoperability problems with MEs) if some card issuer choose values that would be used in further versions of the specification.

Clauses affected:	⌘	4.2

Other specs affected: ⌘	Y	N		⌘
		X	Other core specifications	
		X	Test specifications	
		X	O&M Specifications	

Other comments:	⌘	An equivalent CR for Rel-6 is needed.

4.2 Contents of files at the ISIM ADF (Application DF) level

The EFs in the ISIM ADF contain service and network related information and are required for UE to operate in an IP Multimedia Subsystem.

The File IDs '6F1X' (for EFs), '5F1X' and '5F2X' (for DFs) with X ranging from '0' to 'F' are reserved under the ISIM ADF for administrative use by the card issuer.

3GPP TSG-T3 #34
Barcelona, Spain, 8-11 February 2005

Tdoc ⌘T3-050182

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.103** **CR** 024 ⌘**rev** **-** ⌘ Current version: **6.6.0** ⌘

*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:	⌘	Completion of GBA_U-related procedures
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	09/02/05
Category:	⌘	**F**
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: ⌘ The GBA_U related procedures in TS 31.103, are not in line with those described in TS 33.220. The following points should be clarified in TS 31.103:

- It is stated in the annex G of TS 33.220 that after a successful bootstrap operation, the ME stores in the UICC the Transaction Identifier (B-TID) and the Key Life Time associated with the previous bootstrapped keys. While in section 5.2.8 of TS 31.103 it is only stated that the B-TID shall be updated in EF_{GBABP}
- TS 33.220 clarifies that in the UE there is at most one Ks_int_NAF/Ks_ext_NAF key pair stored per NAF_Id. This clarification should exist in the GBA_U-related procedures in TS 31.103.
- TS 33.220 indicates that if NAF key, derived from one NAF_ID, is updated, the other NAF keys, derived from different NAF_ID values, stored on the UE shall not be affected.
- Finally, in some cases, the NAF_ID is not enough to identify the Ks_int_NAF/Ks_est_NAF unambiguously. For example, a new NAF key generation, from which the http session was not able to complete towards the corresponding NAF, results in different Ks_ext_NAF/Ks_int_NAF key pairs (one in the UE and another in the NAF) identified with the same NAF_ID. Therefore, text should also be added in TS 31.103 to indicate that the ISIM shall store B-TID together with Ks_int_NAF and NAF_ID in order to identify unambiguously the Ks_int_NAF key.

Summary of change:	⌘	Complete the description of GBA_U procedures
Consequences if not approved:	⌘	Incomplete description of GBA_U procedures in TS 31.103 that could result in the misinterpretation of the original requirements and procedures, which are described in TS 33.220.

Clauses affected:	⌘	5.2.8, 7.1.1.3			
Other specs affected:	⌘	**Y** / **N**	Other core specifications	⌘	
			X	Test specifications	
			X	O&M Specifications	
			X		
Other comments:	⌘				

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

5.2.8 Generic Bootstrapping architecture (Bootstrap)

The Terminal uses the AUTHENTICATE command in GBA security context (Bootstrapping Mode) (see 7.1.1). The response is sent to the Terminal.

After a successful GBA_U Procedure, the Terminal shall update the B-TID field and the Key Life Time field in EF_{GBABP}.

7.1.1.2 GBA security context (Bootstrapping Mode)

ISIM operations in GBA security context are supported if service n°2 is "available".

The ISIM receives the RAND and AUTN. The ISIM first computes the anonymity key AK = $f5_K$ (RAND) and retrieves the sequence number SQN = (SQN ⊕ AK) ⊕ AK.

The ISIM calculates IK = $f4_K$ (RAND) and MAC (by performing the MAC modification function described in TS 33.220 [25]). Then the ISIM computes XMAC = $f1_K$ (SQN || RAND || AMF) and compares this with the MAC previously produced. If they are different, the ISIM abandons the function.

Then the ISIM proceeds as in IMS security context by checking AUTN. If the ISIM detects the sequence numbers to be invalid, this is considered as a synchronisation failure and the ISIM abandons the function. In this case the command response is AUTS, ~~wich~~which is computed as in ISIM security context.

If the sequence number is considered in the correct range, the ISIM computes RES = $f2_K$ (RAND) and the cipher key CK = $f3_K$ (RAND).

The ISIM then derives and stores GBA_U ~~botstrapped~~bootstrapped key material from CK, IK values. The ISIM also stores RAND in the RAND field of EF_{GBABP}

~~Note:~~ The ISIM stores GBA_U ~~botstrapped~~bootstrapped key material from only one bootstrapping procedure. The previous bootstrapped key material, if present, shall be replaced by the new one. This key material is linked with the data contained in EF_{GBABP} : RAND, which is updated by the ISIM and B-TID, which shall be further updated by the ME.

Note: According to TS 33.220 [25], NAF-specific keys that may be stored on the ISIM are not affected by this bootstrapping operation.

RES is included in the command response after flipping the least significant bit.

Input:

- RAND, AUTN

Output:

- RES

or

- AUTS

7.1.1.3 GBA security context (NAF Derivation Mode)

ISIM operations in GBA security context are supported if service n°2 is "available".

The ISIM receives the NAF_ID.

The ISIM performs Ks_ext_NAF and Ks_int_NAF derivation as defined in TS 33.220 [25] using the key material from the previous GBA_U bootstrapping procedure and the IMPI value from EF_{IMPI}

If no key material is available this is considered as a GBA Bootstrapping failure and the ISIM abandons the function. The status word ‘6985’ (Conditions of use not satisfied) is returned.

Otherwise, the ISIM stores Ks_int_NAF and associated B-TID together with NAF_ID in its memory. The Ks_int_NAF keys related to other NAF_IDs, which are already stored in the ISIM, shall not be affected.

Note: According to TS 33.220 [25], ~~T~~the ISIM can contain several Ks_int_NAF together with the associated B-TID and NAF_ID, but there is at most one pair of Ks_int_NAF and associated B-TID stored per NAF_ID.

Then, the ISIM returns Ks_ext_NAF.

Input:

- NAF_ID

Output:

- Ks_ext_NAF

3GPP TSG-T3 #34
Barcelona, Spain, 8-11 February 2005

Tdoc ⌘T3-050185

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.103** **CR** 025 ⌘**rev** **-** ⌘ Current version: **6.6.0** ⌘

*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:	⌘	Storage of NAF-keys identifiers in GBA_U
Source:	⌘	Axalto, Gemplus
Work item code:	⌘	TEI
Date:	⌘	09/02/05
Category:	⌘	**F**
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:	⌘	The ISIM can contain several Ks_int_NAF keys together with associated B-TID and NAF-ID. At the moment the ME cannot detect in the UICC the existence of a Ks_int_NAF key already shared between the UICC and a NAF after a GBA NAF Derivation procedure. This issue is solved by the creation of an EF (EF_{GBANL}) containing the list of NAF_IDs and B-TIDs, which are associated to the last GBA NAF derivation procedure successfully executed for a given NAF. The existence of this EF is very useful for some GBA-based service. E.g. in MBMS the ME needs to detect for a given NAF the presence in the ISIM of the key derived from the last successful GBA NAF Derivation procedure.
Summary of change:	⌘	Creation of an EF listing the NAF_IDs and B-TIDs, which are associated to the last GBA NAF derivation procedure successfully executed for a given NAF.
Consequences if not approved:	⌘	For some GBA-based services the ME can lack of information on the previous GBA NAF Derivation procedure successfully executed on the UICC for a given NAF.

Clauses affected:	⌘	4.2.x (new), 4.3, 7.1.1.3, Annex A, Annex C

Other specs affected:	⌘	Y	N		⌘
			X	Other core specifications	
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘	This CR is related to S3-041126, which was approved by SP#26 in SP-040859

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

4.2.x EF_{GBANL} (GBA NAF List)

If service n°68 is "available", this file shall be present.

This EF contains the list of NAF_ID and B-TID associated to a GBA NAF derivation procedure.

Identifier: '6Fxx'	Structure: Linear fixed	Optional
Record length: Z bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to Z	NAF Key Identifier TLV objects	M	Z bytes

- NAF Key Identifier tags

Description	Tag Value
NAF_ID Tag	'80'
B-TID Tag	'81'

NAF Key Identifier information

Description	Value	M/O	Length (bytes)
NAF_ID Tag	'80'	M	1
Length	X	M	Note
NAF_ID value	--	M	X
B-TID Tag	'81'	M	1
Length	Y	M	Note
B-TID value	--	M	Y
Note: The length is coded according to ISO/IEC 8825 [20]			

- NAF_ID Tag '80'

Contents:

Identifier of Network Application Function used in the GBA_U NAF Derivation procedure.

Coding:

As defined in 33.220 [25]

- B-TID Tag '81'

Content:

Bootstrapping Transaction Identifier of the GBA_U bootstrapped key

Coding:

As defined in TS 33.220 [25]

Unused bytes shall be set to 'FF'

4.3 ISIM file structure

This subclause contains a figure depicting the file structure of the ADF_{ISIM}. ADF_{ISIM} shall be selected using the AID and information in EF_{DIR}.

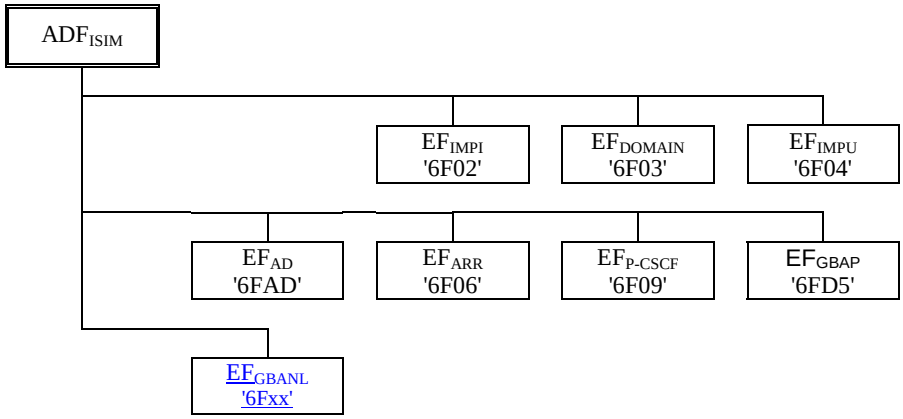

Figure 1: File identifiers and directory structures of ISIM

7.1.1.3 GBA security context (NAF Derivation Mode)

ISIM operations in GBA security context are supported if service n°2 is "available".

The ISIM receives the NAF_ID.

The ISIM performs Ks_ext_NAF and Ks_int_NAF derivation as defined in TS 33.220 [25] using the key material from the previous GBA_U bootstrapping procedure and the IMPI value from EF_{IMPI}

If no key material is available this is considered as a GBA Bootstrapping failure and the ISIM abandons the function. The status word '6985' (Conditions of use not satisfied) is returned.

Otherwise, the ISIM stores Ks_int_NAF together with NAF_ID in its memory~~.~~ and updates EF_{GBANL} as follows:

-If a record with the given NAF_ID already exists, the ISIM updates the B-TID field of this record with the B-TID value associated to the GBA_U bootstrapped key involved in this GBA_U NAF derivation procedure.

-If a record with the given NAF_ID does not exist, the ISIM uses an empty record to store the NAF_ID and the B-TID value associated to the GBA_U bootstrapped key involved in this GBA_U NAF Derivation procedure.

Note: The ISIM can contain several Ks_int_NAF together with NAF_ID

Then, the ISIM returns Ks_ext_NAF.

Input:

- NAF_ID

Output:

- Ks_ext_NAF

Annex A (informative): EF changes via Data Download or CAT applications

This annex defines if changing the content of an EF by the network (e.g. by sending an SMS), or by a CAT Application [22], is advisable. Updating of certain EFs "over the air" could result in unpredictable behavior of the UE; these are marked "Caution" in the table below. Certain EFs are marked "No"; under no circumstances should "over the air" changes of these EFs be considered.

File identification	Description	Change advised
'6F02'	IMS private user identity	Caution (note)
'6F03'	Home Network Domain Name	Caution (note)
'6F04'	IMS public user identity	Caution (note)
'6FAD'	Administrative Data	Caution
'6F06'	Access Rule Reference	Caution
'6F07'	ISIM Service Table	Caution
'6F09'	P-CSCF address	Caution (note)
'6FD5'	GBA Bootstrapping parameters	Caution
'6Fxx'	GBA NAF List	Caution
NOTE: If EF_{IMPI}, EF_{IMPU}, EF_{DOMAIN} or P-CSCF are changed, the UICC should issue a CAT REFRESH command [22].		

Annex C (informative): Suggested contents of the EFs at pre-personalization

If EFs have an unassigned value, it may not be clear from the main text what this value should be. This annex suggests values in these cases.

File Identification	Description	Value
'6F02'	IMS private user identity	'8000FF…FF'
'6F03'	Home Network Domain Name	'8000FF…FF'
'6F04'	IMS public user identity	'8000FF…FF'
'6FAD'	Administrative Data	Operator dependant
'6F06'	Access Rule Reference	Card issuer/operator dependant
'6FD5'	GBA Bootstrapping parameters	'FF…FF'
'6F07'	ISIM Service Table	Operator dependant
'6F09'	P-CSCF address	Operator dependant
'6Fxx'	GBA NAF List	'FF…FF'