3GPP TSG-T (Terminals) Meeting #25
Palm Springs, CA, USA
8 - 10 September 2004

TP-040182

Agenda Item: 5.3.3
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#25 for approval:

Doc-2nd-Level	Spec	CR	Rev	Phase	Subject	Cat	Version-Current	Version-New	Workitem
T3-040546	31.103	017	-	Rel-6	GBAU ME-ISIM interface	B	6.4.0	6.5.0	SEC1-SC
T3-040590	31.103	016	-	Rel-6	New 3GPP2 IMS authentication context in ISIM	B	6.4.0	6.5.0	TEI
T3-040607	31.103	018	-	Rel-5	Correction of PPS procedure	F	5.6.0	5.7.0	TEI

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

Tdoc ⌘ T3-040546

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.103** **CR** 017 ⌘ **rev** **-** ⌘ Current version: **6.4.0** ⌘

*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:	⌘	GBAU ME-ISIM interface
Source:	⌘	T3
Work item code:	⌘	SEC1-SC
Date:	⌘	11/08/2004
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:	⌘	Generic Bootstrapping Architecture in TS 33.220 GBA consists of two mechanisms: ME-based GBA (GBA_ME), which reuses legacy IMS AKA procedure and GBA with UICC-based enhancements (GBA_U) which requires a specific AKA procedure with the ISIM/USIM. GBA_U thus require the definition of some procedures in the ISIM-ME interface.
Summary of change:	⌘	The following changes are included: -New Service in IST for GBA -Storage of parameters associated with a GBA bootstrapping procedure. -New GBA security context in AUTHENTICATE command with two specific modes: Bootstrapping Mode, NAF Derivation
Consequences if not approved:	⌘	Required GBA_U functionalities will not be supported.

Clauses affected:	⌘	2, 4.2.7, 4.2.x (new), 4.3, 5.2.x (new), 5.2.y (new), 7.1, Annex A, Annex E

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

Other comments:	⌘	Note: Further evolutions of 33.220 in GBAU key derivation procedure may

require minor changes to the proposed text.

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.

2 References

The following documents contain provisions that, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TS 21.111: "USIM and IC Card Requirements".

[2] 3GPP TS 31.102: "Characteristics of the USIM Application".

[3] 3GPP TS 31.101: "UICC-Terminal Interface, Physical and Logical Characteristics".

[4] 3GPP TS 33.102: "3G Security; Security Architecture".

[5] 3GPP TS 33.103: "3G Security; Integration Guidelines".

[6] ISO/IEC 7816-4 (1995): "Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 4: Interindustry commands for interchange".

[7] ISO/IEC 7816-5 (1994): "Identification cards - Integrated circuit(s) cards with contacts - Part 5: Numbering system and registration procedure for application identifiers".

[8] void

[9] 3GPP TS 23.003: "Numbering, Addressing and Identification".

[10] ISO/IEC 7816-9 (2000): "Identification cards - Integrated circuit(s) cards with contacts - Part 9: Additional interindustry commands and security attributes".

[11] ISO/IEC 7816-6 (1996): "Identification cards - Integrated circuit(s) cards with contacts - Part 6: Interindustry data elements".

[12] 3GPP TS 25.101: "UE Radio Transmission and Reception (FDD)".

[13] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[14] 3GPP TS 33.203: "3G security; Access security for IP-based services".

[15] 3GPP TS 24.228: "Signalling flows for the IP multimedia call control based on SIP and SDP; Stage 3".

[16] IETF RFC 3261: "SIP: Session Initiation Protocol".

[17] 3GPP TS 23.038: "Alphabets and language-specific information".

[18] ISO 639 (1988): "Code for the representation of names of languages".

[19] 3GPP TS 51.011: "Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface".

[20] ISO/IEC 8825(1990): "Information technology - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)" Second Edition.

[21] 3GPP TS 22.101: "Service aspects; Service principles".

[22] ETSI TS 102 223: "Smart cards; Card Application Toolkit (CAT)".

[23] ETSI TS 101 220: "Smart cards; ETSI numbering system for telecommunication application providers".

[24] IETF RFC 2486: "The Network Access Identifier"

[xx] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic bootstrapping architecture"

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	3rd Generation Partnership Project
AC	Access Condition
ADF	Application Dedicated File
AID	Application IDentifier
AK	Anonymity Key
AKA	Authentication and Key Agreement
ALW	ALWays
AMF	Authentication Management Field
ASN.1	Abstract Syntax Notation One
AuC	Authentication Centre
AUTN	AUthentication TokeN
BER-TLV	Basic Encoding Rule – TLV
B-TID	Bootstrapping Transaction IDentifier
CK	Cipher Key
DF	Dedicated File
EF	Elementary File
FFS	For Further Study
HE	Home Environment
HN	Home Network
ICC	Integrated Circuit Card
ID	IDentifier
IK	Integrity Key
IM	IP Multimedia
IMPI	IM Private Identity
IMPU	IM PUblic identity
IMS	IP Multimedia Subsystem
ISIM	IM Services Identity Module
K	long-term secret Key shared between the ISIM and the AuC
KSI	Key Set Identifier
LI	Language Indication
LSB	Least Significant Bit
MAC	Message Authentication Code
MF	Master File
MSB	Most Significant Bit
NAI	Network Access Identifier
NEV	NEVer
PIN	Personal Identification Number
PL	Preferred Languages
PS_DO	PIN Status Data Object
RAND	RANDom challenge
RES	user RESponse
RFU	Reserved for Future Use
RST	ReSeT
SDP	Session Description Protocol
SFI	Short EF Identifier
SIP	Session Initiation Protocol
SQN	SeQuence Number
SW	Status Word
TLV	Tag Length Value
UE	User Equipment
XRES	eXpected user RESponse

4.2.7 EF_{IST} (ISIM Service Table)

This EF indicates which optional services are available. If a service is not indicated as available in the ISIM, the ME shall not select this service. The presence of this file is mandatory if optional services are provided in the ISIM.

Identifier: '6F07'	Structure: transparent	Optional
SFI: '07'		
File size: X bytes, X >= 1	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Services n°1 to n°8	M	1 byte
2	Services n°9 to n°16	O	1 byte
3	Services n°17 to n°24	O	1 byte
4	Services n°25 to n°32	O	1 byte
etc.			
X	Services n°(8X-7) to n°(8X)	O	1 byte

-Services

Contents:	Service n°1:	P-CSCF address
	Service n°xx	Generic Bootstrapping Architecture (GBA)

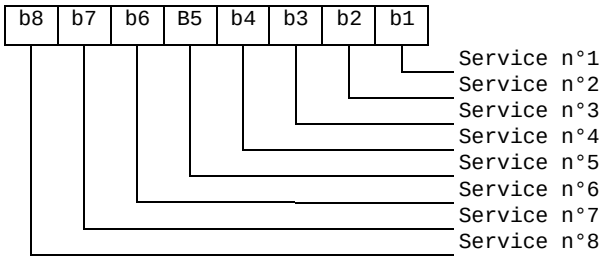
The EF shall contain at least one byte. Further bytes may be included, but if the EF includes an optional byte, then it is mandatory for the EF to also contain all bytes before that byte. Other services are possible in the future and will be coded on further bytes in the EF. The coding falls under the responsibility of the 3GPP.

Coding:

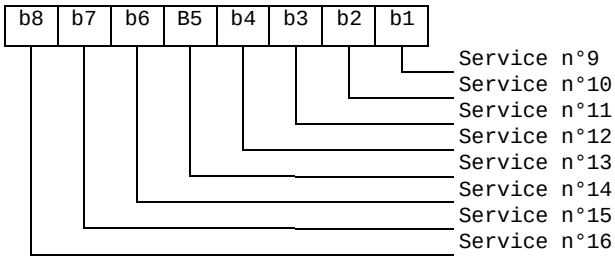
1 bit is used to code each service:
bit = 1: service available;
bit = 0: service not available.

- Service available means that the ISIM has the capability to support the service and that the service is available for the user of the USIM.
  Service not available means that the service shall not be used by the ISIM user, even if the ISIM has the capability to support the service.

First byte:



Second byte:



etc.

**********NEXT CHANGE**********

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

4.2.x EF_{GBABP} (GBA Bootstrapping parameters)

This EF contains the AKA Random challenge (RAND) and Bootstrapping Transaction Identifier (B-TID) associated with a GBA bootstrapping procedure. This file shall be present if the GBA service (service number xx) is allocated in EF_{IST} (ISIM Service Table).

Identifier: '6FXX'	Structure: transparent	Optional
File length: L+X+2 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Length of RAND (16)	M	1 byte
2 to (X+1)	RAND	M	X bytes
X+2	Length of B-TID (L)	M	1 byte
(X+2) to (X+1+L)	B-TID	M	L bytes

- Length of RAND
  Contents: number of bytes, not including this length byte, of RAND field

- RAND
  Contents: Random challenge used in the GBA_U bootstrapping procedure.
  Coding: as defined in 33.103 [13]

- Length of B-TID
  Contents: number of bytes, not including this length byte, of B-TID field

- B-TID
  Content: Bootstrapping Transaction Identifier the GBA_U bootstrapped keys
  Coding: As defined in TS 33.220 [xx]

**********NEXT CHANGE**********

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}.

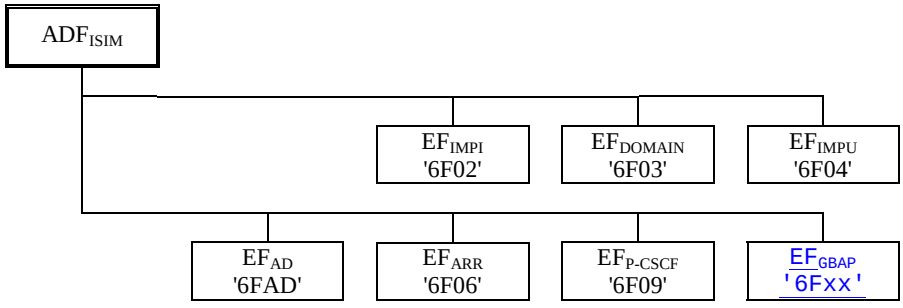


Figure 1: File identifiers and directory structures of ISIM

**********NEXT CHANGE**********

5.2 ISIM security related procedures

5.2.x 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 in EF_{GBABP}

5.2.y Generic Bootstrapping architecture (NAF Derivation)

The Terminal shall first read EF_{GBABP}. The Terminal then uses the AUTHENTICATE command in GBA security context (NAF Derviation Mode) (see 7.1.1). The response is sent to the Terminal.

******************NEXT CHANGE***

7.1 AUTHENTICATE

7.1.1 Command description

The function can be used in several different contexts:

-IMS security context ~~The function is used~~ during the procedure for authenticating the ISIM to its HN and vice versa. In addition, a cipher key and an integrity key are calculated. For the execution of the command the ISIM uses the subscriber authentication key K, which is stored in the ISIM. The function shall be used whenever an IMS context shall be established, i.e. when the terminal receives a challenge from the IMS.

-a GBA_U security context, when a GBA bootstrapping procedure is requested. In this context the function is used in two different modes:

a) Bootstrapping Mode: during the procedure for muthual authenticating of the ISIM and the Bootstrapping Server Function (BSF) and for deriving Bootstrapped key material from the AKA run.

b) NAF Derivation Mode: during the procedure for deriving Network Application Function (NAF) specific keys from previous bootstrapped key material.

The function is related to a particular ISIM and shall not be executable unless the ISIM application has been selected and activated, and the current directory is the ISIM ADF or any subdirectory under this ADF and a successful PIN verification procedure has been performed (see clause 5).

~~The function shall be used whenever an IMS context shall be established, i.e. when the terminal receives a challenge from the IMS.~~

7.1.1.1 IMS security context

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

Then the ISIM computes XMAC = $f1_K$ (SQN || RAND || AMF) and compares this with the MAC which is included in AUTN. If they are different, the ISIM abandons the function.

Next the ISIM verifies that the received sequence number SQN is previously unused. If it is unused and its value is lower than SQN_{MS}, it shall still be accepted if it is among the last 32 sequence numbers generated. A possible verification method is described in 3GPP TS 33.102 [4].

NOTE: This implies that the ISIM has to keep a list of the last used sequence numbers and the length of the list is at least 32 entries.

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, where:

- $AUTS = Conc(SQN_{MS}) \,||\, MACS$;
- $Conc(SQN_{MS}) = SQN_{MS} \oplus f5^*_K(RAND)$ is the concealed value of the counter SQN_{MS} in the ISIM; and
- $MACS = f1^*_K(SQN_{MS} \,||\, RAND \,||\, AMF)$ where:
- *RAND* is the random value received in the current user authentication request;

the AMF assumes a dummy value of all zeroes so that it does not need to be transmitted in clear in the resynchronisation message.

If the sequence number is considered in the correct range, the ISIM computes RES = $f2_K$ (RAND), the cipher key CK = $f3_K$ (RAND) and the integrity key IK = $f4_K$ (RAND) and includes these in the command response. Note that if this is more efficient, RES, CK and IK could also be computed earlier at any time after receiving RAND.

The use of AMF is HN specific and while processing the command, the content of the AMF has to be interpreted in the appropriate manner. The AMF may e.g. be used for support of multiple algorithms or keys or for changing the size of lists, see 3GPP TS 33.102 [4].

**********NEXT CHANGE**********

7.1.1.2 GBA security context (Bootstrapping Mode)

ISIM operations in GBA security context are supported if service n°xx 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 [xx]). 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 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 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 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.

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

Input:

- RAND, AUTN

Output:

- RES

or

- AUTS

7.1.1.y GBA security context (NAF Derivation Mode)

ISIM operations in GBA security context are supported if service n°xx 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 [xx] 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.

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

7.1.2 Command parameters and data

Code	Value
CLA	As specified in 3GPP TS 31.101
INS	'88'
P1	'00'
P2	See table below
Lc	See below
Data	See below
Le	'00', or maximum length of data expected in response

Parameter P2 specifies the authentication context as follows:

Coding of the reference control P2:

Coding b8-b1	Meaning
'1-------'	Specific reference data (e.g. DF specific/application dependant key)
'-XXXXXX-'	'000000'
'-----X-X-X'	Authentication context: 000 Reserved 001 3G IMS context 010 Reserved 100 GBA context

All other codings are RFU.

Command parameters/data:

7.1.2.1 IMS security context

Byte(s)	Description	Length
1	Length of RAND (L1)	1
2 to (L1+1)	RAND	L1
(L1+2)	Length of AUTN (L2)	1
(L1+3) to (L1+L2+2)	AUTN	L2

The coding of AUTN is described in 3GPP TS 33.102 [4]. The most significant bit of RAND is coded on bit 8 of byte 2. The most significant bit of AUTN is coded on bit 8 of byte (L1+3).

Response parameters/data, case 1, command successful:

Byte(s)	Description	Length
1	"Successful 3G authentication" tag = 'DB'	1
2	Length of RES (L3)	1
3 to (L3+2)	RES	L3
(L3+3)	Length of CK (L4)	1
(L3+4) to (L3+L4+3)	CK	L4
(L3+L4+4)	Length of IK (L5)	1
(L3+L4+5) to (L3+L4+L5+4)	IK	L5

The most significant bit of RES is coded on bit 8 of byte 3. The most significant bit of CK is coded on bit 8 of byte (L3+4). The most significant bit of IK is coded on bit 8 of byte (L3+L4+5).

Response parameters/data, case 2, synchronization failure:

Byte(s)	Description	Length
1	"Synchronisation failure" tag = 'DC'	1
2	Length of AUTS (L1)	1
3 to (L1+2)	AUTS	L1

The coding of AUTS is described in 3GPP TS 33.102 [4]. The most significant bit of AUTS is coded on bit 8 of byte 3.

7.1.2.x GBA security context (Bootstrapping Mode)

Byte(s)	Description	Length
1	“GBA Security Context Bootstrapping Mode” tag = ‘DD’	1
2	Length of RAND (L1)	1
3 to (L1+2)	RAND	L1
(L1+3)	Length of AUTN (L2)	1
(L1+4) to (L1+L2+3)	AUTN	L2

Response parameters/data, GBA security context (Bootstrapping Mode), synchronisation failure:

Byte(s)	Description	Length
1	"Synchronisation failure" tag = 'DC'	1
2	Length of AUTS (L1)	1
3 to (L1+2)	AUTS	L1

AUTS coded as for IMS Security context.

Response parameters/data, GBA security context (Bootstrapping Mode), command successful:

Byte(s)	Description	Length
1	"Successful GBA operation" tag = 'DB'	1
2	Length of RES (L)	1
3 to (L+2)	RES	L

RES coded as for IMS Security context.

7.1.2.y GBA security context (NAF Derivation Mode)

Byte(s)	Description	Length
1	“GBA Security Context NAF Derivation Mode” tag = ‘DE’	1
2	Length of NAF_ID (L1)	1
3 to (L1+2)	NAF_ID	L1

Response parameters/data, GBA security context (NAF Derivation Mode), command successful:

Byte(s)	Description	Length
1	"Successful GBA operation" tag = 'DB'	1
2	Length of Ks_ext_NAF (L)	1
3 to (L+2)	Ks_ext_NAF	L

Coding of Ks_ext_NAF as described in TS 33.220 [xx].

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
'6F08'	Ciphering and Integrity Keys for IMS	No
'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
'6FXX'	GBA Bootstrapping parameters	Caution
NOTE: If EF_{IMPI}, EF_{IMPU} or EF_{DOMAIN} 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
'6F08'	Ciphering and Integrity Keys for IMS	'07FF…FF'
'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
'6FXX'	GBA Bootstrapping parameters	'FF…FF'

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

Tdoc ⌘ T3-040590

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.103** **CR** 016 ⌘ **rev** **-** ⌘ Current version: **6.4.0** ⌘

*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:	⌘	New 3GPP2 IMS authentication context in ISIM
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	12/08/2004
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:	⌘	New IMS authentication context (HTTP Digest) is needed for the following considerations: - In 3GPP2 IMS authentication, IMS AKA is one of the option although it is required by 3GPP - 3GPP2 allows another IMS authentication mechanism (HTTP digest) as an alternative - Minimum support of HTTP digest needs to be specified in authenticate command The following are suggested changes to ISIM standard. However, we are flexible with encoding details for P2 in commands parameters.
Summary of change:	⌘	Introduction of a new security context (HTTP Digest) in AUTHENTICATE command
Consequences if not approved:	⌘	

Clauses affected:	⌘	7.1.2

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

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.

2 References

The following documents contain provisions that, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TS 21.111: "USIM and IC Card Requirements".

[2] 3GPP TS 31.102: "Characteristics of the USIM Application".

[3] 3GPP TS 31.101: "UICC-Terminal Interface, Physical and Logical Characteristics".

[4] 3GPP TS 33.102: "3G Security; Security Architecture".

[5] 3GPP TS 33.103: "3G Security; Integration Guidelines".

[6] ISO/IEC 7816-4 (1995): "Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 4: Interindustry commands for interchange".

[7] ISO/IEC 7816-5 (1994): "Identification cards - Integrated circuit(s) cards with contacts - Part 5: Numbering system and registration procedure for application identifiers".

[8] void

[9] 3GPP TS 23.003: "Numbering, Addressing and Identification".

[10] ISO/IEC 7816-9 (2000): "Identification cards - Integrated circuit(s) cards with contacts - Part 9: Additional interindustry commands and security attributes".

[11] ISO/IEC 7816-6 (1996): "Identification cards - Integrated circuit(s) cards with contacts - Part 6: Interindustry data elements".

[12] 3GPP TS 25.101: "UE Radio Transmission and Reception (FDD)".

[13] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[14] 3GPP TS 33.203: "3G security; Access security for IP-based services".

[15] 3GPP TS 24.228: "Signalling flows for the IP multimedia call control based on SIP and SDP; Stage 3".

[16] IETF RFC 3261: "SIP: Session Initiation Protocol".

[17] 3GPP TS 23.038: "Alphabets and language-specific information".

[18] ISO 639 (1988): "Code for the representation of names of languages".

[19] 3GPP TS 51.011: "Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface".

[20] ISO/IEC 8825(1990): "Information technology - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)" Second Edition.

[21] 3GPP TS 22.101: "Service aspects; Service principles".

[22] ETSI TS 102 223: "Smart cards; Card Application Toolkit (CAT)".

[23] ETSI TS 101 220: "Smart cards; ETSI numbering system for telecommunication application providers".

[24] IETF RFC 2486: "The Network Access Identifier"

[xx] IETF RFC 2617: "HTTP Authentication: Basic and Digest Access Authentication". (http://www.ietf.org/rfc/rfc2617.txt)

7.1 AUTHENTICATE

7.1.1 Command description

The function is used during the procedure for authenticating the ISIM to its HN and vice versa. ~~In addition, a cipher key and an integrity key are calculated. For the execution of the command the ISIM uses the subscriber authentication key K, which is stored in the ISIM.~~The function can be used in several different contexts:

- an IMS AKA security context, when IMS AKA authentication data are available. A cipher key and an integrity key are calculated. For the execution of the command the ISIM uses the subscriber authentication key K, which is stored in the ISIM.
- a HTTP Digest security context, when HTTP Digest authentication data are available. Digest authentication operations are described in IETF RFC 2617 [xx].

The function is related to a particular ISIM and shall not be executable unless the ISIM application has been selected and activated, and the current directory is the ISIM ADF or any subdirectory under this ADF and a successful PIN verification procedure has been performed (see clause 5).

~~The function shall be used whenever an IMS context shall be established, i.e. when the terminal receives a challenge from the IMS.~~

7.1.1.1 IMS AKA security context

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

Then the ISIM computes XMAC = $f1_K$ (SQN || RAND || AMF) and compares this with the MAC which is included in AUTN. If they are different, the ISIM abandons the function.

Next the ISIM verifies that the received sequence number SQN is previously unused. If it is unused and its value is lower than SQN_{MS}, it shall still be accepted if it is among the last 32 sequence numbers generated. A possible verification method is described in 3GPP TS 33.102 [4].

NOTE: This implies that the ISIM has to keep a list of the last used sequence numbers and the length of the list is at least 32 entries.

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, where:

- $AUTS = Conc(SQN_{MS}) \,||\, MACS$;
- $Conc(SQN_{MS}) = SQN_{MS} \oplus f5^*_K(RAND)$ is the concealed value of the counter SQN_{MS} in the ISIM; and
- $MACS = f1^*_K(SQN_{MS} \,||\, RAND \,||\, AMF)$ where:
- *RAND* is the random value received in the current user authentication request;

the AMF assumes a dummy value of all zeroes so that it does not need to be transmitted in clear in the resynchronisation message.

If the sequence number is considered in the correct range, the ISIM computes RES = $f2_K$ (RAND), the cipher key CK = $f3_K$ (RAND) and the integrity key IK = $f4_K$ (RAND) and includes these in the command response. Note that if this is more efficient, RES, CK and IK could also be computed earlier at any time after receiving RAND.

The use of AMF is HN specific and while processing the command, the content of the AMF has to be interpreted in the appropriate manner. The AMF may e.g. be used for support of multiple algorithms or keys or for changing the size of lists, see 3GPP TS 33.102 [4].

7.1.2 Command parameters and data

Code	Value
CLA	As specified in 3GPP TS 31.101
INS	'88'
P1	'00'
P2	See table below
Lc	See below
Data	See below
Le	'00', or maximum length of data expected in response

Parameter P2 specifies the authentication context as follows:

Coding of the reference control P2:

Coding b8-b1	Meaning
'1-------'	Specific reference data (e.g. DF specific/application dependant key)
'-XXXXXX-'	'000000'
'-------X'	Authentication context: 0 Reserved 1 ~~3G IMS context~~IMS AKA 2 HTTP Digest

All other codings are RFU.

Command parameters/data:

7.1.2.x IMS AKA security context

Byte(s)	Description	Length
1	Length of RAND (L1)	1
2 to (L1+1)	RAND	L1
(L1+2)	Length of AUTN (L2)	1
(L1+3) to (L1+L2+2)	AUTN	L2

The coding of AUTN is described in 3GPP TS 33.102 [4]. The most significant bit of RAND is coded on bit 8 of byte 2. The most significant bit of AUTN is coded on bit 8 of byte (L1+3).

Response parameters/data, case 1, command successful:

Byte(s)	Description	Length
1	"Successful 3G authentication" tag = 'DB'	1
2	Length of RES (L3)	1
3 to (L3+2)	RES	L3
(L3+3)	Length of CK (L4)	1
(L3+4) to (L3+L4+3)	CK	L4
(L3+L4+4)	Length of IK (L5)	1
(L3+L4+5) to (L3+L4+L5+4)	IK	L5

The most significant bit of RES is coded on bit 8 of byte 3. The most significant bit of CK is coded on bit 8 of byte (L3+4). The most significant bit of IK is coded on bit 8 of byte (L3+L4+5).

Response parameters/data, case 2, synchronization failure:

Byte(s)	Description	Length
1	"Synchronisation failure" tag = 'DC'	1
2	Length of AUTS (L1)	1
3 to (L1+2)	AUTS	L1

The coding of AUTS is described in 3GPP TS 33.102 [4]. The most significant bit of AUTS is coded on bit 8 of byte 3.

7.1.2.y HTTP Digest security context

Byte(s)	Description	Length
1	Length of realm (L1)	1
2 to (L1+1)	Realm	L1
(L1+2)	Length of nonce (L2)	1
(L1+3) to (L1+L2+2)	Nonce	L2
(L1+L2+3)	Length of cnonce (L3)	1
(L1+L2+4) to (L1+L2+L3+3)	Cnonce	L3

The codings of realm, nonce and cnonce are described in IETF RFC 2617 [xx].

Response parameters/data command successful:

Byte(s)	Description	Length
1	"HTTP Digest context reponse" tag = 'DB'	1
2	Length of Response(L4)	1
3 to (L4+2)	Response	L4
(L4+3)	Length of Session Key (L5)	1
(L4+4) to (L4+L5+3)	Session Key	L5

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

Tdoc ⌘ T3-040607
Superseeds *T3-040474*

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.103** **CR** 018 ⌘ **rev** **-** ⌘ Current version: **5.6.0** ⌘

*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:	⌘	Correction of PPS procedure
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	13/08/2004
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)*
Rel-7	*(Release 7)*

Reason for change:	⌘	The terminal may not invoke the PPS procedure as defined in TS 31.101 if the content of TA1 in the ATR is not rrecognised by the terminal. The terminal is according to the specification capable of operating with other than default values and the terminal invokes the PPS procedure in order to try to select another value before using the default values
Summary of change:	⌘	Introduce the PPS procedure
Consequences if not approved:	⌘	Terminals that not can support/recognise the value in TA1 in the ATR may not invoke the PPS procedure to increase the speed on the interface according to its capabilities

Clauses affected:	⌘	8.x (new)

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

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.

8.x PPS procedure

If the value of TA1 in the ATR is not '11' or '01', the PPS procedure shall be used.

When the terminal does not support or cannot recognize the values indicated by the card in character TA1 of the ATR, it shall initiate at least one PPS procedure indicating Fi and Di values specified in TS 31.101 [3] before issuing a PPS with default values.