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

TP-040203

Title: LS concerning harmonization ISIM between 3GPP & 3GPP2

Response to: LS from 3GPP2 TSG-C on ISIM harmonisation

Source: 3GPP TSG T
To: 3GPP2-TSG-C,
Cc: TSG T3

Contact Person:
Name: Nigel Barnes
Tel. Number: +44 1256 790 169
E-mail Address: Nigel.Barnes@motorola.com

Attachments: T3-040590

Overall Description:

Attached please find the approved CR to TS 31.103, which was approved at the recent 3GPP TSG T#25 meeting in Palm Springs.

TSG T and TSG T3 look forward to further harmonising their work with regard to smart cards.

Actions:

3GPP2 TSG-C is invited to note that the CR was approved at 3GPP T#25.

Date of next TP Meeting:

TP#26	8-10 December 2004	Athens, Greece

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