3GPP TSG-SA3 Meeting #19
Newbury, UK, 4-6 July, 2001

Tdoc S3-010384

CR-Form-v3

CHANGE REQUEST

⌘ **33.103** **CR** **16** ⌘ rev **1** ⌘ Current version: **3.5.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM [X] ME/UE [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Correction of USIM data elements for AKA
Source:	⌘	Gemplus
Work item code:	⌘	TEI
Date:	⌘	03-07-2001
Category:	⌘	**F**
Release:	⌘	R99

Use one of the following categories:
- ***F*** *(essential correction)*
- ***A*** *(corresponds to a correction in an earlier release)*
- ***B*** *(Addition of feature),*
- ***C*** *(Functional modification of feature)*
- ***D*** *(Editorial modification)*

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)*

Reason for change:	⌘	33.103 has not been updated regarding some CRs approved on 33.102. As a result, the table regarding the parameters to be stored on the USIM for AKA needs some correction to be consistent.
Summary of change:	⌘	Removal of the following data elements : - WINDOW – LIST – $RAND_G$ – SRES Addition of the array for previously reveived sequence numbers. The "THRESHOLD" status is changed from optional to mandatory and its length is corrected to 24 bits. Clarification that (KSI, CK, IK) are stored for each domain.
Consequences if not approved:	⌘	Inconsistency of the specifications.

Clauses affected:	⌘	Section 4.2.2
Other specs affected:	⌘	[ ] Other core specifications ⌘ [ ] Test specifications [ ] O&M Specifications
Other comments:	⌘	

4.2.2 Authentication and key agreement (AKA_{USIM})

The USIM shall support the UMTS mechanism for authentication and key agreement described in 6.3 of 3G TS 33.102.

The following data elements need to be stored on the USIM:

a) K: a permanent secret key;

b) SQN_{MS}: a counter that is equal to the highest sequence number SQN in an AUTN parameter accepted by the user;

c) SQN_{MS} [ ] array: an array for past accepted sequence numbers

~~c~~d) $RAND_{MS}$: the random challenge which was received together with the last AUTN parameter accepted by the user. It is used to calculate the re-synchronisation message together with the highest accepted sequence number (SQN_{MS});

~~d~~e) KSI: key set identifier;

~~e~~f) $THRESHOLD_{C}$: a threshold defined by the HE to trigger re-authentication and to control the cipher key lifetime;

~~f~~g) CK The access link cipher key established as part of authentication;

~~g~~h) IK The access link integrity key established as part of authentication;

~~h~~i) $HFN_{MS:}$ Stored Hyper Frame Number provides the Initialisation value for most significant part of COUNT-C and COUNT-I. The least significant part is obtained from the RRC sequence number;

~~i~~j) AMF: A 16-bit field used Authentication Management. The use and format are unspecified in the architecture but examples are given in an informative annex;

~~j~~k) The GSM authentication parameter and GSM cipher key derived from the UMTS to GSM conversion functions.

Table 3 provides an overview of the data elements stored on the USIM to support authentication and key agreement.

Table 3: USIM – Authentication and key agreement – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
K	Permanent secret key	1 (note 1)	Permanent	128 bits	Mandatory
SQN_{MS}	Highest previously accepted sSequence number counter	1	Updated when AKA protocol is executed	48 bits	Mandatory
SQN_{MS}[ ] array	array of last accepted sequence number	1	Updated when AKA protocol is executed	at least 32 entries	Mandatory
~~WINDOW (option 1)~~	~~accepted sequence number array~~	~~1~~	~~Updated when AKA protocol is executed~~	~~10 to 100 bits~~	~~Optional~~
~~LIST (option 2)~~	~~Ordered list of sequence numbers received~~	~~1~~	~~Updated when AKA protocol is executed~~	~~32-64 bits~~	~~Optional~~
$RAND_{MS}$	Random challenge received by the user.	1	Updated when AKA protocol is executed	128 bits	Mandatory
KSI	Key set identifier	~~1~~2 (note 2)	Updated when AKA protocol is executed	3 bits	Mandatory
$THRESHOLD_{~~G~~}$	Threshold value for cipher~~ing~~ key lifetime	1	Permanent	~~32~~24 bits	~~Optional~~Mandatory
CK	Cipher key	~~1~~2 (note 2)	Updated when AKA protocol is executed	128 bits	Mandatory
IK	Integrity key	~~1~~ 2 (note 2)	Updated when AKA protocol is executed	128 bits	Mandatory
$HFN_{MS:}$	Initialisation value for most significant part for COUNT-C and for COUNT-I	1	Updated when connection is released	25 bits	Mandatory
AMF	Authentication Management Field (indicates the algorithm and key in use)	1	Updated when AKA protocol is executed	16 bits	Mandatory
~~$RAND_{G}$~~	~~GSM authentication parameter from conversion function~~	~~1~~	~~Updated when GSM AKA or UMTS AKA protocol is executed~~	~~As for GSM~~	~~Optional~~
~~SRES~~	~~GSM authentication parameter from conversion function~~	~~1~~	~~Updated when GSM AKA or UMTS AKA protocol is executed~~	~~As for GSM~~	~~Optional~~
Kc	GSM cipher Key	~~1~~ 2 (note 2)	Updated when GSM AKA or UMTS AKA protocol is executed	As for GSM	Optional

NOTE 1: HE policy may dictate more than one, the active key signalled using the AMF function.

NOTE 2: one for circuit-switched domain, one for packet-switched domain.