

## CHANGE REQUEST

⌘ **33.103 CR 016** ⌘ rev **2** ⌘ Current version: **3.6.0** ⌘

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

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

<b>Title:</b>	⌘ Correction of USIM data elements for AKA		
<b>Source:</b>	⌘ SA WG3		
<b>Work item code:</b>	⌘ TEI	<b>Date:</b>	⌘ 03-07-2001
<b>Category:</b>	⌘ <b>F</b>	<b>Release:</b>	⌘ R99
	Use <u>one</u> of the following categories: <b>F</b> (essential correction) <b>A</b> (corresponds to a correction in an earlier release) <b>B</b> (Addition of feature), <b>C</b> (Functional modification of feature) <b>D</b> (Editorial modification)		Use <u>one</u> 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)

<b>Reason for change:</b>	⌘ 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.
<b>Summary of change:</b>	⌘ Removal of the following data elements : - WINDOW - LIST - RAND <sub>G</sub> - SRES  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.
<b>Consequences if not approved:</b>	⌘ Inconsistency of the specifications.

<b>Clauses affected:</b>	⌘ Section 4.2.2		
<b>Other specs affected:</b>	⌘ <input type="checkbox"/> Other core specifications <input type="checkbox"/> Test specifications <input type="checkbox"/> O&M Specifications	⌘	
<b>Other comments:</b>	⌘		

## 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)  $RAND_{MS}$ : 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) KSI: key set identifier;
- e)  $THRESHOLD_e$ : a threshold defined by the HE to trigger re-authentication and to control the cipher key lifetime;
- f) CK The access link cipher key established as part of authentication;
- g) IK The access link integrity key established as part of authentication;
- h)  $HFN_{MS}$ : 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) 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) 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 <sub>MS</sub>	Highest previously accepted sequence number counter	1	Updated when AKA protocol is executed	48 bits	Mandatory
SQN <sub>MS</sub> [ ] array	array of last accepted sequence number	1	Updated when AKA protocol is executed	at least 32 entries	MandatoryOptional
WINDOW (option 1)	accepted sequence number array	4	Updated when AKA protocol is executed	40 to 100 bits	Optional
LIST (option 2)	Ordered list of sequence numbers received	4	Updated when AKA protocol is executed	32-64 bits	Optional
RAND <sub>MS</sub>	Random challenge received by the user.	1	Updated when AKA protocol is executed	128 bits	Mandatory
KSI	Key set identifier	4 2 (note 2)	Updated when AKA protocol is executed	3 bits	Mandatory
THRESHOLD <sub>e</sub>	Threshold value for ciphering key lifetime	1	Permanent	3224 bits	OptionalMandatory
CK	Cipher key	4 2 (note 2)	Updated when AKA protocol is executed	128 bits	Mandatory
IK	Integrity key	4 2 (note 2)	Updated when AKA protocol is executed	128 bits	Mandatory
HFN <sub>MS</sub>	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 <sub>e</sub>	GSM authentication parameter from conversion function	4	Updated when GSM AKA or UMTS AKA protocol is executed	As for GSM	Optional
SRES	GSM authentication parameter from conversion function	4	Updated when GSM AKA or UMTS AKA protocol is executed	As for GSM	Optional
Kc	GSM cipher Key	4 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.