3GPP TSG SA WG 3 (Security) meeting #10 **S3-000044**
Antwerpen, 19—21 January, 2000.

3G CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

33.102 **CR** Current Version: 3.3.1

3G specification number ↑ *↑ CR number as allocated by 3G support team*

For submission to TSG: SA #7 *list TSG meeting no. here ↑*
for approval: X *(only one box should be marked with an X)*
for information:

Form: 3G CR cover sheet, version 1.0 *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/3GCRF-xx.rtf*

Proposed change affects: *(at least one should be marked with an X)* USIM [X] ME [ ] UTRAN [ ] Core Network [ ]

Source: Ericsson **Date:** 2000-Jan-17

Subject: Local Authenication and connection establishment

3G Work item: Security

Category: *(only one category shall be marked with an X)*

F	Correction	
A	Corresponds to a correction in a 2G specification	
B	Addition of feature	
C	Functional modification of feature	
D	Editorial modification	X

Reason for change: Clarification needed on :
Local Authentication, Cipher and integrity key setting and
Cipher and integrity key identification

Clauses affected: 6.4, 6.4.1 and 6.4.4

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs:
Other 2G core specifications	[ ]	→ List of CRs:
MS test specifications	[ ]	→ List of CRs:
BSS test specifications	[ ]	→ List of CRs:
O&M specifications	[ ]	→ List of CRs:

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR.

6.4 Local authentication and connection establishment

Local authentication is obtained by integrity protection functionality.

6.4.1 Cipher key and integrity key setting

~~Mutual key setting is the procedure that allows the MS and the RNC to agree on the key IK used to compute message authentication codes using algorithm UIA.~~ Authentication and key setting ~~is~~ are triggered by the authentication procedure and described in 6.3. Authentication and key setting may be initiated by the network as often as the network operator wishes. Key setting can occur as soon as the identity of the mobile subscriber (i.e. P-TMSI, TM~~U~~SI or IM~~U~~SI) is known by the ~~SN/~~VLR/SGSN. The CK and~~key~~ IK ~~is~~are stored in the ~~SN/~~VLR/SGSN and transferred to the RNC when ~~it is~~ needed. The CK and ~~key~~ IK for the CS domain are ~~is~~ stored ~~i~~on the USIM ~~until it is~~ and updated at the next authentication from this domain. The CK and IK for the PS domain are stored on the USIM and updated at the next authentication from this domain.

If an authentication procedure is performed during a data transfer in the PS mode, the new cipher key CK and integrity key IK shall be taken in use in both the RNC and the UE as part of the security mode negotiation (see 6.4.5) that follows the authentication procedure.

6.4.4 Cipher key and integrity key identification

The key set identifier (KSI) is a number which is associated with the cipher and integrity keys derived during authentication. The key set identifier is allocated by the network and sent with the authentication request message to the mobile station where it is stored together with the calculated cipher key CK and integrity key IK. KSI in UMTS corresponds to CKSN in GSM. The USIM stores one KSI/CKSN for the PS domain key set and one KSI/CKSN for the CS domain key set.

The purpose of the key set identifier is to make it possible for the network to identify the cipher key CK and integrity key IK which ~~is~~are stored in the mobile station without invoking the authentication procedure. This is used to allow re-use of the cipher key CK and integrity key IK during subsequent connection set-ups.

KSI and CKSN have the same format. The key set identifier is three bits. Seven values are used to identify the key set. A value of "111" is used by the mobile station to indicate that a valid key is not available for use. The value '111' in the other direction from network to mobile station is reserved.