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	**057**	Current Version:	3.3.1

GSM (AA.BB) or 3G (AA.BBB) specification number ↑   *↑ CR number as allocated by MCC support team*

For submission to:	TSG SA #7	for approval	**X**	strategic		*(for SMG*
list expected approval meeting # here ↑		for information		non-strategic		*use only)*

Form: CR cover sheet, version 2 for 3GPP and SMG   The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc

Proposed change affects: (U)SIM **X**   ME **X**   UTRAN / Radio **X**   Core Network **X**
(at least one should be marked with an X)

Source:	Ericsson		**Date:**	2000-02-17

Subject:	Cipher key and integrity key selection

Work item:	Security

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

F	Correction			Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification	**X**		Release 99	**X**
				Release 00	

Reason for change:	Editorial changes in the section 6.3.3.1

Clauses affected:	6.3.3.1, 6.3.3.1.2

Other specs affected:

Other 3G core specifications		→ List of CRs:	
Other GSM 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.

6.3.3.1 Cipher key and integrity key selection

Because of the separate mobility management for CS and PS services, the USIM establishes a separate cipher/integrity keys set with both each of the CS and the PS core network service domains. The conditions on the use of these cipher keys in the user and control planes are given below.

6.3.3.1.1 User plane

The CS user data connections are ciphered with the cipher key CK_{CS} established between the user and the 3G CS core network service domain and identified in the security mode setting procedure. The PS user data connections are ciphered with the cipher key CK_{PS} established between the user and the 3G PS core network service domain and identified in the security mode setting procedure.

6.3.3.1.2 Control plane

When a security mode setting procedure is performed, the established cipher/integrity key set of the core network service domain that is specified by this procedure is applied to the common signalling plane, what ever core network service domain is specified in the procedure. This may require that the cipher/integrity key of an (already ciphered/integrity protected) ongoing signalling connection is changed. This change should be completed within five seconds.