Technical Specification Group Services and System Aspects *TSGS#5(99)495*
(=S3-99351, rev. of S3-99265)

TSG SA WG3 #5bis, Bonn, 25 August, 1999

DRAFT 3G CHANGE REQUEST

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

TS 33.102 **CR** **20** Current Version: V3.1.0

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

For submission to TSG SA#5 *list TSG meeting no. here ↑* for approval [X] for information [ ] *(only one box should be marked with an X)*

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 [X] UTRAN [X] Core Network [ ]

Source: S3 **Date:** 99-08-25

Subject: Cipher/integrity key setting

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	[X]
D	Editorial modification	[ ]

Reason for change: Within the UTRAN, cipher keys for a user can be generated within both the circuit switched (CS) and packet switched (PS) domains. V3.1.0 of 33.102 contains two options for the handling of cipher keys generated in different domains. This CR removes the options and gives definite requirements.

Clauses affected: 6.6.4

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: It is assumed that the frequency of changing the cipher key of a signalling connection is not a major obstacle.

6.6.4 ~~6.6.4~~ Cipher key selection

Because of the separate mobility management for CS and PS services, the USIM establishes cipher keys with both the CS and the PS core network ~~nodes. Currently two options are considered for the selection of the cipher key:~~service domains. The conditions on the use of these cipher keys in the user and control planes are given below.

6.6.4.1 ~~Option 1: Two key solution~~User plane

The CS user data connections are ciphered with the~~most recent~~ cipher key CK_{CS}~~agreed between the user and the 3G CS core network node.~~ 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~~most recently~~ cipher key CK_{PS} ~~agreed~~established between the user and the 3G PS core network service domain and identified in the security mode setting procedure. ~~node. The (common) signalling data connections are ciphered with the most recently cipher key established between the user and the~~

6.6.4.2 Control plane

~~network, i.e., the youngest of CK_{CS} and CK_{PS}. This requires that the cipher~~When a security mode setting procedure is performed, the cipher/integrity key set by this procedure is applied to the 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~~ after an authentication and key establishment protocol has been executed~~.

~~6.6.4.2 Option 2: One key solution~~

~~All connections (CS user data, PS user data and signalling data) are ciphered with the most recently cipher key CK agreed between the user and either one of the core network nodes. This requires that the cipher key of any (already ciphered) ongoing connection is changed. This change should be completed within five seconds after an authentication an key establishment protocol has been executed.~~