3GPP TSG SA WG3 (Security) meeting #11
Mainz, 22-24 February, 2000

Document* *S3-000167
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

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** **058r1** 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	☒	strategic	□	*(for SMG use only)*
list expected approval meeting # here ↑		for information	□	non-strategic	□	

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 □ ME ☒ UTRAN / Radio ☒ Core Network ☒
(at least one should be marked with an X)

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

Subject: Clarification on ciphering and integrity mode setting

Work item: Security

Category:	F	Correction	☒	**Release:**	Phase 2	□
	A	Corresponds to a correction in an earlier release	□		Release 96	□
(only one category	B	Addition of feature	□		Release 97	□
shall be marked	C	Functional modification of feature	□		Release 98	□
with an X)	D	Editorial modification	□		Release 99	☒
					Release 00	□

Reason for change: Due to the use of a common MS-RNC connection for both CN domains, the two CN domains must have the same preferences and requirements regarding ciphering and integrity mode.
Editorial changes in the section 6.4.2

Clauses affected: 6.4.2

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.

6.4.2 Ciphering ~~key~~ and integrity mode negotiation

When an MS wishes to establish a connection with the network, the MS shall indicate to the network in the MS/USIM Classmark which cipher and integrity algorithms the MS supports. This ~~message~~ information itself must be integrity protected. As it is the case that the RNC does not have the integrity key IK when receiving the MS/USIM Classmark ~~the cipher and i~~this information must be stored in the RNC. ~~and the~~The data integrity of the classmark is performed, during the security mode set-up procedure ~~with~~ by use of the ~~newly~~ ~~last~~ most recently generated IK (see section 6.4.5).~~and this value is transmitted to the RNC after the authentication procedure is complete~~.

The network shall compare its integrity protection capabilities and preferences, and any special requirements of the subscription of the MS, with those indicated by the MS and act according to the following rules:

1) If the MS and the SN have no versions of the UIA algorithm in common, then the connection shall be released.

2) If the MS and the SN have at least one version of the UIA algorithm in common, then the network shall select one of the mutually acceptable versions of the UIA algorithm for use on that connection.

The network shall compare its ciphering capabilities and preferences, and any special requirements of the subscription of the MS, with those indicated by the MS and act according to the following rules:

1) If the MS and the network have no versions of the UEA algorithm in common and the network is not prepared to use an unciphered connection, then the connection shall be released.

2) If the MS and the network have at least one version of the UEA algorithm in common, then the network shall select one of the mutually acceptable versions of the UEA algorithm for use on that connection.

3) If the MS and the network have no versions of the UEA algorithm in common and the user (respectively the user's HE) and the SN are willing to use an unciphered connection, then an unciphered connection shall be used.

Because of the separate mobility management for CS and PS services, one CN domain may, independent of the other CN, establish a connection to one and the same MS. Change of ciphering and integrity mode (algorithms) at establishment of a second MS to CN connection shall not be permitted. The preferences and special requirements for the ciphering and integrity mode setting shall be common for ~~the~~ both domains. (e.g. the order of preference of the algorithms).