3GPP TSG SA 3 Meeting #12
Stockholm, Sweden, 11-14 April 2000

***Document* S3-000252**
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.

03.20	CR		Current Version:	8.0.0

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

Source: Siemens Atea **Date:** April 7, 2000

Subject: GPRS Ciphering algorithm negotiation

Work item: Security

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

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

Reason for change: GSM 03.20 does no reflect the fact that the SGSN and the ME are capable to negotiate an unciphered connection.

Clauses affected: D.4.8

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.

D.4.8 Negotiation of GPRS-A5 algorithm

Not more than seven versions of the A5 algorithm will be defined.

When an MS wishes to establish a connection with the network, the MS shall indicate to the network which version(s) of the GPRS-A5 algorithm it supports. The negotiation of GPRS-A5 algorithm happens during the authentication procedure.

The network may renegotiate the version of the GPRS-A5 algorithm in use at inter SGSN routing area update by performing an authentication procedure.

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 may take one of the following decisions:

~~1) The network decides to release the connection because no common version of the GPRS-A5 algorithm is available or because the MS indicated an illegal combination of supported algorithms.~~

~~2) The network selects one of the mutually acceptable versions of GPRS-A5 to be used.~~

1) If the MS and the network have no versions of the GPRS A5 algorithm in common and the network is not prepared to use an unciphered connections, then the connection is released.

2) If the MS and the network have at least one version of the GPRS A5 algorithm in common, then the network shall select one of the mutually acceptable versions of the GPRS A5 algorithms for use on that connection.

3) If the MS and the network have no versions of the GPRS A5 algorithm in common and the network is willing to use an unciphered version, then an unciphered connection shall be used.