3GPP TSG SA 3 Meeting #17
Gothenburg, 27 Feb – 2 Mar, 2001

***Document* S3-010094**
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	104	Current Version:	3.7.0

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

For submission to:	SA#11	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	X	Core Network	X

Source: Siemens **Date:** 26 Feb, 2001

Subject: Timing of security mode procedure

Work item: Security

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

F	Correction	X	**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			Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change: Sections 6.5.5 and 6.6.5 contain a sentence which gives a time limit for a change of the ciphering and integrity keys to be completed. This time limit is meant to apply to the RNC only. This is clarified as it has created confusion.

Clauses affected: 6.5.5 and 6.6.5

Other specs Affected:				
	Other 3G core specifications	X	→ 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.

6.5.5 Integrity key selection

There may be one IK for CS connections (IK_{CS}), established between the CS service domain and the user and one IK for PS connections (IK_{PS}) established between the PS service domain and the user.

The data integrity of radio bearers for user data is not protected.

The signalling radio bearers are used for transfer of signalling data for services delivered by both CS and PS service domains. These signalling radio bearers are data integrity protected by the IK of the service domain for which the most recent security mode negotiation took place. This may require that the integrity key of an (already integrity protected) ongoing signalling connection has to be changed, when a new connection is established with another service domain, or when a security mode negotiation follow a re-authentication during an ongoing connection. This change should be completed by the RNC within five seconds after receiving the security mode ~~negotiation~~command from the VLR/SGSN.

Note: For the behaviour of the terminal regarding key changes see section 6.4.5.

6.6.5 Cipher key selection

There is one CK for CS connections (CK_{CS}), established between the CS service domain and the user and one CK for PS connections (CK_{PS}) established between the PS service domain and the user.

The radio bearers for CS user data are ciphered with CK_{CS}.

The radio bearers for PS user data are ciphered with CK_{PS}.

The signalling radio bearers are used for transfer of signalling data for services delivered by both CS and PS service domains. These signalling radio bearers are ciphered by the CK of the service domain for which the most recent security mode negotiation took place. This may require that the cipher key of an (already ciphered) ongoing signalling connection has to be changed, when a new connection is established with another service domain, or when a security mode negotiation follows a re-authentication during an ongoing connection. This change should be completed by the RNC within five seconds after receiving the security mode ~~negotiation~~ command from the VLR/SGSN.

Note: For the behaviour of the terminal regarding key changes see section 6.4.5.

.

Proposal for compromise on IM domain security - for decision

Integrity (and confidentiality, if required) of SIP messages between the UE and the S-CSCF shall be provided in a hop-by-hop fashion.

The first hop extends between the UE and the P-CSCF,
security associations are user specific here and are established
via the IM AKA.

The second hop extends between the P-CSCF and the S-CSCF,
security associations are not user specific here and are established
via the Network Domain Security mechanisms.

The authentication is terminated in the home network.
It is ffs whether it is performed in the HSS or the S-CSCF.

It is ffs whether confidentiality of SIP messages is required on all hops.