CHANGE REQUEST No :	**A012**	*Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.*

Technical Specification GSM 22.00   Version: 3.1.0

Submitted to SMG		for approval	**X**	without presentation ("non-strategic")	
list SMG plenary meeting no. here ↑		for information		with presentation ("strategic")	**X**

PT SMG CR cover form is available from: http://docbox.etsi.org/tech-org/smg/Document/smg/tools/CR_form/crf28_1.zip

Proposed change affects: SIM ☐   ME **X**   Network **X**
(at least one should be marked with an X)

Work item: UMTS Release 99 Requirements

Source: Vodafone   **Date:** 8th March 1999

Subject: Security Requirements

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

Reason for change: Change of functional requirements to reflect views of SMG10

Clauses affected: 10

Other specs affected:	Other releases of same spec	☐	→ List of CRs:	
	Other core specifications	☐	→ List of CRs:	
	MS test specifications / TBRs	☐	→ 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.

10   Security Features

With respect to the GSM security mechanisms the following additional features may be implemented for UMTS Release 99phase 1 if required by SMG10 :

1) Mutual authentication between user and serving network, between user and home environment and between serving network and home environment;

2) Possibility for a user to verify that a serving network is authorized by the user's HE to offer services to that user;

32)Confidentiality of user and signalling data between MS and RNC to and within the access network (and possibly into the core network);

4) Integrity of critical signalling data between MS and RNC (and possibly into the core network);

5) Periodic in-call integrity protection of signalling data to prevent channel hijack.

3) End to end encryption (as an optional service) between UMTS users, with access to plaintext for lawful interception purposes

4) TTP (trusted 3rd party) mechanisms, including public key techniques and associated certificates and signing, verification and revocation procedures used, for example, before accessing 3rd party services.

5) Authentication, confidentiality and integrity of signalling between UMTS network (both core and access) nodes

6) Confidentiality of the user identity on the radio interface.