TSG-SA Working Group 1 (Services) meeting #2 TSGS1#2(99)185
Edinburgh, UK, 9th - 12th March 1999

CHANGE REQUEST No : **A013** *Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.*

Technical Specification GSM / UMTS: 22.00 Version 3.1.0

Submitted to SMG 1 *list plenary meeting or STC here ↑* for approval **X** for information; without presentation ("non-strategic") ; with presentation ("strategic")

PT SMG CR cover form. Filename: crf26_3.doc

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

Work item: Variable length of security parameters such as RAND and SRES

Source: S1 ~~FUJITSU~~ **Date:** 10 March, 1999

Subject: Flexible protocols for the support of various authentication algorithms

Category: *(one category and one release only 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	**X**		Release 97
C	Functional modification of feature			Release 98
D	Editorial modification			Release 99
				UMTS **X**

Reason for change: Highly secured system is regarded as one of main feature of UMTS. Required security level by each operator may be different therefore it is desirable to choose appropriate algorithm which meets the operator's security requirement. To prepare the emerging authentication algorithms, protocol shall have enough flexibility to support them.

Clauses affected: 10 Security Features

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 phase 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) Confidentiality of user and signalling data to and within the access network (and possibly into the core network)

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.

7) Flexible protocol to support various authentication algorithms.