**CHANGE REQUEST No:** A013

<table>
<thead>
<tr>
<th>Technical Specification GSM / UMTS:</th>
<th>22.00</th>
<th>Version: 3.1.0</th>
</tr>
</thead>
</table>

Submitted to SMG list plenary meeting or STC here ↑ for approval without presentation ("non-strategic")

<table>
<thead>
<tr>
<th>Proposed change affects:</th>
<th>SIM</th>
<th>ME</th>
<th>Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>(at least one should be marked with an X)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

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

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

**Subject:** Flexible protocols for the support of various authentication algorithms

**Category:**
- **F** Correction
- **A** Corresponds to a correction in an earlier release
- **B** Addition of feature
- **C** Functional modification of feature
- **D** Editorial modification

**Release:**
- **Phase 2** Release 96
- **Release 97** Release 97
- **Release 98** Release 98
- **Release 99** UMTS

**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

<table>
<thead>
<tr>
<th>Other specs affected:</th>
<th>Other releases of same spec</th>
<th>→ List of CRs:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other core specifications</td>
<td>→ List of CRs:</td>
<td></td>
</tr>
<tr>
<td>MS test specifications / TBRs</td>
<td>→ List of CRs:</td>
<td></td>
</tr>
<tr>
<td>BSS test specifications</td>
<td>→ List of CRs:</td>
<td></td>
</tr>
<tr>
<td>O&amp;M specifications</td>
<td>→ List of CRs:</td>
<td></td>
</tr>
</tbody>
</table>

**Other comments:**

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.