# 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 | **0xx** | Current Version: | 3.5.0 |

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

| For submission to: | SA#9 | for approval | **X** | strategic | | *(for SMG* |
| *list expected approval meeting # here* ↑ | | for information | | non-strategic | | *use only)* |

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

| **Source:** | Vodafone | | **Date:** | 4 September 2000 |

| **Subject:** | Removal of secure authentication mechanism negotiation. |

| **Work item:** | Security |

| **Category:** | F | Correction | **X** | **Release:** | Phase 2 | |
| | A | Corresponds to a correction in an earlier release | | | Release 96 | |
| *(only one category* | B | Addition of feature | | | Release 97 | |
| *shall be marked* | C | Functional modification of feature | | | Release 98 | |
| *with an X)* | D | Editorial modification | | | Release 99 | **X** |
| | | | | | Release 00 | |

| **Reason for change:** | Secure authentication mechanism negotiation is not provided in the R99 specifications so it is deleted from 33.102. |

| **Clauses affected:** | 5.1.2 |

| **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.

## 5.1.2 Entity authentication

The following security features related to entity authentication are provided:

- **authentication mechanism agreement:** the property that the user and the serving network can securely negotiate the mechanism for authentication and key agreement that they shall use subsequently;

- **user authentication:** the property that the serving network corroborates the user identity of the user;

- **network authentication:** the property that the user corroborates that he is connected to a serving network that is authorised by the user's HE to provide him services; this includes the guarantee that this authorisation is recent.

To achieve these objectives, it is assumed that entity authentication should occur at each connection set-up between the user and the network. Two mechanisms have been included: an authentication mechanism using an authentication vector delivered by the user's HE to the serving network, and a local authentication mechanism using the integrity key established between the user and serving network during the previous execution of the authentication and key establishment procedure.

Clause 6.3 describes an authentication and key establishment mechanism that achieves the security features listed above and in addition establishes a secret cipher key (see 5.1.3) and integrity key (see 5.1.4) between the user and the serving network. This mechanism should be invoked by the serving network after a first registration of a user in a serving network and after a service request, location update request, attach request, detach request or connection re-establishment request, when the maximum number of local authentications using the derived integrity key have been conducted.

Clause 6.5 describes the local authentication mechanism. The local authentication mechanism achieves the security features user authentication and network authentication and uses an integrity key established between user and serving network during the previous execution of the authentication and key establishment procedure. This mechanism should be invoked by the serving network after a service request, location update request, attach request, detach request or connection re-establishment request, provided that the maximum number of local authentications using the same derived integrity key has not been reached yet.