CR-Form-v3

CHANGE REQUEST

| ⌘ **33.105** | **CR** **CR-Num** | ⌘ rev | **-** | ⌘ | Current version: | **3.6.0** | ⌘ |

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM **X** ME/UE **X** Radio Access Network ☐ Core Network ☐

Title: ⌘	Minimum clock frequency updated	
Source: ⌘	SA3	
Work item code: ⌘	Security	***Date:*** ⌘ 1/3/2001
Category: ⌘	**F**	***Release:*** ⌘ R99

Use one of the following categories:
F (essential correction)
A (corresponds to a correction in an earlier release)
B (Addition of feature),
C (Functional modification of feature)
D (Editorial modification)
Detailed explanations of the above categories can
be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change: ⌘	Advise from T3 is taken into account
Summary of change: ⌘	Minimum clock frequency used by the terminal during USIM sessions is updated from 3.25 MHz to 3 MHz
Consequences if not approved: ⌘	The requirements for authentication algorithm are a bit too loose.

Clauses affected: ⌘	5.1.5

Other specs affected: ⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments: ⌘	

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at: http://www.3gpp.org/3G_Specs/CRs.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://www.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2000-09 contains the specifications resulting from the September 2000 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

5.1.5   Implementation and operational considerations

The functions f1—f5, f1* and f5* shall be designed so that they can be implemented on an IC card equipped with a 8-bit microprocessor running at 3.25 MHz with 8 kbyte ROM and 300byte RAM and produce AK, XMAC-A, RES, CK and IK in less than 500 ms execution time.