

CHANGE REQUEST

⌘ **33.102** CR **CRNum** ⌘ rev **-** ⌘ Current version: **3.b.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 ME/UE Radio Access Network Core Network

Title:	⌘ Correction of (U)SIM toolkit security reference				
Source:	⌘ Vodafone				
Work item code:	⌘ Security	Date:	⌘ 10 May 2002		
Category:	⌘ F	Release:	⌘ REL-4		
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:		
	F (correction)		2 (GSM Phase 2)		
	A (corresponds to a correction in an earlier release)		R96 (Release 1996)		
	B (addition of feature),		R97 (Release 1997)		
	C (functional modification of feature)		R98 (Release 1998)		
	D (editorial modification)		R99 (Release 1999)		
	Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		REL-4 (Release 4)		
			REL-5 (Release 5)		

Reason for change:	⌘ The reference to 02.48 is wrong since 02.48 does not exist in Rel-4. TS 22.048 replaces GSM 02.48 from Rel-4 onwards.
Summary of change:	⌘ The reference to 02.48 is replaced with a reference to 22.048.
Consequences if not approved:	⌘ Incorrect reference.

Clauses affected:	⌘ 2, 5.4.1
Other specs affected:	⌘ <input type="checkbox"/> Other core specifications ⌘ <input type="checkbox"/>
	<input type="checkbox"/> Test specifications ⌘ <input type="checkbox"/>
	<input type="checkbox"/> O&M Specifications ⌘ <input type="checkbox"/>
Other comments:	⌘ <input type="text"/>

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.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://ftp.3gpp.org/specs/](http://ftp.3gpp.org/specs/). For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 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.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

- [1] 3GPP TS 21.133: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Threats and Requirements".
- [2] 3GPP TS 33.120: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Principles and Objectives".
- [3] 3GPP TR 21.905: "3rd Generation Partnership Project (3GPP); Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications (Release 1999)".
- [4] 3GPP TS 23.121: "3rd Generation Partnership Project (3GPP); Technical Specification Group Services and System Aspects; Architecture Requirements for Release 99".
- [5] 3GPP TS 31.101: "3rd Generation Partnership Project (3GPP); Technical Specification Group Terminals; UICC-terminal interface; Physical and logical characteristics".
- [6] 3GPP TS 22.022: "3rd Generation Partnership Project (3GPP); Technical Specification Group Services and System Aspects; Personalisation of UMTS Mobile Equipment (ME); Mobile functionality specification".
- [7] 3GPP Ts 23.048: "3rd Generation Partnership Project (3GPP); Technical Specification Group Services and System Aspects; Security Mechanisms for the USIM application toolkit; Stage 2".
- [8] ETSI GSM 03.20: "Digital cellular telecommunications system (Phase 2+); Security related network functions".
- [9] 3GPP TS 23.060: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 2".
- [10] ISO/IEC 9798-4: "Information technology - Security techniques - Entity authentication - Part 4: Mechanisms using a cryptographic check function".
- [11] 3GPP TS 35.201: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications".
- [12] 3GPP TS 35.202: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification".
- [13] 3GPP TS 35.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementers' test data".
- [14] 3GPP TS 35.204: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data".

- [15] 3GPP TS 31.111: "3rd Generation Partnership Project; Technical Specification Group Terminals; USIM Application Toolkit (USAT)".
- [16] 3GPP TS ~~202.0~~48: "Security Mechanisms for the SIM Application Toolkit; Stage 1".
- [17] 3GPP TS 25.331: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; RRC Protocol Specification".
- [18] 3GPP TS 25.321: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; MAC protocol specification".
- [19] 3GPP TS 25.322: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; RLC Protocol Specification".
- [20] 3GPP TS 31.102: "3rd Generation Partnership Project (3GPP); Technical Specification Group Terminals; Characteristics of the USIM Application".
- [21] 3GPP TS 22.101: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service aspects; Service principles".

*** NEXT MODIFICATION ***

5.4.1 Secure messaging between the USIM and the network

USIM Application Toolkit, as specified in 3G TS 31.111 [15], provides the capability for operators or third party providers to create applications which are resident on the USIM (similar to SIM Application Toolkit in GSM). There exists a need to secure messages which are transferred over the network to applications on the USIM, with the level of security chosen by the network operator or the application provider.

Security features for USIM Application Toolkit are implemented by means of the mechanisms described in TS 23.048 [7]. These mechanisms address the security requirements identified in ~~GSM-TS 022.0~~48 [16].