

CHANGE REQUEST

⌘ **33.102** CR **142** ⌘ rev **1** ⌘ Current version: **3.7.0** ⌘

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:	⌘ Definition corrections		
Source:	⌘ SA WG3		
Work item code:	⌘ Security	Date:	⌘ 21/2/2001
Category:	⌘ F	Release:	⌘ R99
<i>Use <u>one</u> of the following categories:</i>		<i>Use <u>one</u> of the following releases:</i>	
F (essential 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:	⌘ Definitions corrections
Summary of change:	⌘ Only changes to definitions and references sections
Consequences if not approved:	⌘ Possible incorrect interpretation of terms used in TS 33.102. Definition of R98- and R99+ was requested by SA#09.

Clauses affected:	⌘ 2; 3.1
Other specs Affected:	⌘ <input type="checkbox"/> Other core specifications ⌘ <input type="checkbox"/>
	<input type="checkbox"/> Test specifications
	<input type="checkbox"/> O&M Specifications
Other comments:	⌘

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 02.48: "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 22.101: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service aspects; Service principles".

3 Definitions, symbols and abbreviations

3.1 Definitions

In addition to the definitions included in TR 21.905 [3] and TS 22.101[20], for the purposes of the present document, the following definitions apply:

NOTE: 'User' and 'Subscriber' have been defined in TR 21.905[3]. 'User Equipment', 'USIM', 'SIM' and IC Card' have been defined in TS 22.201[20]

Confidentiality: The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Data integrity: The property that data has not been altered in an unauthorised manner.

Data origin authentication: The corroboration that the source of data received is as claimed.

Entity authentication: The provision of assurance of the claimed identity of an entity.

Key freshness: A key is fresh if it can be guaranteed to be new, as opposed to an old key being reused through actions of either an adversary or authorised party.

~~**USIM—User Services Identity Module.** In a security context, this module is responsible for performing UMTS subscriber and network authentication and key agreement. It should also be capable of performing GSM authentication and key agreement to enable the subscriber to roam easily into a GSM Radio Access Network.~~

~~**SIM— GSM Subscriber Identity Module.** In a security context, this module is responsible for performing GSM subscriber authentication and key agreement. This module is **not** capable of handling UMTS authentication nor storing UMTS style keys.~~

UMTS Entity authentication and key agreement: Entity authentication according to this specification.

GSM Entity authentication and key agreement: The entity Authentication and Key Agreement procedure to provide authentication of a SIM to a serving network domain and to generate the key Kc in accordance to the mechanisms specified in TS ETSI GSM 03.20.

~~Entity authentication according to TS ETSI GSM 03.20~~

User access module: either a USIM or a SIM

Mobile station, user: the combination of user equipment and a user access module.

User: Within the context of this specification a user is either a UMTS subscriber (Section 6.8.1) or a GSM Subscriber (Section 6.8.2) or a physical person as defined in TR 21.905[3] (Section 5.3 and 5.5)

UMTS subscriber: a Mobile Equipment with a UICC inserted and activated USIM-application.

GSM subscriber: a Mobile Equipment with a SIM inserted or a Mobile Equipment with a UICC inserted and activated SIM-application.

~~**UMTS subscriber:** a mobile station that consists of user equipment with a USIM inserted.~~

~~**GSM subscriber:** a mobile station that consists of user equipment with a SIM inserted.~~

UMTS security context: a state that is established between a user and a serving network domain as a result of the execution of UMTS AKA. At both ends "UMTS security context data" is stored, that consists at least of the UMTS cipher/integrity keys CK and IK and the key set identifier KSI. One is still in a UMTS security context, if the keys CK/IK are converted into Kc to work with a GSM BSS.

GSM security context: a state that is established between a user and a serving network domain usually as a result of the execution of GSM AKA. At both ends "GSM security context data" is stored, that consists at least of the GSM cipher key Kc and the cipher key sequence number CKSN.

Quintet, UMTS authentication vector: temporary authentication and key agreement data that enables an VLR/SGSN to engage in UMTS AKA with a particular user. A quintet consists of five elements: a) a network challenge RAND, b) an expected user response XRES, c) a cipher key CK, d) an integrity key IK and e) a network authentication token AUTN.

Triplet, GSM authentication vector: temporary authentication and key agreement data that enables an VLR/SGSN to engage in GSM AKA with a particular user. A triplet consists of three elements: a) a network challenge RAND, b) an expected user response SRES and c) a cipher key Kc.

Authentication vector: either a quintet or a triplet.

Temporary authentication data: either UMTS or GSM security context data or UMTS or GSM authentication vectors.

R98-: Refers to a network node or ME that conforms to R97 or R98 specifications.

R99+: Refers to a network node or ME that conforms to R99 or later specifications.