

Source : S1
To : S3
cc : SMG1
Title : LS on security requirements for UMTS Phase 1 Release 99

The specification UMTS 22.100 addresses the UMTS Phase 1 capabilities for RELEASE 99. The section 11 of this specification deals with security requirements.

S1 would like to remind that it is extremely important to clarify now all the capability requirements for Release 99 in order to leave time enough to other WGs to complete the specifications before the end of this year.

S3 has been mandated to define security requirements for UMTS. S1 wants to inform S3 that it has modified the section 11 of TS 22.100 and that the new text content only makes reference to the UMTS 21.133 specification (see attached proposed CR). However, S1 has been aware that S3 has not yet clarified the requirements for Release 99 and then would like to remind S3 that it is very important to clarify them as soon as possible.

S1 would like to receive an answer to this LS from S3 clarifying if UMTS 21.133 is the appropriate specification dealing with security requirements on UMTS Release 99 and would like to be informed of the security requirements for Release 99 once defined.

TSG-SA Working Group 1 (Services) meeting #3
 Hampton Court, Surrey, UK 10th-12th May 1999
 TSG_SA_WG1
 Edinburgh
 Agenda: 9.0.6
 8-12 March 1999

TSGS1#3(99)366
 Agenda: 6.1.4
S1-99 148

CHANGE REQUEST No : <input type="text"/>		<i>Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.</i>
Technical Specification GSM	<input type="text" value="22.100"/>	Version: <input type="text" value="3.3.0"/>
Submitted to TSG #4 <input type="text"/>	for approval <input checked="" type="checkbox"/>	without presentation ("non-strategic") <input type="checkbox"/>
SA <input type="text"/>	for information <input type="checkbox"/>	with presentation ("strategic") <input checked="" type="checkbox"/>
<small>list SMG plenary meeting no. here ↑</small>		
<small>PT SMG CR cover form is available from: http://docbox.etsi.org/tech-org/smg/Document/smg/tools/CR_form/crf28_1.zip</small>		

Proposed change affects: SIM ME Network
(at least one should be marked with an X)

Work item: UMTS Release 99 Requirements

Source: Rapporteur of 22.100 **Date:** 12th March 1999

Subject: Rewriting of section 11 about security requirements.
 Adding of reference to S3 specifications for security requirements for REL99.

Category:	F Correction	<input type="checkbox"/>	Release:	Phase 2	<input type="checkbox"/>
<small>(one category and one release only shall be marked with an X)</small>	A Corresponds to a correction in an earlier release	<input type="checkbox"/>		Release 96	<input type="checkbox"/>
	B Addition of feature	<input type="checkbox"/>		Release 97	<input type="checkbox"/>
	C Functional modification of feature	<input checked="" type="checkbox"/>		Release 98	<input type="checkbox"/>
	D Editorial modification	<input type="checkbox"/>		Release 99	<input checked="" type="checkbox"/>

Reason for change: To align the specification with the fact that S3 defines security requirements for UMTS Phase 1 Release 99.

Clauses affected: section 11

Other specs affected:	Other releases of same spec	<input type="checkbox"/>	→ List of CRs:	<input type="text"/>
	Other core specifications	<input type="checkbox"/>	→ List of CRs:	<input type="text"/>
	MS test specifications / TBRs	<input type="checkbox"/>	→ List of CRs:	<input type="text"/>
	BSS test specifications	<input type="checkbox"/>	→ List of CRs:	<input type="text"/>
	O&M specifications	<input type="checkbox"/>	→ List of CRs:	<input type="text"/>

Other comments:



<----- double-click here for help and instructions on how to create a CR.

1 Scope

The UMTS system will be defined in a phased approach. This document specifies the content of the first phase of requirements for UMTS. Some requirements affecting phase 1 to ensure a smooth transition to later releases are also indicated.

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.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

2.1 Normative references

This document is the starting point of the set of specifications that define the UMTS Service Requirements for UMTS Phase 1. The UMTS Service requirements for UMTS phase 1 are defined in the following normative specifications.

- [1] UMTS 22.01: "Universal Mobile Telecommunications System (UMTS): Service aspects; Service principles".
- [2] UMTS 22.05: "Universal Mobile Telecommunications System (UMTS); Services and Service Capabilities".
- [3] UMTS 22.15: "Universal Mobile Telecommunications System (UMTS); Service Aspects: Charging and Billing".
- [4] UMTS 22.20: "Universal Mobile Telecommunications System (UMTS); VHE Stage 1".
- [5] [UMTS TS ??, Handover requirements between UMTS and GSM or other Radio System]".
- [6] [UMTS 21.133 : "Universal Mobile Telecommunications System \(UMTS\) ; Security threats and requirements"](#)

These specifications may refer (directly or indirectly) to further specifications which provide detailed descriptions of service requirements incorporated in UMTS. In particular the service requirements of any GSM component of a UMTS system are specified by reference to GSM service requirements specifications.

11 Security Features

~~With respect to the GSM security mechanisms the following additional features may be implemented for UMTS phase 1 if required by SMG10: Security requirements for UMTS Phase 1 Release 99 are defined in the UMTS 21.133 specification [6].~~

- ~~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.~~