
Source: SA WG3

Title: 2 CR to 21.133: Definition of UICC (Rel-99 and Rel-4)

Document for: Approval

Agenda Item: 7.3.3

Spec	CR	Rev	Phase	Cat	Subject	Version-Current	Version-New	Doc-2nd-Level
21.133	002		Rel-99	F	Definition of UICC	3.1.0	3.2.0	S3-010558
21.133	003		Rel-4	A	Definition of UICC	3.1.0	3.2.0	S3-010559

CHANGE REQUEST

⌘ **21.133 CR 002** ⌘ ev **-** ⌘ Current version: **3.1.0** ⌘

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 of UICC				
Source:	⌘ SA WG3				
Work item code:	⌘ Security	Date:	⌘ 19 October 2001		
Category:	⌘ F	Release:	⌘ R99		
	Use <u>one</u> of the following categories: F (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 <u>one</u> 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:	⌘ To make sure that the abbreviation UICC is the same as in the 3G Vocabulary to avoid misunderstandings.
Summary of change:	⌘ 2 TR 21.905 added 3.2 UICC = Universal Integrated Circuit Card and not UMTS Integrated Circuit Card 5.1.5 Reference to TR 21.905 3G Vocabulary 5.3 Removal of definition of UICC
Consequences if not approved:	⌘ Inconsequent definitions of UICC leading to misunderstandings.

Clauses affected:	⌘ 2, 3.2, 5.1.5, and 5.3
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.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] 3G TS 33.120: "3G Security; Security Principles and Objectives".

[2] 3G TS 33.102: "3G Security; Security Architecture".

Baseline documents:

3GPP s3-99003: UMTS 33.21, version 2.0.0: "Security requirements".

3GPP s3-99016: ARIB, Requirements and Objectives for 3G Mobile Services and System, Annex 8 - Security Design Principles.

ETSI SMG10 99C019: Countermeasures to active attacks on the radio access link.

[3] ETSI ETR 332: "Security Techniques Advisory Group; Security requirements capture".

[4] ETSI ETR 331: "Definition of user Requirements for lawful interception of telecommunications; Requirements of the law enforcement agencies".

[5] ISO 7498-2: "Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture".

[6] ISO/IEC 10181-2: "Information Technology - Open Systems Interconnection - Security Frameworks in Open Systems".

[7] ISO/IEC 11770-1: "Information Technology – Security Techniques – Key Management, Part 1: Key Management Framework".

[8] UMTS 22.00: "Universal Mobile Telecommunications System (UMTS): UMTS Phase 1".

[9] UMTS 22.01: "Universal Mobile Telecommunications System (UMTS): Service aspects; service principles".

[10] UMTS 22.21: "Universal Mobile Telecommunications System (UMTS): Virtual Home Environment".

[11] UMTS 23.01: "Universal Mobile Telecommunications System (UMTS): General UMTS Architecture".

[12] UMTS 30.01: "Universal Mobile Telecommunications System (UMTS): UMTS Baseline Document; Positions on UMTS agreed by SMG".

[13] UMTS 33.20: "Universal Mobile Telecommunications System (UMTS): Security Principles".

[14] 3G TR 21.905 "3G Vocabulary for 3GPP Specifications"

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

GSM	Global System for Mobile communications
HE	Home Environment
IMEI	International Mobile Equipment Identity
IMT-2000	International Mobile Telecommunications-2000
IMUI	International Mobile User Identity
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ITU	International Telecommunications Union
N-ISDN	Narrowband ISDN
PIN	Personal Identification Number
PSTN	Public Switched Telephone Network
SIM	Subscriber Identity Module
SN	Serving Network
TD-CDMA	Time Division - Code Division Multiple Access
TMN	Telecommunications Management Network
UICC	UMTS-Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunication System
UPT	Universal Personal Telecommunication
USIM	User Services Identity Module
UTRAN	UMTS Terrestrial Radio Access Network
VHE	Virtual Home Environment
W-CDMA	Wideband - Code Division Multiple Access

5.1.5 Security management

- a) 3G security shall be based on the use of a physically secure device ~~called a~~, i.e. a-UICC as defined in [14], that can be inserted and removed from terminal equipment. ~~The~~ This UICC shall contain one or more applications at least one of which must be a USIM.
- b) A USIM contained in a UICC shall be used to represent and identify a user and his association with a home environment in the provision of 3G services.
- c) The USIM shall be developed on the basis of the phase 2+ GSM SIM. [8]
- d) 3G terminal equipment shall support GSM phase 2 and phase 2+ SIMs as access modules to 3G networks. This will result in security being limited in extent and quality to GSM level. For this reason 3G operators shall be able to decide whether or not to accept GSM SIMs as access modules to 3G services. [8]
- e) Simultaneous activation of multiple USIMs on one terminal equipment is not required in 3G phase 1. [8]

5.3 3G architecture

In this subclause various architectural components of the 3G system that have an impact on the design of 3G security features are listed.

User Services Identity Module (USIM): an application that represents and identifies a user and his association with a home environment in the provision of 3G services. The USIM contains functions and data needed to identify and authenticate users when 3G services are accessed. It may also contain a copy of the user's service profile. It may also provide other security features. The USIM contains the user's IMUI and any security parameters which need to be carried by the user. The USIM is always implemented in a removable IC card called the UICC.

~~**UMTS Integrated Circuit Card (UICC):** a physically secure device that can be inserted and removed from terminal equipment. It can contain one or more applications one of which must be the USIM.~~

CHANGE REQUEST

⌘ **21.133 CR 003** ⌘ ev **-** ⌘ Current version: **4.0.0** ⌘

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 of UICC		
Source:	⌘ SA WG3		
Work item code:	⌘ SEC1	Date:	⌘ 19 October 2001
Category:	⌘ A	Release:	⌘ REL-4
	Use <u>one</u> of the following categories: F (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 <u>one</u> 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:	⌘ To make sure that the abbreviation UICC is the same as in the 3G Vocabulary to avoid misunderstandings.
Summary of change:	⌘ 2 TR 21.905 added 3.2 UICC = Universal Integrated Circuit Card and not UMTS Integrated Circuit Card 5.1.5 Reference to TR 21.905 3G Vocabulary 5.3 Removal of definition of UICC
Consequences if not approved:	⌘ Inconsequent definitions of UICC leading to misunderstandings.

Clauses affected:	⌘ 2, 3.2, 5.1.5, and 5.3		
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.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] 3G TS 33.120: "3G Security; Security Principles and Objectives".

[2] 3G TS 33.102: "3G Security; Security Architecture".

Baseline documents:

3GPP s3-99003: UMTS 33.21, version 2.0.0: "Security requirements".

3GPP s3-99016: ARIB, Requirements and Objectives for 3G Mobile Services and System, Annex 8 - Security Design Principles.

ETSI SMG10 99C019: Countermeasures to active attacks on the radio access link.

[3] ETSI ETR 332: "Security Techniques Advisory Group; Security requirements capture".

[4] ETSI ETR 331: "Definition of user Requirements for lawful interception of telecommunications; Requirements of the law enforcement agencies".

[5] ISO 7498-2: "Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture".

[6] ISO/IEC 10181-2: "Information Technology - Open Systems Interconnection - Security Frameworks in Open Systems".

[7] ISO/IEC 11770-1: "Information Technology – Security Techniques – Key Management, Part 1: Key Management Framework".

[8] UMTS 22.00: "Universal Mobile Telecommunications System (UMTS): UMTS Phase 1".

[9] UMTS 22.01: "Universal Mobile Telecommunications System (UMTS): Service aspects; service principles".

[10] UMTS 22.21: "Universal Mobile Telecommunications System (UMTS): Virtual Home Environment".

[11] UMTS 23.01: "Universal Mobile Telecommunications System (UMTS): General UMTS Architecture".

[12] UMTS 30.01: "Universal Mobile Telecommunications System (UMTS): UMTS Baseline Document; Positions on UMTS agreed by SMG".

[13] UMTS 33.20: "Universal Mobile Telecommunications System (UMTS): Security Principles".

[14] 3G TR 21.905 "3G Vocabulary for 3GPP Specifications"

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

GSM	Global System for Mobile communications
HE	Home Environment
IMEI	International Mobile Equipment Identity
IMT-2000	International Mobile Telecommunications-2000
IMUI	International Mobile User Identity
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ITU	International Telecommunications Union
N-ISDN	Narrowband ISDN
PIN	Personal Identification Number
PSTN	Public Switched Telephone Network
SIM	Subscriber Identity Module
SN	Serving Network
TD-CDMA	Time Division - Code Division Multiple Access
TMN	Telecommunications Management Network
UICC	UMTS-Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunication System
UPT	Universal Personal Telecommunication
USIM	User Services Identity Module
UTRAN	UMTS Terrestrial Radio Access Network
VHE	Virtual Home Environment
W-CDMA	Wideband - Code Division Multiple Access

5.1.5 Security management

- a) 3G security shall be based on the use of a physically secure device ~~called a~~, i.e. a-UICC as defined in [14], that can be inserted and removed from terminal equipment. ~~The~~ This UICC shall contain one or more applications at least one of which must be a USIM.
- b) A USIM contained in a UICC shall be used to represent and identify a user and his association with a home environment in the provision of 3G services.
- c) The USIM shall be developed on the basis of the phase 2+ GSM SIM. [8]
- d) 3G terminal equipment shall support GSM phase 2 and phase 2+ SIMs as access modules to 3G networks. This will result in security being limited in extent and quality to GSM level. For this reason 3G operators shall be able to decide whether or not to accept GSM SIMs as access modules to 3G services. [8]
- e) Simultaneous activation of multiple USIMs on one terminal equipment is not required in 3G phase 1. [8]

5.3 3G architecture

In this subclause various architectural components of the 3G system that have an impact on the design of 3G security features are listed.

User Services Identity Module (USIM): an application that represents and identifies a user and his association with a home environment in the provision of 3G services. The USIM contains functions and data needed to identify and authenticate users when 3G services are accessed. It may also contain a copy of the user's service profile. It may also provide other security features. The USIM contains the user's IMUI and any security parameters which need to be carried by the user. The USIM is always implemented in a removable IC card called the UICC.

~~**UMTS Integrated Circuit Card (UICC):** a physically secure device that can be inserted and removed from terminal equipment. It can contain one or more applications one of which must be the USIM.~~