

Source: TSG-T3
Title: Change Requests to TS 31.103 "ISIM"
Document for: Approval

This document contains several change requests as follows:

Doc-1st-Level	Spec	CR	Phase	Subject	Cat	Vers. old	Vers. new	Doc-2nd-Level
TP-020281	31.103	002	Rel-5	Replace TS 31.110 by ETSI TS 101 220	F	5.1.0	5.2.0	T3-020896
TP-020281	31.103	003	Rel-5	Management of Last Selected ISIM	F	5.1.0	5.2.0	T3-020915
TP-020281	31.103	004	Rel-6	Move all 3GPP-specific card platform requirements to TS 31.101, and remove them from 31.103.	D	5.1.0	6.0.0	T3-020911

CR-Form-v7
CHANGE REQUEST
⌘ 31.103 CR 002 ⌘ rev - ⌘ Current version: 5.1.0 ⌘

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

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ Replace TS 31.110 by ETSI TS 101 220		
Source:	⌘ T3		
Work item code:	⌘ TEI	Date:	⌘ 06/11/2002
Category:	⌘ F	Release:	⌘ REL-5
	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 <u>TR 21.900</u> .		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) Rel-6 (Release 6)

Reason for change:	⌘ 3GPP TS 31.110 does not exist. Replace it by ETSI TS 101 220		
Summary of change:	⌘ Change of the reference		
Consequences if not approved:	⌘ Reference to a non existing specification		

Clauses affected:	⌘ 2, 3.1								
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="width: 20px; text-align: center;"> </td> <td style="width: 20px; text-align: center;"> </td> </tr> <tr> <td style="width: 20px; text-align: center;"> </td> <td style="width: 20px; text-align: center;"> </td> </tr> </table> Other core specifications ⌘ Test specifications ⌘ O&M Specifications ⌘	Y	N						
Y	N								
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/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/> 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 that, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) 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 21.111: "USIM and IC Card Requirements".
- [2] 3GPP TS 31.102: "Characteristics of the USIM Application".
- [3] 3GPP TS 31.101: "UICC-Terminal Interface, Physical and Logical Characteristics".
- [4] 3GPP TS 33.102: "3G Security; Security Architecture".
- [5] 3GPP TS 33.103: "3G Security; Integration Guidelines".
- [6] ISO/IEC 7816-4 (1995): "Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 4: Interindustry commands for interchange".
- [7] ISO/IEC 7816-5 (1994): "Identification cards - Integrated circuit(s) cards with contacts - Part 5: Numbering system and registration procedure for application identifiers".
- [8] ITU-T Recommendation T.50: "International Reference Alphabet (IRA) (Formerly International Alphabet No. 5 or IA5) - Information technology - 7-bit coded character set for information interchange
- [8a] ISO 646 (1983): "Information processing - ISO 7-bits coded characters set for information interchange".
- [9] 3GPP TS 23.003: "Numbering, Addressing and Identification".
- [10] ISO/IEC 7816-9 (2000): "Identification cards - Integrated circuit(s) cards with contacts - Part 9: Additional interindustry commands and security attributes".
- [11] ISO/IEC 7816-6 (1996): "Identification cards - Integrated circuit(s) cards with contacts - Part 6: Interindustry data elements".
- [12] 3GPP TS 25.101: "UE Radio Transmission and Reception (FDD)".
- [13] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".
- [14] 3GPP TS 33.203: "3G security; Access security for IP-based services".
- [15] 3GPP TS 24.228: "Signalling flows for the IP multimedia call control based on SIP and SDP; Stage 3".
- [16] IETF RFC 3261: "SIP: Session Initiation Protocol".
- [17] 3GPP TS 23.038: "Alphabets and language-specific information".
- [18] ISO 639 (1988): "Code for the representation of names of languages".
- [19] 3GPP TS 51.011: "Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface".
- [20] ISO/IEC 8825(1990): "Information technology - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)" Second Edition.

- [21] 3GPP TS 22.101: "Service aspects; Service principles".
- [22] ETSI TS 102 223: "Smart cards; Card Application Toolkit (CAT)".
- [23] ~~3GPP TS 31.110: "Numbering system for telecommunication IC card applications"~~ ETSI TS 101 220: "Smart cards; ETSI numbering system for telecommunication application providers".

3 Definitions, symbols, abbreviations and coding conventions

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

ISIM: application residing on the UICC, an IC card specified in 3GPP TS 31.101 [3]

In particular, 3GPP TS 31.101 [3] specifies the application independent properties of the UICC/terminal interface such as the physical characteristics and the logical structure

The AID of ISIM is defined in ~~3GPP TS 31.110~~ ETSI TS 101 220 [23] and is stored in EF_{DIR}.

ADM: access condition to an EF which is under the control of the authority which creates this file

CR-Form-v7

CHANGE REQUEST

⌘ **31.103 CR 003** ⌘ rev **-** ⌘ Current version: **5.1.0** ⌘

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

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ Management of Last Selected ISIM				
Source:	⌘ TSG T3				
Work item code:	⌘ TEI	Date:	⌘ 07/11/2002		
Category:	⌘ F	Release:	⌘ Rel-5		
	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)	
			Rel-6	(Release 6)	

Reason for change:	⌘	The selection by partial AID applies to the ISIM. The according behaviour has to be described.
Summary of change:	⌘	Addition of a section describing the the storage of the last selected ISIM application on the UICC.
Consequences if not approved:	⌘	Missing description for the use of Select by partial AID

Clauses affected:	⌘	5.1.1.1										
Other specs affected:	⌘	<table border="1" style="display: inline-table; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20px;">Y</td> <td style="width: 20px;">N</td> </tr> <tr> <td style="width: 20px;"> </td> <td style="width: 20px;">X</td> </tr> <tr> <td style="width: 20px;"> </td> <td style="width: 20px;">X</td> </tr> <tr> <td style="width: 20px;"> </td> <td style="width: 20px;">X</td> </tr> </table>	Y	N		X		X		X	Other core specifications	⌘
		Y	N									
			X									
	X											
	X											
		Test specifications										
		O&M Specifications										
Other comments:	⌘											

5.1 ISIM management procedures

5.1.1 Initialisation

5.1.1.1 ISIM application selection

If the Terminal wants to engage in IMS operation, then after UICC activation (see 3GPP TS 31.101 [3]), the Terminal shall select an ISIM application, if an ISIM application is listed in the EF_{DIR} file, using the SELECT by DF name as defined in 3GPP TS 31.101.

After a successful ISIM application selection, the selected ISIM (AID) is stored on the UICC. This application is referred to as the last selected ISIM application. The last selected ISIM application shall be available on the UICC after a deactivation followed by an activation of the UICC.

If a ISIM application is selected using partial DF name, the partial DF name supplied in the command shall uniquely identify a ISIM application. Furthermore if a ISIM application is selected using a partial DF name as specified in TS 31.101 [3] indicating in the SELECT command the last occurrence the UICC shall select the ISIM application stored as the last ISIM application. If, in the SELECT command, the options first, next/previous are indicated, they have no meaning if an application has not been previously selected in the same session and shall return an appropriate error code.

Introduction

~~The present document defines the IM Services Identity Module (ISIM) application.~~

The present document defines the IM Services Identity Module (ISIM) application. This application resides on the UICC, an IC card specified in TS 31.101 [3]. In particular, TS 31.101 [3] specifies the application independent properties of the UICC/terminal interface such as the physical characteristics and the logical structure.

TS 31.101 [3] is one of the core documents for this specification and is therefore referenced in many places in the present document.

2 References

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

- References are either specific (identified by date of publication and/or edition number or version number) 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 21.111: "USIM and IC Card Requirements".
- [2] 3GPP TS 31.102: "Characteristics of the USIM Application".
- [3] 3GPP TS 31.101: "UICC-Terminal Interface, Physical and Logical Characteristics".
- [4] 3GPP TS 33.102: "3G Security; Security Architecture".
- [5] 3GPP TS 33.103: "3G Security; Integration Guidelines".
- [6] ISO/IEC 7816-4 (1995): "Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 4: Interindustry commands for interchange".
- [7] ISO/IEC 7816-5 (1994): "Identification cards - Integrated circuit(s) cards with contacts - Part 5: Numbering system and registration procedure for application identifiers".
- [8] ~~void~~~~ITU-T Recommendation T.50: "International Reference Alphabet (IRA) (Formerly International Alphabet No. 5 or IA5) - Information technology - 7-bit coded character set for information interchange"~~
- ~~[8a] ISO 646 (1983): "Information processing - ISO 7 bits coded characters set for information interchange".~~
- [9] 3GPP TS 23.003: "Numbering, Addressing and Identification".
- [10] ISO/IEC 7816-9 (2000): "Identification cards - Integrated circuit(s) cards with contacts - Part 9: Additional interindustry commands and security attributes".
- [11] ISO/IEC 7816-6 (1996): "Identification cards - Integrated circuit(s) cards with contacts - Part 6: Interindustry data elements".
- [12] 3GPP TS 25.101: "UE Radio Transmission and Reception (FDD)".
- [13] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".
- [14] 3GPP TS 33.203: "3G security; Access security for IP-based services".

- [15] 3GPP TS 24.228: "Signalling flows for the IP multimedia call control based on SIP and SDP; Stage 3".
- [16] IETF RFC 3261: "SIP: Session Initiation Protocol".
- [17] 3GPP TS 23.038: "Alphabets and language-specific information".
- [18] ISO 639 (1988): "Code for the representation of names of languages".
- [19] 3GPP TS 51.011: "Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface".
- [20] ISO/IEC 8825(1990): "Information technology - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)" Second Edition.
- [21] 3GPP TS 22.101: "Service aspects; Service principles".
- [22] ETSI TS 102 223: "Smart cards; Card Application Toolkit (CAT)".
- [23] 3GPP TS 31.110: "Numbering system for telecommunication IC card applications".

4 Files

This clause specifies the EFs for the IMS session defining access conditions, data items and coding. A data item is a part of an EF which represents a complete logical entity.

~~EFs or data items having an unassigned value, or, which during the IMS session, are cleared by the Terminal, shall have their bytes set to 'FF'. After the administrative phase all data items shall have a defined value or have their bytes set to 'FF'. If a data item is 'deleted' during a IMS session by the allocation of a value specified in another 3G TS, then this value shall be used and the data item is not unassigned.~~

~~EFs are mandatory (M) or optional (O). The file size of an optional EF may be zero. All implemented EFs with a file size greater than zero shall contain all mandatory data items. Optional data items may either be filled with 'F', or, if located at the end of an EF, need not exist.~~

~~When the coding is according to ITU T Recommendation T.50 [8], bit 8 of every byte shall be set to 0.~~

For an overview containing all files see figure 4.1.

4.1 Contents of the EFs at the MF level

There are four EFs at the Master File (MF) level. These EFs are specified in 3GPP TS 31.101 [3].

~~The file EF_{ARR} is mandatory for the ISIM.~~

5 Application protocol

~~When involved in administrative management operations, the ISIM interfaces with appropriate equipment. These operations are outside the scope of the present document.~~

~~When involved in IMS operations, the ISIM interfaces with a Terminal, with which messages are exchanged. A message can be a command or a response.~~

- ~~— An ISIM Application command/response pair is a sequence consisting of a command and the associated response.~~
- ~~— An ISIM Application procedure consists of one or more ISIM Application command/response pairs, which are used to perform all, or part of an application oriented task. A procedure shall be considered as a whole that is to say that the corresponding task is achieved if and only if the procedure is completed. The Terminal shall ensure that, when operated according to the manufacturer's manual, any unspecified interruption of the sequence of command/response pairs, which realise the procedure, leads to the abortion of the procedure itself.~~
- ~~— An ISIM session is the interval of time starting at the completion of the ISIM initialisation procedure and ending either with the start of the ISIM session termination procedure, or at the first instant the link between the UICC and the Terminal is interrupted.~~

~~During the IMS operation phase, the Terminal plays the role of the master and the ISIM plays the role of the slave.~~

~~The ISIM shall execute all commands and procedures in such a way as not to jeopardise, or cause suspension, of service provisioning to the user. This could occur if, for example, execution of the AUTHENTICATE is delayed in such a way which would result in the IMS denying or suspending service to the user.~~

[The requirements stated in the corresponding section of 3GPP TS 31.101 \[3\] apply to the ISIM application.](#)

The procedures listed in subclause "ISIM management procedures" are required for execution of the procedures in the subsequent subclauses "ISIM security related procedures" and "Subscription related procedures". The procedures listed in subclauses "ISIM security related procedures" are mandatory. The procedures listed in "Subscription related procedures" are only executable if the associated services, which are optional, are provided in the ISIM. However, if the procedures are implemented, it shall be in accordance with subclause "Subscription related procedures".

6 Security features

The security aspects of IMS are specified in 3GPP TS 33.203 [14]. This clause gives information related to security features supported by the ISIM ~~with respect to user verification and file access conditions, to enable the following:~~

- ~~— authentication of the ISIM to the network;~~
- ~~— authentication of the network to the ISIM;~~
- ~~— authentication of the user to the ISIM.~~

6.1 User verification and file access conditions

~~The ISIM application uses 2 PINs for user verification, PIN and PIN2. PIN2 is used only in the ADF. The PIN and PIN2 are mapped into key references as defined in 3GPP TS 31.101 [3]. Each key reference is associated with a usage qualifier as defined in ISO/IEC 7816-9 [10]. The PIN status is indicated in the PS_DO, which is part of the FCP response when an ADF/DF is selected. The coding of the PS_DO is defined in 3GPP TS 31.101 [3].~~

~~PIN and PIN2 are coded on 8 bytes. Only (decimal) digits (0-9) shall be used, coded in CCITT T.50 [8] with bit 8 set to zero. The minimum number of digits is 4. If the number of digits presented by the user is less than 8 then the Terminal shall pad the presented PIN with 'FF' before sending it to the ISIM.~~

~~The coding of the UNBLOCK PINs is identical to the coding of the PINs. However, the number of (decimal) digits is always 8.~~

The security architecture as defined in 3GPP TS 31.101 [3] applies to the ISIM and UICC with the following definitions and additions:

- The ISIM application shall use a global key reference as PIN1 as specified in 3GPP TS 31.101 [3].
- For access to DF_{TELECOM^{elecom}} the PIN shall be verified.
- The only valid usage qualifier is '08' which means user authentication knowledge based (PIN) as defined in ISO/IEC 7816-9 [10]. ~~The terminal shall support the multi-application capabilities as defined in 3GPP TS 31.101 [3].~~
- ~~— Every file in the ISIM application shall have a reference to an access rule stored in EF_{ARR}.~~
- ~~— The ISIM shall reside on a multi-verification/application capable UICC (from the security context point of view) and this UICC shall support the referenced format using SEID as defined in 3GPP TS 31.101 [3].~~
- ~~— The UICC on which the ISIM resides shall support the replacement of an ISIM application PIN with the Universal PIN as defined in 3GPP TS 31.101 [3]. Only the Universal PIN is allowed as a replacement.~~

~~The security architecture as defined in 3GPP TS 31.101 [3] applies to the terminal supporting ISIM application with the following definitions and requirements:~~

- ~~— A terminal shall support the use of level 1 user verification requirement as defined in 3GPP TS 31.101 [3].~~
- ~~— A terminal shall support the replacement of an ISIM application PIN with the Universal PIN, as defined in 3GPP TS 31.101 [3].~~
- ~~— A terminal shall support the security attributes defined using tag's '8C', 'AB' and '8B' as defined in 3GPP TS 31.101 [3]. In addition both the referencing methods indicated by tag '8B' shall be supported as defined in 3GPP TS 31.101 [3].~~

~~The access rule is referenced in the FCP using tag '8B'. The TLV object contains the file ID (the file ID of EF_{ARR}) and record number, or file ID (the file ID of EF_{ARR}), SEID and record number, pointer to the record in EF_{ARR} where the access rule is stored. Each SEID refers to a record number in EF_{ARR}. EFs having the same access rule use the same record reference in EF_{ARR}. For an example EF_{ARR}, see 3GPP TS 31.101 [3].~~

8 ~~void~~UICC Characteristics

8.1 ~~Voltage classes~~

~~A UICC holding an ISIM application shall support at least two consecutive voltage classes as defined in 3GPP TS 31.101 [3], e.g. AB or BC. If the UICC supports more than two classes, they shall all be consecutive, e.g. ABC.~~

8.2 ~~File Control Parameters (FCP)~~

~~This subclause defines the contents of the data objects which are part of the FCP information where there is a difference compared to the values as specified in 3GPP TS 31.101 [3]. This subclause also specifies values for data objects in the FCP information where there is no exact value given in 3GPP TS 31.101 [3] and there is a need for such from the ISIM application point of view.~~

8.2.1 ~~Minimum application clock frequency~~

~~This data object is indicated by tag '82' in the proprietary constructed data object in the FCP information, identified by tag 'A5', as defined in 3GPP TS 31.101 [3]. This data object specifies the minimum clock frequency to be provided by the terminal during the ISIM session. The value indicated in this data object shall not exceed 3 MHz, corresponding to '1E'. The terminal shall use a clock frequency between the value specified by this data object and the maximum clock frequency for the UICC as defined in 3GPP TS 31.101 [3]. If this data object is not present in the FCP response or the value is 'FF' then the terminal shall assume that the minimum clock frequency is 1 MHz.~~
