3GPP TSG-T (Terminals) Meeting #17
Biarritz, France 4 – 6 September 2002

Tdoc TP-020211

Source: T3

Title: Change Request to TS 31.103

Document for: Approval

This document contains one change request as follows:

T3 Doc	Spec	CR	Rv	Rel	Cat	Subject
T3-020665	31.103	001	-	Rel-5	F	Corrections

3GPP TSG-T3 Meeting #24
Seattle, USA, 19-22 August 2002

Tdoc ⌘T3-020665

CR-Form-v7

CHANGE REQUEST

⌘ **31.103** **CR** **001** ⌘ **rev** **-** ⌘ Current version: **5.0.0** ⌘

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

Proposed change affects: UICC apps⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Corrections
Source:	⌘	T3
Work item code:	⌘	IMS
Date:	⌘	22/08/2002
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one 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 one 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:	⌘	Some editorial errors need to be corrected. RFC 3261 replaces and obsoletes RFC 2543 which is referenced in TS 31.103. SA3 indicated that there is no need for an OFM bit at the ISIM level Wrong SFI in EF_{Keys}
Summary of change:	⌘	Various Corrections. Replacement of RFC 2543 with RFC 3261 Removal of OFM bit Correction of SFI in EF_{Keys} Make Annex D informative
Consequences if not approved:	⌘	May lead to wrong implementations. Presence of unused information

Clauses affected:	⌘	2, 3.3, 4.2.1, 4.2.2, 4.2.3, 4.2.4, 4.2.5, 4.3, 6.1, Annex D

Other specs affected:	⌘	Y	N		⌘
			X	Other core specifications	
			X	Test specifications	
			X	O&M Specifications	

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 ~~2543~~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".

3.3 Abbreviations

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

3GPP	3rd Generation Partnership Project
AC	Access Condition
ADF	Application Dedicated File
AID	Application IDentifier
AK	Anonymity Key
AKA	Authentication and Key Agreement
ALW	ALWays
AMF	Authentication Management Field
ASN.1	Abstract Syntax Notation One
AuC	Authentication Centre
AUTN	AUthentication TokeN
BER-TLV	Basic Encoding Rule - TLV
CK	Cipher Key
DF	Dedicated File
EF	Elementary File
FFS	For Further Study
HE	Home Environment
HN	Home Network
ICC	Integrated Circuit Card
ID	IDentifier
IK	Integrity Key
IM	IP Multimedia
IMPI	IM Private Identity
IMPU	IM PUblic identity
IMS	IP Multimedia Subsystem
ISIM	IM Services Identity Module
K	long-term secret Key shared between the ISIM and the AuC
KSI	Key Set Identifier
LI	Language Indication
LSB	Least Significant Bit
MAC	Message Authentication Code
MF	Master File
MSB	Most Significant Bit
NEV	NEVer
PIN	Personal Identification Number
PL	Preferred Languages
PS_DO	PIN Status Data Object
RAND	RANDom challenge
RES	user RESponse
RFU	Reserved for Future Use
RST	ReSeT
SDP	Session Description Protocol
SFI	Short EF Identifier
SIP	Session Initiation Protocol
SQN	SeQuence Number
SW	Status Word
TLV	Tag Length Value
UE	User Equipment

~~ISIM~~ ~~IM Services Identity Module~~
XRES eXpected user RESponse

4.2.1 EF_{Keys} (Ciphering and Integrity Keys for IMS)

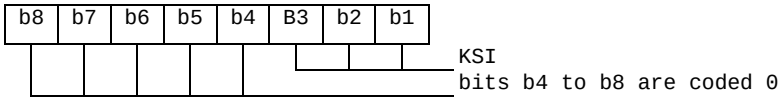
This EF contains the ciphering key CK, the integrity key IK and the key set identifier KSI for the IP Multimedia Subsystem.

Identifier: '6F08'	Structure: transparent	Mandatory
SFI: '01~~8~~'		
File size: 33 bytes	Update activity: high	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1	Key set identifier KSI	M	1 byte
2 to 17	Ciphering key CK	M	16 bytes
18 to 33	Integrity key IK	M	16 bytes

- Key Set Identifier KSI.

  Coding:



- Ciphering key CK.

  Coding:

  - the least significant bit of CK is the least significant bit of the 17th byte. The most significant bit of CK is the most significant bit of the 2nd byte.

- Integrity key IK.

  Coding:

  - the least significant bit of IK is the least significant bit of the 33rd byte. The most significant bit of IK is the most significant bit of the 18th byte.

4.2.2 EF_{IMPI} (IMS private identifier)

This EF contains the private SIP Identity (SIP URI) of the user.

Identifier: '6F02'	Structure: transparent	Mandatory
SFI: '02'		
File size: X bytes	Update activity: low	
Access Conditions: READ PIN UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to X	URI TLV data object	M	X bytes

- URI

  Contents:

  - Private SIP URI of the user.

  Coding:

  - For contents and coding of URI TLV data object values see IETF RFC ~~2543~~ 3261 [16]. The tag value of the URI TLV data object shall be '80'.

4.2.3 EF_{DOMAIN} (SIP domain URI)

This EF contains the SIP entry point in the home operator's network, if different from the host part of the private SIP URI of the user from file EF_{IMPI}.

Identifier: '6F03'	Structure: transparent	Mandatory
SFI: '05'		
File size: X bytes	Update activity: low	
Access Conditions: READ PIN UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to X	URI TLV data object	M	X bytes

- URI

  Contents:

  - Request-URI.

  Coding:

  - For contents and coding of URI TLV data object values see IETF RFC ~~2543~~ 3261 [16]. The tag value of the URI TLV data object shall be '80'.

4.2.4 EF_{IMPU} (IMS public Identifier of user)

This EF contains one or more public SIP Identities (SIP URI) of the user.

Identifier: '6F04'	Structure: linear fixed	Mandatory
SFI: '04'		
Record length: X bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	URI TLV data object	M	X bytes

- URI

  Contents:

  - SIP URI by which other parties know the subscriber.

  Coding:

  - For contents and coding of URI TLV data object values see IETF RFC ~~2543~~ 3261 [16]. The tag value of the URI TLV data object shall be '80'.

4.2.5 EF_{AD} (Administrative Data)

This EF contains information concerning the mode of operation according to the type of ISIM, such as normal (to be used by IMS subscribers for IMS operations), type approval (to allow specific use of the Terminal during type approval procedures of e.g. the network equipment), manufacturer specific (to allow the Terminal manufacturer to perform specific proprietary auto-test in its Terminal during e.g. maintenance phases).

It also provides an indication of whether some Terminal features should be activated during normal operation.

Identifier: '6FAD'	Structure: transparent	Mandatory
SFI: '03'		
File size: 3+X bytes	Update activity: low	

Access Conditions:

READ	ALW
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	UE operation mode	M	1 byte
2 to 3	Additional information	M	2 bytes
4 to 3+X	RFU	O	X bytes

- UE operation mode:

  Contents:

  - mode of operation for the UE

  Coding:

  - Initial value

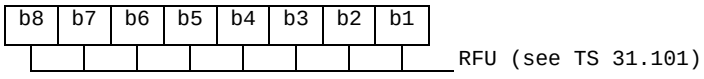
- '00' normal operation.
- '80' type approval operations.
- '01' normal operation + specific facilities.
- '81' type approval operations + specific facilities.
- '02' maintenance (off line).

- Additional information:

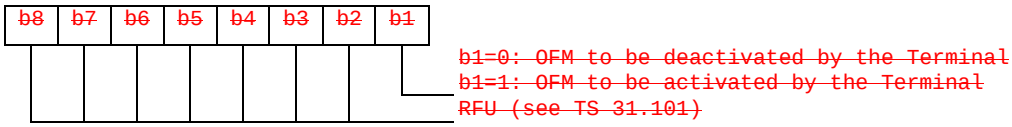
  Coding:

  - specific facilities (if b1=1 in byte 1);

    Bytes 2 and 3 (first byte of additional information):



~~Byte 3:~~



~~The OFM bit is used to control the Ciphering Indicator as specified in TS 22.101 [21].~~

~~Terminal manufacturer specific information (if b2=1 in byte 1).~~

4.3 ISIM file structure

This subclause contains a figure depicting the file structure of the ADF_{ISIM}. ADF_{ISIM} shall be selected using the AID and information in EF_{DIR}.

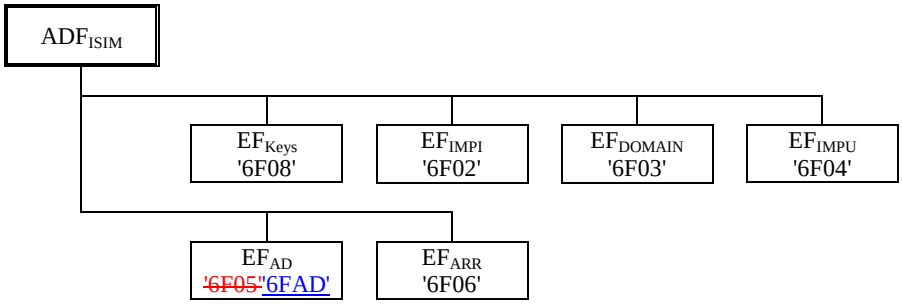


Figure 1: File identifiers and directory structures of ISIM

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/IEC7816-9 [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 referenceas PIN1 as specified in 3GPP TS 31.101 [3].
- For access to DFTelecom 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 a example EF_{ARR}, see 3GPP TS 31.101 [3].

Annex D (~~normative~~informative): List of SFI Values

This annex lists SFI values assigned in the present document.

D.1 List of SFI Values at the ISIM ADF Level

File Identification	SFI	Description
'6F08'	'01'	Ciphering and Integrity Keys for IMS
'6F02'	'02'	IMS private identifier
'6F03'	'05'	SIP domain URI
'6F04'	'04'	IMS public Identifier of user
'6FAD'	'03'	Administrative Data
'6F06'	'06'	Access Rule Reference

All other SFI values are reserved for future use.