



**Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);**

LTE;

**Characteristics of the IP Multimedia Services
Identity Module (ISIM) application
(3GPP TS 31.103 version 15.3.0 Release 15)**



ReferenceRTS/TSGC-0631103vf30

Keywords

GSM,LTE,UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:

<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.

Information on the current status of this and other ETSI documents is available at

<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommiteeSupportStaff.aspx>

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2018.

All rights reserved.

DECTTM, PLUGTESTSTM, UMTSTM and the ETSI logo are trademarks of ETSI registered for the benefit of its Members.

3GPPTM and LTETM are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

oneM2M logo is protected for the benefit of its Members.

GSM[®] and the GSM logo are trademarks registered and owned by the GSM Association.

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<https://ipr.etsi.org/>).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under <http://webapp.etsi.org/key/queryform.asp>.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Intellectual Property Rights	2
Foreword.....	2
Modal verbs terminology.....	2
Foreword.....	5
Introduction	5
1 Scope	6
2 References	6
3 Definitions, symbols, abbreviations and coding conventions	8
3.1 Definitions	8
3.2 Symbols.....	8
3.3 Abbreviations	8
3.4 Coding Conventions.....	9
4 Files	9
4.1 Contents of the EFs at the MF level	10
4.2 Contents of files at the ISIM ADF (Application DF) level	10
4.2.1 Void	10
4.2.2 EF _{IMPI} (IMS private user identity).....	10
4.2.3 EF _{DOMAIN} (Home Network Domain Name)	11
4.2.4 EF _{IMPU} (IMS public user identity).....	11
4.2.5 EF _{AD} (Administrative Data).....	12
4.2.6 EF _{ARR} (Access Rule Reference).....	13
4.2.7 EF _{IST} (ISIM Service Table).....	14
4.2.8 EF _{P-CSCF} (P-CSCF Address).....	15
4.2.9 EF _{GBABP} (GBA Bootstrapping parameters).....	16
4.2.10 EF _{GBANL} (GBA NAF List).....	17
4.2.11 EF _{NAFKCA} (NAF Key Centre Address)	18
4.2.12 EF _{SMS} (Short messages)	18
4.2.13 EF _{SMSS} (SMS status)	20
4.2.14 EF _{SMR} (Short message status reports).....	20
4.2.15 EF _{SMSP} (Short message service parameters).....	21
4.2.16 EF _{UICCIARI} (UICC IARI).....	22
4.2.17 EF _{FromPreferred} (From Preferred)	23
4.2.18 EF _{IMSConfigData} (IMS Configuration Data)	23
4.2.19 EF _{XCAPConfigData} (XCAP Configuration Data).....	24
4.2.20 EF _{WebRTCURI} (WebRTC URI).....	28
4.2.21 EF _{WLAN_EPS_Roaming_Handover} (WLAN to EPS Handover when Roaming).....	28
4.3 ISIM file structure	29
4.4 Contents of EFs at the TELECOM level	31
4.4.1 EF _{PSISMSC} (Public Service Identity of the SM-SC)	31
4.5 Contents of DFs at the TELECOM level.....	31
4.5.1 Contents of files at the DF _{MCS} level	31
5 Application protocol.....	31
5.1 ISIM management procedures.....	31
5.1.1 Initialisation	31
5.1.1.1 ISIM application selection	31
5.1.1.2 ISIM initialisation	32
5.1.2 ISIM Session termination	32
5.1.3 ISIM application closure.....	32
5.1.4 UICC presence detection	32
5.1.5 Administrative information request	32
5.2 ISIM security related procedures.....	33
5.2.1 Authentication procedure.....	33
5.2.2 IMPI request	33

5.2.3	IMPU request.....	33
5.2.4	SIP Domain request	33
5.2.5	Void	33
5.2.6	ISIM Service Table request	33
5.2.7	P-CSCF address request.....	33
5.2.8	Generic Bootstrapping architecture (Bootstrap)	33
5.2.9	Generic Bootstrapping architecture (NAF Derivation)	33
5.2.10	HTTP-Digest security request.....	33
5.2.11	NAF Key Centre Address request.....	33
5.3	Subscription related procedures	34
5.3.1	SM-over-IP	34
5.3.2	Communication Control for IMS by ISIM	34
5.3.3	UICC access to IMS	34
5.3.4	From Preferred related procedures.....	34
5.3.5	IMS Configuration Data related procedures	34
5.3.6	XCAP Configuration Data related procedures.....	34
5.3.7	WLAN to EPS Handover when Roaming.....	34
5.4	MCS related procedures	35
5.5	WebRTC related procedures	35
6	Security features	35
6.1	User verification and file access conditions	35
7	ISIM Commands	35
7.1	AUTHENTICATE	35
7.1.1	Command description	35
7.1.1.1	IMS AKA security context.....	36
7.1.1.2	GBA security context (Bootstrapping Mode)	36
7.1.1.3	GBA security context (NAF Derivation Mode)	37
7.1.1.4	HTTP-Digest security context.....	38
7.1.1.5	Local Key Establishment security context (Key Derivation mode)	38
7.1.1.6	Local Key Establishment security context (Key Availability Check mode)	38
7.1.2	Command parameters and data	39
7.1.2.1	IMS AKA security context.....	40
7.1.2.2	HTTP Digest security context	41
7.1.2.3	GBA security context (Bootstrapping Mode)	41
7.1.2.4	GBA security context (NAF Derivation Mode)	42
7.1.2.5	Local Key Establishment security context (All Modes).....	42
7.1.2.5.1	Local Key Establishment security context (Key Derivation mode).....	42
7.1.2.5.2	Local Key Establishment security context (Key Availability Check mode)	44
7.1.3	Status Conditions Returned by the ISIM	45
7.1.3.1	Security management	45
7.1.3.2	Status Words of the Commands	45
7.2	GET CHALLENGE	46
8	Void.....	46
Annex A (informative):	EF changes via Data Download or USAT applications	47
Annex B (informative):	Tags defined in 31.103	48
Annex C (informative):	Suggested contents of the EFs at pre-personalization	49
Annex D (informative):	List of SFI Values.....	50
D.1	List of SFI Values at the ISIM ADF Level	50
Annex E (informative):	ISIM Application Session Activation / Termination.....	51
Annex F (informative):	Change History	52
History		55

Foreword

This Technical Specification (TS) has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
 - 1 presented to TSG for information;
 - 2 presented to TSG for approval;
 - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

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.

1 Scope

The present document defines the ISIM application for access to IMS services.

The present document specifies:

- specific command parameters;
- file structures;
- contents of EFs (Elementary Files);
- security functions;
- application protocol to be used on the interface between UICC (ISIM) and Terminal.

This is to ensure interoperability between an ISIM and Terminal independently of the respective manufacturer, card issuer or operator.

The present document does not define any aspects related to the administrative management phase of the ISIM. Any internal technical realisation of either the ISIM or the Terminal is only specified where these are reflected over the interface. The present document does not specify any of the security algorithms that may be used.

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: "Identification cards - Integrated circuit cards, Part 4: Organization, security and commands for interchange". |
| [7] | Void. |
| [8] | Void. |
| [9] | 3GPP TS 23.003: "Numbering, Addressing and Identification". |
| [10] | Void. |
| [11] | Void. |
| [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] Void
- [19] 3GPP TS 51.011 Release 4: "Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface".
- [20] ISO/IEC 8825-1 (2008): "Information technology – ASN.1 encoding rules : Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)".
- [21] 3GPP TS 22.101: "Service aspects; Service principles".
- [22] Void.
- [23] ETSI TS 101 220: "Smart cards; ETSI numbering system for telecommunication application providers".
- [24] IETF RFC 2486: "The Network Access Identifier".
- [25] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic bootstrapping architecture".
- [26] IETF RFC 2617: "HTTP Authentication: Basic and Digest Access Authentication".
(<http://www.ietf.org/rfc/rfc2617.txt>)
- [27] IETF RFC 3629 (2003): "UTF-8, a transformation format of ISO 10646".
- [28] 3GPP TS 33.110: "Key establishment between a Universal Integrated Circuit Card (UICC) and a terminal".
- [29] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)".
- [30] 3GPP TS 24.011: "Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".
- [31] 3GPP TS 31.111: "USIM Application Toolkit (USAT)".
- [32] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".
- [33] 3Void
- [34] 3GPP TS 24.607: "Originating Identification Presentation (OIP) and Originating Identification Restriction (OIR) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification".
- [35] 3GPP TS 24.167: "3GPP IMS Management Object (MO); Stage 3".
- [36] 3GPP TS 24.341: "Support of SMS over IP networks; Stage 3".
- [37] OMA-DDS-DM_ConnMO_3GPPPS-V1_0-20081024-A: " Standardized Connectivity Management Objects 3GPP Packet Switched Bearer Paramaters".
- [38] OMA-DDS-DM_ConnMO-V1_0-20081107-A: " Standardized Connectivity Management Objects".
- [39] 3GPP TS 24.424: "Management Object (MO) for Extensible Markup Language (XML) Configuration Access Protocol (XCAP) over the Ut interface for Manipulating Supplementary Services (SS)".

- [40] 3GPP TS 24.623: "Extensible Markup Language (XML) Configuration Access Protocol (XCAP) over the Ut interface for Manipulating Supplementary Services".
- [41] OMA OMA-TS-XDM_MO-V1_1-20080627-A: "OMA Management Object for XML Document Management".
- [42] vod.
- [43] 3GPP TS 24.483: "Mission Critical Services(MCS) Management Object (MO)".

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 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

The AID of ISIM is defined in 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

3.2 Symbols

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

	Concatenation
⊕	Exclusive or
f1	Message authentication function used to compute MAC
f1*	A message authentication code (MAC) function with the property that no valuable information can be inferred from the function values of f1* about those of f1, ... , f5 and vice versa
f2	Message authentication function used to compute RES and XRES
f3	Key generating function used to compute CK
f4	Key generating function used to compute IK
f5	Key generating function used to compute AK

3.3 Abbreviations

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

3GPP	3 rd 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
B-TID	Bootstrapping Transaction Identifier
CK	Cipher Key
DF	Dedicated File
EF	Elementary File

FFS	For Further Study
FQDN	Fully Qualified Domain Name
HE	Home Environment
HN	Home Network
IARI	IMS Application Reference Identifier
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
MCData	Mission Critical Data
MCPTT	Mission Critical Push To Talk
MCS	Mission Critical Services
MCVideo	Mission Critical Video
MF	Master File
MSB	Most Significant Bit
NAI	Network Access Identifier
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
WebRTC	Web Real-Time Communication
WWSF	WebRTC Web Server Function
XRES	eXpected user RESponse

3.4 Coding Conventions

The following coding conventions apply to the present document.

All lengths are presented in bytes, unless otherwise stated. Each byte is represented by bits b8 to b1, where b8 is the most significant bit (MSB) and b1 is the least significant bit (LSB). In each representation, the leftmost bit is the MSB.

The coding of Data Objects in the present document is according to TS 31.101 [3].

'XX': Single quotes indicate hexadecimal values. Valid elements for hexadecimal values are the numbers '0' to '9' and 'A' to 'F'.

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.

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 TS 31.101 [3].

4.2 Contents of files at the ISIM ADF (Application DF) level

The EFs in the ISIM ADF contain service and network related information and are required for UE to operate in an IP Multimedia Subsystem.

The File IDs '6F1X' (for EFs), '5F1X' and '5F2X' (for DFs) with X ranging from '0' to 'F' are reserved under the ISIM ADF for administrative use by the card issuer.

4.2.1 Void

4.2.2 EF_{IMPI} (IMS private user identity)

This EF contains the private user identity 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	NAI TLV data object		M	X bytes

- NAI

Contents:

- Private user identity of the user.

Coding:

- For contents and syntax of NAI TLV data object values see IETF RFC 2486 [24]. The NAI shall be encoded to an octet string according to UTF-8 encoding rules as specified in IETF RFC 3629 [27]. The tag value of the NAI TLV data object shall be '80'.

4.2.3 EF_{DOMAIN} (Home Network Domain Name)

This EF contains the home operator's network domain name.

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	Home Network Domain Name TLV data object	M	X bytes	

- URI

Contents:

- Home Network Domain Name.

Coding:

- For contents and syntax of Home Network Domain Name TLV data object values see TS 23.003 [9]. The Home Network Domain Name, i.e. FQDN shall be encoded to an octet string according to UTF-8 encoding rules as specified in IETF RFC 3629 [27]. The tag value of the Home Network Domain Name TLV data object shall be '80'.

4.2.4 EF_{IMPU} (IMS public user identity)

This EF contains one or more records, with each record able to hold a public SIP Identity (SIP URI) of the user. The first (or only) record in the EF shall be used when performing emergency registration; or as the default SIP Identity in case that no record is explicitly selected either in the current session or as a carryover from a prior session.

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 syntax of URI TLV data object values see IETF RFC 3261 [16]. The URI shall be encoded to an octet string according to UTF-8 encoding rules as specified in IETF RFC 3629 [27]. 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):

b8	b7	b6	b5	b4	b3	b2	b1

RFU (see TS 31.101)