ETSI TS 131 103 V19.0.0 (2025-10)

TECHNICAL SPECIFICATION

Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
LTE;
5G;
Characteristics of
the IP Multimedia Services Identity Module (ISIM) application
(3GPP TS 31.103 version 19.0.0 Release 19)

Reference
RTS/TSGC-0631103vj00

Keywords
5G,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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

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. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found at 3GPP to ETSI numbering cross-referencing.

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
Legal Notice 2
Modal verbs terminology 2
Foreword 6
Introduction 7
1 Scope 8
2 References 8
3 Definitions, symbols, abbreviations and coding conventions 10
3.1 Definitions 10
3.2 Symbols 10
3.3 Abbreviations 10
3.4 Coding Conventions 11
4 Files 12
4.1 Contents of the EFs at the MF level 12
4.2 Contents of files at the ISIM ADF (Application DF) level 12
4.2.1 Void 12
4.2.2 EF_{IMPI} (IMS private user identity) 12
4.2.3 EF_{DOMAIN} (Home Network Domain Name) 13
4.2.4 EF_{IMPU} (IMS public user identity) 13
4.2.5 EF_{AD} (Administrative Data) 14
4.2.6 EF_{ARR} (Access Rule Reference) 15
4.2.7 EF_{IST} (ISIM Service Table) 15
4.2.8 $EF_{P\text{-}CSCF}$ (P-CSCF Address) 17
4.2.9 EF_{GBABP} (GBA Bootstrapping parameters) 18
4.2.10 EF_{GBANL} (GBA NAF List) 19
4.2.11 EF_{NAFKCA} (NAF Key Centre Address) 19
4.2.12 EF_{SMS} (Short messages) 20
4.2.13 EF_{SMSS} (SMS status) 21
4.2.14 EF_{SMSR} (Short message status reports) 22
4.2.15 EF_{SMSP} (Short message service parameters) 23
4.2.16 $EF_{UICCIARI}$ (UICC IARI) 24
4.2.17 $EF_{FromPreferred}$ (From Preferred) 25
4.2.18 $EF_{IMSConfigData}$ (IMS Configuration Data) 25
4.2.19 $EF_{XCAPConfigData}$ (XCAP Configuration Data) 27
4.2.20 $EF_{WebRTCURI}$ (WebRTC URI) 31
4.2.21 $EF_{MuDMiDConfigData}$ (MuD and MiD Configuration Data) 31
4.2.22 $EF_{AC\_GBAUAPI}$ (Access Control to GBA_U_API) 32
4.2.23 EF_{IMSDCI} (IMS Data Channel Indication) 33
4.3 ISIM file structure 34
4.4 Contents of EFs at the TELECOM level 34
4.4.1 $EF_{PSISMSC}$ (Public Service Identity of the SM-SC) 34
4.5 Contents of DFs at the TELECOM level 34
4.5.1 Contents of files at the DF_{MCS} level 35
5 Application protocol 35
5.1 ISIM management procedures 35
5.1.1 Initialisation 35
5.1.1.1 ISIM application selection 35
5.1.1.2 ISIM initialisation 35
5.1.2 ISIM Session termination 36
5.1.3 ISIM application closure 36
5.1.4 UICC presence detection 36
5.1.5 Administrative information request 36

5.2 ISIM security related procedures....36
5.2.1 Authentication procedure....36
5.2.2 IMPI request....36
5.2.3 IMPU request....37
5.2.4 SIP Domain request....37
5.2.5 Void....37
5.2.6 ISIM Service Table request....37
5.2.7 P-CSCF address request....37
5.2.8 Generic Bootstrapping architecture (Bootstrap)....37
5.2.9 Generic Bootstrapping architecture (NAF Derivation)....37
5.2.10 HTTP-Digest security request....37
5.2.11 NAF Key Centre Address request....37
5.3 Subscription related procedures....37
5.3.1 SM-over-IP....37
5.3.2 Communication Control for IMS by ISIM....38
5.3.3 UICC access to IMS....38
5.3.4 From Preferred related procedures....38
5.3.5 IMS Configuration Data related procedures....38
5.3.6 XCAP Configuration Data related procedures....38
5.4 MCS related procedures....38
5.5 WebRTC related procedures....38
5.6 IMS DC Establishment indication procedures....39
5.6.1 IMS DC Establishment indication procedure....39

6 Security features....39
6.1 User verification and file access conditions....39

7 ISIM Commands....39
7.1 AUTHENTICATE....39
7.1.1 Command description....39
7.1.1.1 IMS AKA security context....40
7.1.1.2 GBA security context (Bootstrapping Mode)....40
7.1.1.3 GBA security context (NAF Derivation Mode)....41
7.1.1.4 HTTP-Digest security context....41
7.1.1.5 Local Key Establishment security context (Key Derivation mode)....42
7.1.1.6 Local Key Establishment security context (Key Availability Check mode)....42
7.1.2 Command parameters and data....43
7.1.2.1 IMS AKA security context....44
7.1.2.2 HTTP Digest security context....45
7.1.2.3 GBA security context (Bootstrapping Mode)....45
7.1.2.4 GBA security context (NAF Derivation Mode)....46
7.1.2.5 Local Key Establishment security context (All Modes)....46
7.1.2.5.1 Local Key Establishment security context (Key Derivation mode)....46
7.1.2.5.2 Local Key Establishment security context (Key Availability Check mode)....48
7.1.3 Status Conditions Returned by the ISIM....49
7.1.3.1 Security management....49
7.1.3.2 Status Words of the Commands....50
7.2 GET CHALLENGE....50

8 Void....50

Annex A (informative): EF changes via Data Download or USAT applications....51

Annex B (informative): Tags defined in 31.103....52

Annex C (informative): Suggested contents of the EFs at pre-personalization....53

Annex D (informative): List of SFI Values....54

D.1 List of SFI Values at the ISIM ADF Level....54

Annex E (informative): ISIM Application Session Activation / Termination....55

Annex F (informative): Change History....56

History 59

Foreword

This Technical Specification 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.

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

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] void.

[43] 3GPP TS 24.483: "Mission Critical Services(MCS) Management Object (MO)".

[44] 3GPP TS 24.175: "Management Object (MO) for Multi-Device and Multi-Identity in IMS".

[45] 3GPP TS 24.174: "Support of Multi-Device and Multi-Identity in IMS; Stage 3".

[46] 3GPP TS 31.130: "(U)SIM Application Programming Interface (API);(U)SIM API for Java Card".

[47] 3GPP TS 24.275: "Management Object (MO) for basic communication part of IMS multimedia telephony (MMTEL) communication service".

[48] 3GPP TS 24.186: "IMS Data Channel applications; Protocol specification".

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	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
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
MiD	Multi-iDentity
MSB	Most Significant Bit
MuD	Multi-Device
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; oras 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

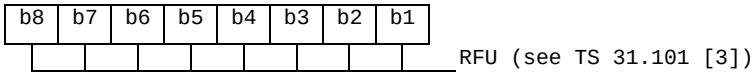
  Coding:

  - 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):



4.2.6 EF_{ARR} (Access Rule Reference)

This EF contains the access rules for files located under the ISIM ADF in the UICC. If the security attribute tag '8B' is indicated in the FCP it contains a reference to a record in this file.

Structure of EF_{ARR} at ADF-level

Identifier: '6F06'	Structure: Linear fixed	Mandatory
SFI: '06'		
Record Length: X bytes	Update activity: low	
Access Conditions: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to X	Access Rule TLV data objects	M	X bytes

This EF contains one or more records containing access rule information according to the reference to expanded format as defined in ISO/IEC 7816-4 [6]. Each record represents an access rule. Unused bytes in the record are set to 'FF'.

If the card cannot access EF_{ARR} , any attempt to access a file with access rules indicated in this EF_{ARR} shall not be granted.

4.2.7 EF_{IST} (ISIM Service Table)

This EF indicates which optional services are available. If a service is not indicated as available in the ISIM, the ME shall not select this service. The presence of this file is mandatory if optional services are provided in the ISIM.

Identifier: '6F07'	Structure: transparent	Optional
SFI: '07'		
File size: X bytes, X >= 1	Update activity: low	
Access Conditions: READ PIN UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1	Services n°1 to n°8	M	1 byte
2	Services n°9 to n°16	O	1 byte
3	Services n°17 to n°24	O	1 byte
4	Services n°25 to n°32	O	1 byte
etc.			
X	Services n°(8X-7) to n°(8X)	O	1 byte

-Services

Contents:		
	Service n°1:	P-CSCF address
	Service n°2	Generic Bootstrapping Architecture (GBA)
	Service n°3	HTTP Digest
	Service n°4	GBA-based Local Key Establishment Mechanism
	Service n°5	Support of P-CSCF discovery for IMS Local Break Out
	Service n°6	Short Message Storage (SMS)
	Service n°7	Short Message Status Reports (SMSR)
	Service n°8	Support for SM-over-IP including data download via SMS-PP as defined in TS 31.111 [31]
	Service n°9	Communication Control for IMS by ISIM
	Service n°10	Support of UICC access to IMS
	Service n°11	URI support by UICC
	Service n°12	Media Type support
	Service n°13	IMS call disconnection cause
	Service n°14	URI support for MO SHORT MESSAGE CONTROL
	Service nº15	Mission Critical Services
	Service n°16	URI support for SMS-PP DOWNLOAD as defined in 3GPP TS 31.111 [31]
	Service n°17	From Preferred
	Service n°18	IMS configuration data
	Service n°19	XCAP Configuration Data
	Service n°20	WebRTC URI
	Service n°21	MuD and MiD configuration data
	Service n°22	IMS Data Channel Indication

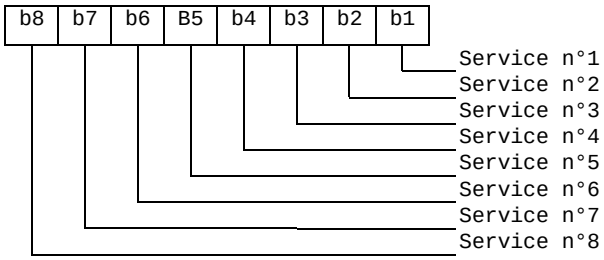
The EF shall contain at least one byte. Further bytes may be included, but if the EF includes an optional byte, then it is mandatory for the EF to also contain all bytes before that byte. Other services are possible in the future and will be coded on further bytes in the EF. The coding falls under the responsibility of the 3GPP.

Coding:

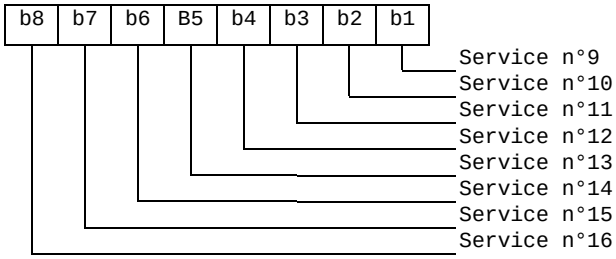
1 bit is used to code each service:
bit = 1: service available;
bit = 0: service not available.

- Service available means that the ISIM has the capability to support the service and that the service is available for the user of the ISIM.
  Service not available means that the service shall not be used by the ISIM user, even if the ISIM has the capability to support the service.

First byte:



Second byte:



etc.

4.2.8 $EF_{P\text{-}CSCF}$ (P-CSCF Address)

If service n°1 and/or service n°5 is "available", this file shall be present.

A UE supporting IMS Local Breakout shall use this EF only if EF_{IST} indicates that service n°5 is "available".

This EF contains one or more Proxy Call Session Control Function addresses. The first record in the EF shall be considered to be of the highest priority. The last record in the EF shall be considered to be the lowest priority.

Identifier: '6F09'	Structure: linear fixed	Optional
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	P-CSCF Address TLV data object	M	X bytes

P-CSCF

Contents:

- Address of Proxy Call Session Control Function, in the format of a FQDN, an IPv4 address, or an IPv6 address.

Coding:

- The tag value of this P-CSCF address TLV data object shall be '80'. The format of the data object is as follows:

Field	Length (bytes)
Tag	1
Length	1
Address Type	1
P-CSCF Address	Address Length

Address Type: Type of the P-CSCF address.

This field shall be set to the type of the P-CSCF address according to the following:

Value	Name
'00'	FQDN
'01'	IPv4
'02'	IPv6
All other values are reserved	

P-CSCF Address: Address of the Proxy Call Session Control Function

This field shall be set to the address of the Proxy Call Session Control Function. When the P-SCSF type is set to '00', the corresponding P-CSCF Address shall be encoded to an octet string according to UTF-8 encoding rules as specified in IETF RFC 3629 [27].

Unused bytes shall be set to 'FF'.

4.2.9 EF_{GBABP} (GBA Bootstrapping parameters)

If service n°2 is "available", this file shall be present.

This EF contains the AKA Random challenge (RAND) and Bootstrapping Transaction Identifier (B-TID) associated with a GBA bootstrapping procedure.

Identifier: '6FD5'	Structure: transparent	Optional
File length: L+X+N+3 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Length of RAND (16)	M	1 byte
2 to (X+1)	RAND	M	X bytes
X+2	Length of B-TID (L)	M	1 byte
(X+3) to (X+2+L)	B-TID	M	L bytes
X+L+3	Length of key lifetime	M	1 byte
(X+L+4) to (X+L+N+3)	Key lifetime	M	N bytes

- Length of RAND
  Contents: number of bytes, not including this length byte, of RAND field

- RAND
  Contents: Random challenge used in the GBA_U bootstrapping procedure.
  Coding: as defined in TS 33.103 [5].

- Length of B-TID
  Contents: number of bytes, not including this length byte, of B-TID field

- B-TID
  Content: Bootstrapping Transaction Identifier the GBA_U bootstrapped keys

  Coding: As defined in TS 33.220 [25]

- Length of key lifetime

Contents: number of bytes, not including this length byte, of key lifetime field

- Key lifetime
  Content: Lifetime of the GBA_U bootstrapped keys

  Coding: As defined in TS 33.220 [25]

4.2.10 EF_{GBANL} (GBA NAF List)

If service n°2 is "available", this file shall be present.

This EF contains the list of NAF_ID and B-TID associated to a GBA NAF derivation procedure.

Identifier: '6FD7'	Structure: Linear fixed	Optional
Record length: Z bytes	Update activity: low	
Access Conditions: READ PIN UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to Z	NAF Key Identifier TLV objects	M	Z bytes

NAF Key Identifier tags

Description	Tag Value
NAF_ID Tag	'80'
B-TID Tag	'81'

NAF Key Identifier information

Description	Value	M/O	Length (bytes)
NAF_ID Tag	'80'	M	1
Length	X	M	Note
NAF_ID value	--	M	X
B-TID Tag	'81'	M	1
Length	Y	M	Note
B-TID value	--	M	Y
NOTE: The length is coded according to ISO/IEC 8825-1 [20]			

- NAF_ID Tag '80'

  Contents:

  - Identifier of Network Application Function used in the GBA_U NAF Derivation procedure.

  Coding:

  - As defined in TS 33.220 [25]

- B-TID Tag '81'

  Content:

  - Bootstrapping Transaction Identifier of the GBA_U bootstrapped key

  Coding:

  - As defined in TS 33.220 [25]

Unused bytes shall be set to 'FF'

4.2.11 EF_{NAFKCA} (NAF Key Centre Address)

If service n°2 and service n°4 are "available", this file shall be present.

This EF contains one or more NAF Key Centre addresses. The first record in the EF shall be considered to be of the highest priority. The last record in the EF shall be considered to be the lowest priority.

Identifier: '6FDD'	Structure: Linear fixed	Optional
Record length: Z bytes	Update activity: low	

Access Conditions:
READ PIN
UPDATE ADM
DEACTIVATE ADM
ACTIVATE ADM

Bytes	Description	M/O	Length
1 to Z	NAF Key Centre TLV object	M	Z bytes

Unused bytes shall be set to 'FF'.

NAF Key Centre tags

Description	Tag Value
NAF Key Centre address Tag	'80'

NAF Key Centre information

Description	Value	M/O	Length (bytes)
NAF Key Centre address Tag	'80'	M	1
Length	X	M	Note
NAF Key Centre address value	--	M	X
Note: The length is coded according to ISO/IEC 8825-1 [20]			

- NAF Key Centre Address value (Tag '80')

  Contents:

  Fully qualified Domain Name (FQDN) of the NAF Key Centre used in the Local Key Establishment procedures (see TS 33.110 [28]).

  Coding:

  Encoded to an octet string according to UTF-8 encoding rules as described in IETF RFC 3629 [27].

4.2.12 EF_{SMS} (Short messages)

This file shall be present if and only if service n°6 and n°8 are "available".

This EF contains information in accordance with TS 23.040 [29] comprising short messages (and associated parameters) which have either been received by the UE from the network, or are to be used as an UE originated message.

Identifier: '6F3C'	Structure: linear fixed	Optional
Record length: 176 bytes	Update activity: low	

Access Conditions:
READ PIN
UPDATE PIN
DEACTIVATE ADM
ACTIVATE ADM

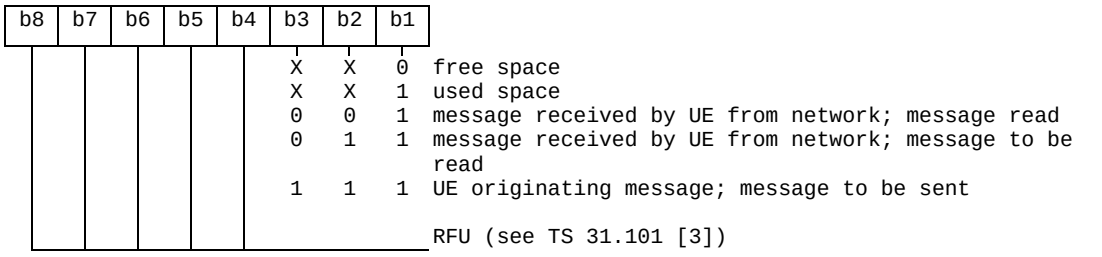
Bytes	Description	M/O	Length
1	Status	M	1 byte
2 to 176	Remainder	M	175 bytes

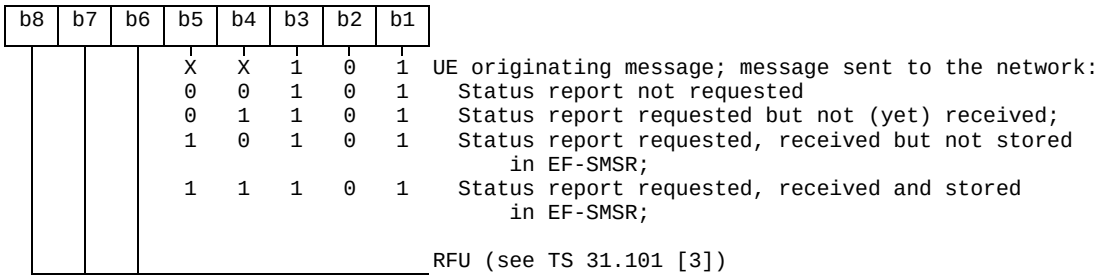
- Status.

Contents:

Status byte of the record which can be used as a pattern in the SEARCH RECORD command. For UE originating messages sent to the network, the status shall be updated when the UE receives a status report, or sends a successful SMS Command relating to the status report.

Coding:





- Remainder.

Contents:

This data item commences with the TS-Service-Centre-Address as specified in TS 24.011 [30]. The bytes immediately following the TS-Service-Centre-Address contain an appropriate short message TPDU as specified in TS 23.040 [29], with identical coding and ordering of parameters.

Coding:

according to TS 23.040 [29] and TS 24.011 [30]. Any TP-message reference contained in an UE originated message stored in the ISIM, shall have a value as follows:

Value of the TP-message-reference:
message to be sent: 'FF'.
message sent to the network: the value of TP-Message-Reference used in the message sent to the network.

Any bytes in the record following the TPDU shall be filled with 'FF'.

It is possible for a TS-Service-Centre-Address of maximum permitted length, e.g. containing more than 18 address digits, to be associated with a maximum length TPDU such that their combined length is 176 bytes. In this case the ME shall store in the ISIM the TS-Service-Centre-Address and the TPDU in bytes 2 to 176 without modification, except for the last byte of the TPDU, which shall not be stored.

4.2.13 EF_{SMSS} (SMS status)

This file shall be present if and only if service n°6 and n°8 are "available".

This EF contains status information relating to the short message service.

Identifier: '6F43'	Structure: transparent	Optional
File size: 2+X bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Last Used TP-MR	M	1 byte
2	SMS "Memory Cap. Exceeded" Not. Flag	M	1 byte
3 to 2+X	RFU	O	X bytes

- Last Used TP-MR.

Contents:

- the value of the TP-Message-Reference parameter in the last mobile originated short message, as defined in TS 23.040 [29].

Coding:

- as defined in TS 23.040 [29].

- SMS "Memory Capacity Exceeded" Notification Flag.

Contents:

- this flag is required to allow a process of flow control, so that as memory capacity in the UE becomes available, the Network can be informed. The process for this is described in TS 23.040 [29].

Coding:

b1=1 means flag unset; memory capacity available;
b1=0 means flag set;
b2 to b8 are reserved and set to 1.

4.2.14 EF_{SMSR} (Short message status reports)

This file shall be present if and only if service n°7 and n°8 are "available".

This EF contains information in accordance with TS 23.040 [29] comprising short message status reports which have been received by the UE from the network.

Each record is used to store the status report of a short message in a record of EF_{SMS}. The first byte of each record is the link between the status report and the corresponding short message in EF_{SMS}.

Identifier: '6F47'	Structure: linear fixed	Optional
Record length: 30 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	SMS record identifier	M	1
2 to 30	SMS status report	M	29 bytes

- SMS record identifier.

Contents:

- this data item identifies the corresponding SMS record in EF_{SMS}, e.g. if this byte is coded '05' then this status report corresponds to the short message in record #5 of EF_{SMS}.

Coding:

- '00' - empty record;
- '01' to 'FF' - record number of the corresponding SMS in EF_{SMS}.

- SMS status report:

Contents:

- this data item contains the SMS-STATUS-REPORT TPDU as specified in TS 23.040 [29], with identical coding and ordering of parameters.

Coding:

- according to TS 23.040 [29]. Any bytes in the record following the TPDU shall be filled with 'FF'.

4.2.15 EF_{SMSP} (Short message service parameters)

If service n°8 is "available", this file shall be present.

This EF contains values for Short Message Service header Parameters (SMSP), which can be used by the ME for user assistance in preparation of mobile originated short messages. For example, a service centre address will often be common to many short messages sent by the subscriber.

The EF consists of one or more records, with each record able to hold a set of SMS parameters. The first (or only) record in the EF shall be used as a default set of parameters, if no other record is selected.

To distinguish between records, an alpha-identifier may be included within each record, coded on Y bytes.

The SMS parameters stored within a record may be present or absent independently. When a short message is to be sent from the UE, the parameter in the ISIM record, if present, shall be used when a value is not supplied by the user.

Identifier: '6F42'	Structure: linear fixed	Optional
Record length: 28+Y bytes	Update activity: low	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to Y	Alpha-Identifier	O	Y bytes
Y+1	Parameter Indicators	M	1 byte
Y+2 to Y+13	TP-Destination Address	M	12 bytes
Y+14 to Y+25	TS-Service Centre Address	M	12 bytes
Y+26	TP-Protocol Identifier	M	1 byte
Y+27	TP-Data Coding Scheme	M	1 byte
Y+28	TP-Validity Period	M	1 byte

Storage is allocated for all of the possible SMS parameters, regardless of whether they are present or absent. Any bytes unused, due to parameters not requiring all of the bytes, or due to absent parameters, shall be set to 'FF'.

- Alpha-Identifier.

Contents:

Alpha Tag of the associated SMS-parameter.

Coding:

see TS 31.102 [2] (EF_{ADN}).

NOTE: The value of Y may be zero, i.e. the alpha-identifier facility is not used. By using the command GET RESPONSE the ME can determine the value of Y.

- Parameter Indicators.

Contents:

each of the default SMS parameters which can be stored in the remainder of the record are marked absent or present by individual bits within this byte.

Coding:

allocation of bits:
bit number Parameter indicated.
1 TP-Destination Address.
2 TS-Service Centre Address.
3 TP-Protocol Identifier.
4 TP-Data Coding Scheme.
5 TP-Validity Period.
6 reserved, set to 1.
7 reserved, set to 1.
8 reserved, set to 1.

Bit value Meaning.
0 Parameter present.
1 Parameter absent.

- TP-Destination Address.

Contents and Coding:
as defined for SM-TL address fields in TS 23.040 [29].

- TP-Service Centre Address.

Contents and Coding:
as defined for RP-Destination address Centre Address in TS 24.011 [30].

- TP-Protocol Identifier.

Contents and Coding:
as defined in TS 23.040 [29].

- TP-Data Coding Scheme.

Contents and Coding:
as defined in TS 23.038 [17].

- TP-Validity Period.

Contents and Coding:
as defined in TS 23.040 [29] for the relative time format.

4.2.16 $EF_{UICCIARI}$ (UICC IARI)

If service n°10 is "available", this file shall be present.

As specified in TS 24.229 [32] a ME includes the list of IARIs for the IMS applications it intends to use when sending an initial registration or when sending subsequent registrations to the IMS in the form of a SIP REGISTER request.

This EF contains a list of IARIs associated with active applications installed on the UICC that are included in the SIP REGISTER request in accordance with the procedures of TS 24.229 [32].

NOTE: If this file is present in both the USIM and the ISIM, the file in the ISIM is used. It is assumed that the presence of this file in the USIM when an ISIM is present on the UICC is an incorrect configuration of the UICC.

Identifier: '6FE7'	Structure: linear fixed	Optional
Record length: X bytes.	Update activity: low	
Access Conditions: READ PIN UPDATE ADM ACTIVATE ADM DEACTIVATE ADM		

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

IARI TLV object:
Contents:

- The content and coding is defined below.

Coding of the IARI TLV objects

Length	Description	Value	Status
1 byte	IARI TLV TAG	'80'	M
1 byte	Length of IARI	Y	M
Y bytes	IARI value	-	M

- Coding:

  IMS Application Reference Identifier: shall be coded as specified in TS 24.229 [32].

Unused bytes shall be set to 'FF'.

4.2.17 $EF_{FromPreferred}$ (From Preferred)

If service n°17 is "available", this file shall be present.

It shall be possible to define if the UE uses the From header field for the determination of the originating party identity in the OIP service. For more detailed description see 3GPP TS 24.607 [34] clause 4.5.2.12.

NOTE: If this file is present in both the USIM and the ISIM, the file in the ISIM is used. It is assumed that the presence of this file in the USIM when an ISIM is present on the UICC is an incorrect configuration of the UICC.

For the structure, content and coding of this file, see $EF_{FromPreferred}$ in 3GPP TS 31.102 [2]

4.2.18 $EF_{IMSConfigData}$ (IMS Configuration Data)

If service n°18 is "available", this file shall be present.

This EF contains the IMS configuration data object as specified in 3GPP TS 24.167 [35].

Identifier: '6FF8'	Structure: BER-TLV	Optional
File size: X bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
N/A	IMS configuration data encoding	M	3 bytes
N/A	IMS configuration data	O	Y bytes

IMS configuration data object tags:

IMS configuration data objects	Tag Values
IMS configuration data encoding	'80'
IMS configuration data	'81'

Coding of the IMS configuration data encoding object

Contents:

Indicates the coding used for all the IMS configuration management objects stored in the $EF_{IMSConfigData}$.

Coding:

A value of '00' indicates the XML format described in 3GPP TS 24.167 [35]. All other values are reserved.

Unused bytes shall be set to 'FF'.

IMS configuration data object:

Coding of the IMS Configuration data object

Length	Description	Value	Status
1 byte	IMS configuration data object Tag	'81'	M
X byte	IMS configuration data object Length	Y	M
Y bytes	IMS configuration data	-	M

Contents:

The IMS configuration data can contain the following nodes and associated parent node from 3GPP TS 24.167 [35]:

1 Default_EPS_bearer_context_usage_restriction_policy node and its descendant nodes as described in 3GPP TS 24.167 [35]. Procedures for use of this policy are described in 3GPP TS 24.229 [32] clause L.2.2.5.1D.

2 Media_type_restriction_policy node and its descendant nodes as described in 3GPP TS 24.167 [35]. Procedures for use of this policy are described in 3GPP TS 24.229 [32] clause 6.1.1.

3 Reliable_18x_policy node and its descendant nodes as described in 3GPP TS 24.167 [35]. Procedures for use of this policy are described in TS 24.229 [32] clause 5.1.4.2.

4 EPS_initial_attach_ConRefs node and its descendant nodes as described in 3GPP TS 24.167 [35]. Procedures for use of this policy are described in TS 24.229 [32] clause L.2.2.1.

5 Precondition_disabling_policy node and its descendant nodes as described in 3GPP TS 24.167 [35]. Procedures for use of this policy are described in TS 24.229 [32] clause 5.1.5A.

6 Timer_Emerg-reg leaf as described in 3GPP TS 24.167 [35]. Procedures for use of this policy are described in TS 24.229 [32] clause 5.1.6.1.

7 EPC_via_untrusted_WLAN_mean_rekeying_time leaf as described in 3GPP TS 24.167 [35]. Procedures for use of this policy are described in TS 24.229 [32] Annex R.2.2.1.

8 EPC_via_untrusted_WLAN_NAT_keep_alive_time leaf as described in 3GPP TS 24.167 [35]. Procedures for use of this policy are described in TS 24.229 [32] Annex R.2.2.1.

9 EPC_via_untrusted_WLAN_timeout_period_for_liveness_check leaf as described in 3GPP TS 24.167 [35]. Procedures for use of this policy are described in TS 24.229 [32] Annex R.2.2.1.

10 Policy_on_local_numbers node and its descendant nodes as described in 3GPP TS 24.167 [35]. Procedures for use of this policy are described in TS 24.229 [32] clause 5.1.2A.1.5A.

11 SMSoIP_usage_policy leaf as described in 3GPP TS 24.167 [35]. Procedures for use of this policy are described in TS 24.341 [36] clause 5.2.1.3.

12 Timer_Emerg-request leaf as described in 3GPP TS 24.167 [35]. Procedures for use of this policy are described in TS 24.229 [32] clause 5.1.6.8.1.

13 IMS_Registration_Policy node as described in 3GPP TS 24.167 [35]. Procedures for use of this policy are described in TS 24.229 [32] Annex B.3.1.0a and TS 24.229 [32] Annex L.3.1.0a.

14 Default_QoS_Flow_usage_restriction_policy node and its descendant nodes as described in 3GPP TS 24.167 [35]. Procedures for use of this policy are described in 3GPP TS 24.229 [32] clause U.2.2.5.1D.

15 Timer_Emerg_non3gpp leaf as described in 3GPP TS 24.167 [35]. Procedures for use of this policy are described in 3GPP TS 24.229 [32] Annex R.2.2.6.1 and W.2.2.6.1.

16 Allow_Handover_PDN_connection_WLAN_and_EPS node as described in 3GPP TS 24.167 [35]. Procedures for use of this policy are described in TS 24.229 [32] Annex L.2.2.1 and TS 24.229 [32] Annex R.3.1.0.

17 SMS_Over_IP_Networks_Indication leaf as described in 3GPP TS 24.167 [35]. Procedures for use of this policy are described in TS 24.341 [36] clause 5.2.1.3 and in 3GPP TS 24.167 [35] clauses 5.28 and 5.71.

18 Allow_Handover_PDU_session_non-3GPP_and_NG-RAN node as described in 3GPP TS 24.167 [35]. Procedures for use of this policy are described in TS 24.229 [32] Annex R.2.2.1 TS 24.229 [32] Annex U.2.2.1 and TS 24.229 [32] Annex W.2.2.1.

19 Allow_Handover_PDN_connection_non-3GPP_and_NG-RAN node as described in 3GPP TS 24.167 [35]. Procedures for use of this policy are described in TS 24.229 [32] Annex R.2.2.1 TS 24.229 [32] Annex U.2.2.1.

Other nodes from 3GPP TS 24.167 [35] can be present in the IMS configuration data, however the ME shall ignore them.

Coding:

As specified in 3GPP TS 24.167 [35].

4.2.19 $EF_{XCAPConfigData}$ (XCAP Configuration Data)

If service n°19 is "available", this file shall be present.

This EF contains the XCAP configuration data object as specified in 3GPP TS 24.424 [39], OMA OMA-TS-XDM_MO-V1_1-20080627-A [41] and OMA-DDS-DM_ConnMO-V1_0-20081107-A [38]:

Identifier: '6FFC'	Structure: BER-TLV	Optional
File size: X bytes	Update activity: low	
Access Conditions: READ PIN UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1-X	XCAP_conn_params_policy data object	M	X bytes

Data object tags:

Data objects	Tag Values	Coding
XCAP_conn_params_policy	'80'	As specified below.

Coding of the XCAP_conn_params_policy data object:

Coding of the XCAP_conn_params_policy data object

Length	Description	Value	Status
1 byte	XCAP_conn_params_policy TLV TAG	'A0'	M
X bytes	Length of XCAP_conn_params_policy		M
1	AccessForXCAP Tag	'81'	M
1	AccessForXCAP Length	-	M
1	AccessForXCAP	-	M
1	Number of XCAP connection parameters policy part TLV's Tag	'82'	M
1	Number of XCAP connection parameters policy part TLV's Length	-	M
1	Number of XCAP connection parameters policy part TLV's	-	M
1	XCAP connection parameters policy part TLV	'A1'	M

Coding of the AccessForXCAP

Contents:

Contains an access type used for XCAP.

Coding:

See 3GPP TS 24.424 [39] AccessForXCAP leaf for coding.

Coding Number of XCAP connection parameters policy part TLV's

Contents:

Contains the number of instances of the XCAP connection parameters policy part TLV container.

The following fields may appear multiple times

XCAP connection parameters policy part:

Coding of the XCAP connection parameters object TLV container

Length	Description	Value	Status
1	XCAP connection parameters policy part TLV	'A1'	M
Y bytes	Length XCAP connection parameters policy part		M
1	Access Tag	'81'	M
1	Access Length		
1	Access		
1	Application name Tag	'82'	O
1 or 2	Length Application name		
A bytes	Application name		
1	Provider-ID Tag	'83'	O
1 or 2	Length Provider ID		
B bytes	Provider ID		
1	URI Tag	'84'	M
1 or 2	Length URI		
C bytes	URI		
1	XCAP Authentication User Name Tag	'85'	O
1 or 2	Length XCAP Authentication User Name		
D bytes	XCAP Authentication User Name		
1	XCAP Authentication Password Tag	'86'	O
1 or 2	Length XCAP Authentication Password		
E bytes	XCAP Authentication Password		
1	XCAP Authentication type Tag	'87'	O
1	Length XCAP Authentication type		
1	XCAP Authentication type		
1	Address Type Tag	'88'	O
1	Length Address Type		
F bytes	Address Type		
1	Address Tag	'89'	O
1 or 2	Length Address		
G bytes	Address		
1	PDPAuthenticationType Tag	'8A'	O
1	Length PDPAuthenticationType		
1	PDPAuthenticationType		
1	PDPAuthentication Name Tag	'8B'	O
1 or 2	Length PDPAuthentication Name		
I bytes	PDPAuthentication Name		
1	PDPAuthentication secret Tag	'8C'	O
1 or 2	Length PDPAuthentication secret		
J bytes	PDPAuthentication secret		

Coding of the Access

Contents:

Contains an access identifier.

Coding:

See 3GPP TS 24.424 [39] Access leaf for coding.

Coding of the Application name

Contents and coding see:

See OMA OMA-TS-XDM_MO-V1_1-20080627-A [41] Name leaf for coding.

Coding of the Provider-ID

Contents and coding see:

See OMA OMA-TS-XDM_MO-V1_1-20080627-A [41] ProviderID leaf for coding.

Coding of the URI

Contents and coding see:

See OMA OMA-TS-XDM_MO-V1_1-20080627-A [41] URI leaf for coding.

Coding of the XCAP Authentication User Name

Contents and coding see:

See OMA OMA-TS-XDM_MO-V1_1-20080627-A [41] AAUTHNAME leaf for coding.

Coding of the XCAP Authentication Password

Contents and coding see:

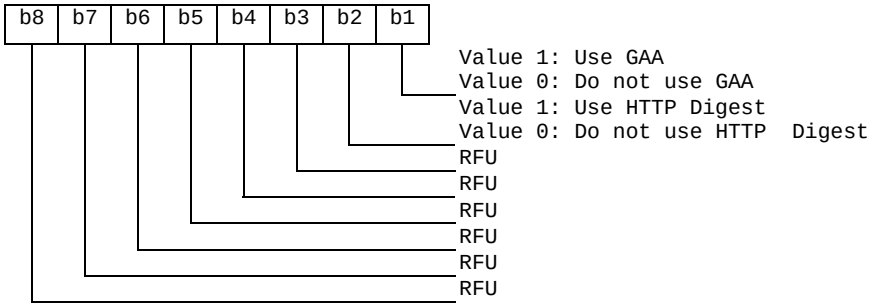
See OMA OMA-TS-XDM_MO-V1_1-20080627-A [41] AAUTHSECRET leaf for coding.

Coding of the XCAP Authentication type

Contents and coding see:

See OMA OMA-TS-XDM_MO-V1_1-20080627-A [41] AAUTHTYPE leaf for authentication types allowed:

.



Coding of the Address type

Contents and coding see:

See OMA-DDS-DM_ConnMO-V1_0-20081107-A [38] AddrTyoe leaf node and OMA-DDS-DM_ConnMO_3GPPPS-V1_0-20081024-A [37] clause 6.2 AddrType for coding.

Coding of the Address

Contents and coding see:

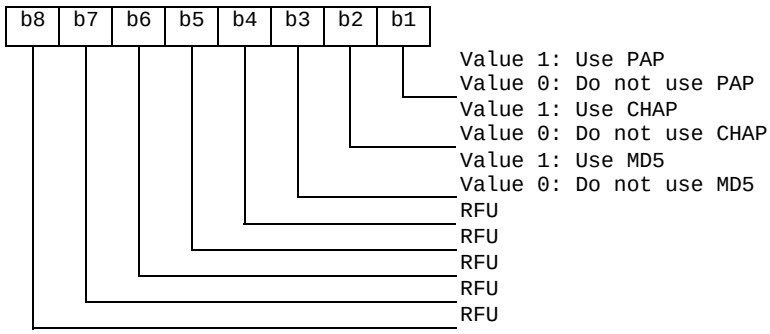
See OMA-DDS-DM_ConnMO-V1_0-20081107-A [38] Addr leaf node and OMA-DDS-DM_ConnMO_3GPPPS-V1_0-20081024-A [37] clause 6.2 AddrType for coding.

Coding of the PDPAuthentication type

Contents and coding see:

See OMA-DDS-DM_ConnMO-V1_0-20081107-A [38] AuthInfo/AuthType leaf node and OMA-DDS-DM_ConnMO_3GPPPS-V1_0-20081024-A [37] clause 6.2 AuthType for authentication types allowed.

.



`

Coding of the PDPAuthentication Name

Contents and coding see:

See OMA-DDS-DM_ConnMO-V1_0-20081107-A [38] AuthInfo/AuthName leaf node leaf for coding.

Coding of the PDPAuthentication Secret

Contents and coding see:

See OMA-DDS-DM_ConnMO-V1_0-20081107-A [38] AuthInfo/AuthSecret leaf node leaf for coding.

4.2.20 $EF_{WebRTCURI}$ (WebRTC URI)

If service n°20 is "available", this file shall be present.

This EF contains URI of the WWSF.

Identifier: '6FFA'	Structure: linear fixed	Optional
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:

  - URI of the WebRTC WWSF.

  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'.

4.2.21 $EF_{MuDMiDConfigData}$ (MuD and MiD Configuration Data)

If service n°21 is "available", this file shall be present.

This EF contains the Multi-Device and Multi-Identity configuration data object as specified in 3GPP TS 24.175 [44]:

Identifier: '6FFE'	Structure: BER-TLV	Optional
File size: X bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
N/A	MuD_and_MiD_configuration_data encoding	M	3 bytes
N/A	MuD_and_MiD_configuration_data	O	Y

Data object tags:

Data objects	Tag Values	Coding
MuD_and_MiD_configuration_data encoding	'80'	As specified below.
MuD_and_MiD_configuration_data	'81'	

Coding of the MuD_and_MiD_configuration_data encoding object

Coding of the MuD_and_MiD_configuration_data encoding object

Length	Description	Value	Status
1 byte	MuD_and_MiD_configuration_data encoding object Tag	'80'	M
1 byte	MuD_and_MiD_configuration_data encoding object Length	1	M
1 byte	MuD_and_MiD_configuration_data encoding object	-	M

Contents:

Indicates the coding used for all the MuD and Mid configuration objects stored in the $EF_{IMSConfigData}$.

Coding:

A value of '00' indicates the XML format described in 3GPP TS 24.175 [44]. All other values are reserved.

MuD_and_MiD_configuration_data object

Coding of the MuD_and_MiD_configuration_data object

Length	Description	Value	Status
1 byte	MuD_and_MiD_configuration_data object Tag	'81'	M
X bytes	MuD_and_MiD_configuration_data object Length	Y	M
Y bytes	MuD_and_MiD_configuration_data object	-	M

Contents:

Contains the management object as specified in 3GPP TS 24.175 [44].

Coding:

As specified in the MuD_and_MiD_configuration_data encoding object above.

4.2.22 $EF_{AC\_GBAUAPI}$ (Access Control to GBA_U_API)

If service n°2 is "available", this file shall be present.

This EF contains the list of Applet AID associated with a NAF_ID and indicates the Applet allowed to access to GBA_U API defined in 3GPP TS 31.130[46] and using Ks_int_NAF associated to specified NAF_ID.

Identifier: '6F0A'	Structure: Linear fixed	Optional
Record length: Z>7 bytes	Update activity: low	
Access Conditions: READ ADM UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to Z	Applet NAF Access Control TLV objects	M	Z bytes

Applet NAF Access Control TLV object parameters tags:

Description	Tag Value
Applet NAF Access Control TLV object Tag	'80'

Applet NAF Access Control TLV object contains:

Description	Value	M/O	Length (bytes)
Applet NAF Access Control TLV object tag	'80'	M	1
Length	Note 1	M	Note 2
Length	X	M	Note 2
AID value	--	M	5-16bytes
Length	Y	M	Note 2
NAF_ID value	--	M	Y
Note 1: This is the total size of the constructed TLV object. Note 2: The length is coded according to ISO/IEC 8825-1 [35].			

Note: The use of this EF is described in 3GPP TS 31.130[46]

4.2.23 EF_{IMSDCI} (IMS Data Channel Indication)

If service n°22 is "available", this file shall be present.

This EF contains an indication to the ME for IMS Data Channel.

Identifier: '6F0B'	Structure: transparent	Optional
File size: 1 byte	Update activity: low	
Access Conditions: READ PIN UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1	IMS DC Establishment Indication	M	1 byte

- IMS DC Establishment Indication:
  Contents:
  - IMS Data Channel Establishment Indication

  Coding:
  - '00' - IMS data channel is not allowed
  - '01' - IMS data channel is allowed but not allowed to be setup simultaneously while establishing an IMS session
  - '02' - IMS data channel is allowed and allowed to be setup simultaneously while establishing an IMS session

- All other values are RFU

NOTE: See Management object as defined in 3GPP TS 24.275[47].

4.3 ISIM file structure

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

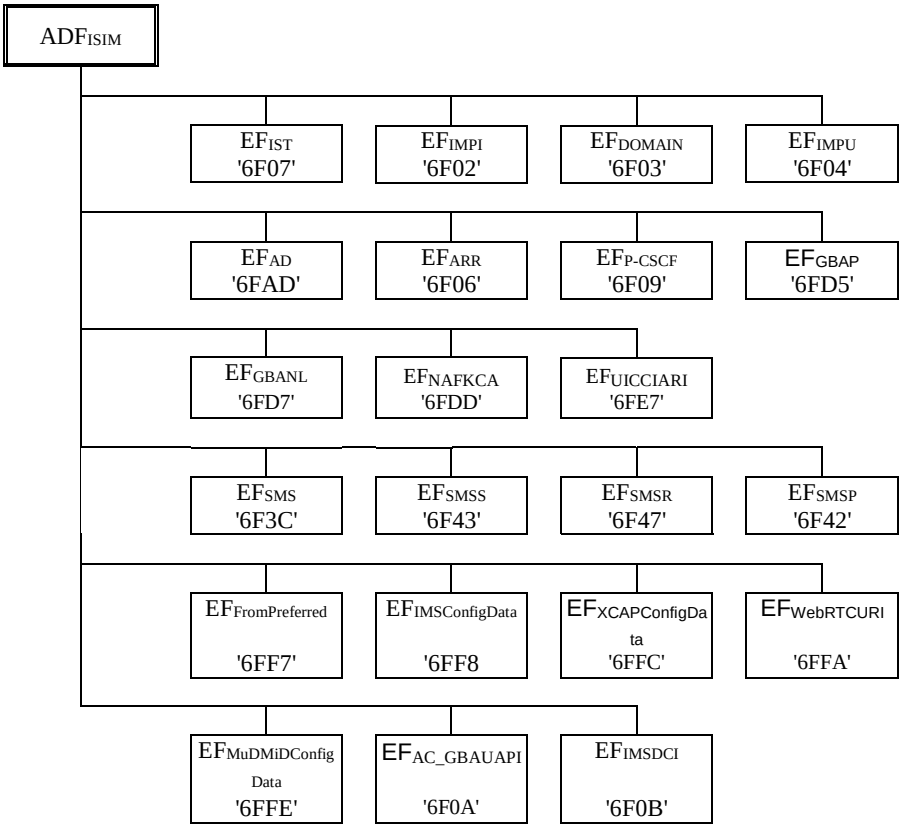


Figure 1: File identifiers and directory structures of ISIM

NOTE: The value '6FF9' under ADF_{ISIM} was used in earlier versions of this specification, and should not be re-assigned in future versions.

4.4 Contents of EFs at the TELECOM level

The EFs in the Dedicated File $DF_{TELECOM}$ contain service related information as defined in TS 31.102 [2].

The structure of DF TELECOM is defined in TS 31.102 [2].

4.4.1 $EF_{PSISMSC}$ (Public Service Identity of the SM-SC)

If service n°8 is "available", this file shall be present.

Coding and usage of this EF is defined in TS 31.102 [2].

This EF can be found in DF TELECOM with an identifier equal to '6FE5' as defined in TS 31.102 [2].

4.5 Contents of DFs at the TELECOM level

DFs may be present as child directories of $DF_{TELECOM}$ as defined in 3GPP TS 31.102 [2].

If service nº15 is "available", DF_{MCS} as defined in 3GPP TS 31.102 [2] shall be present.

4.5.1 Contents of files at the DF_{MCS} level

The EFs in the Dedicated File DF_{MCS} contain management objects related to Mission Critical Services, as specified in 3GPP TS 24.483 [432].

The coding, usage and conditions for presence for these EFs are defined in 3GPP TS 31.102 [2].

5 Application protocol

The requirements stated in the corresponding clause of TS 31.101 [3] apply to the ISIM application.

The procedures listed in clause "ISIM management procedures" are required for execution of the procedures in the subsequent clause "ISIM security related procedures". The procedures authentication procedure, IMPI request, IMPU request and SIPdomain request, which are listed in clause "ISIM security related procedures" are mandatory. If an ISIM Service table is available, the additional procedures are only executable if these services are indicated as "service available" in the ISIM Service table. However, if the procedures are implemented, it shall be in accordance with clause " ISIM security related procedures".

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 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 TS 31.101 [3].

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.

5.1.1.2 ISIM initialisation

The ISIM shall not indicate any language preference. It shall use the language indicated by any other application currently active on the UICC or by default, choose a language from EF_{PL} at the MF level according the procedure defined in TS 31.101 [3].

If the terminal does not support the languages of EF_{PL}, then the terminal shall use its own internal default selection.

The Terminal then runs the user verification procedure. If the procedure is not performed successfully, the ISIM initialisation stops.

Then the Terminal performs the administrative information request.

If all these procedures have been performed successfully then the ISIM session shall start. In all other cases the ISIM session shall not start.

After the previous procedures have been completed successfully, the Terminal runs the following procedures:

- IMPI request.
- IMPU request.
- SIP Domain request.
- ISIM Service Table request. If the ISIM Service Table is not present, the terminal shall assume that no optional services are available.
- P-CSCF address request

After the ISIM initialisation has been completed successfully, the Terminal is ready for an ISIM session and shall indicate this to the ISIM by sending a particular STATUS command.

5.1.2 ISIM Session termination

NOTE 1: This procedure is not to be confused with the deactivation procedure in TS 31.101 [3].

The ISIM session is terminated by the Terminal as follows.

The Terminal shall indicate to the ISIM by sending a particular STATUS command that the termination procedure is starting.

Finally, the ME deletes all these subscriber related information elements from its memory.

NOTE 2: If the Terminal has already updated any of the subscriber related information during the ISIM session, and the value has not changed until ISIM session termination, the Terminal may omit the respective update procedure.

To actually terminate the session, the Terminal shall then use one of the mechanisms described in TS 31.101 [3].

5.1.3 ISIM application closure

After termination of the ISIM session as defined in clause 5.1.2, the ISIM application may be closed by closing the logical channels that are used to communicate with this particular ISIM application.

5.1.4 UICC presence detection

The Terminal checks for the presence of the UICC according to TS 31.101 [3] within all 30 s periods of inactivity on the UICC-Terminal interface during a IMS session. If the presence detection according to TS 31.101 [3] fails the session shall be terminated as soon as possible but at least within 5s after the presence detection has failed.

5.1.5 Administrative information request

The Terminal performs the reading procedure with EF_{AD}.

5.2 ISIM security related procedures

5.2.1 Authentication procedure

The Terminal selects an ISIM application and uses the AUTHENTICATE command (see clause 7.1). The response is sent to the Terminal (in case of the T=0 protocol when requested by a subsequent GET RESPONSE command).

5.2.2 IMPI request

The Terminal performs the reading procedure with $EF_{IMPI.}$

5.2.3 IMPU request

The Terminal performs the reading procedure with EF_{IMPU}.

5.2.4 SIP Domain request

The Terminal performs the reading procedure with EF_{DOMAIN}.

5.2.5 Void

5.2.6 ISIM Service Table request

Requirement: ISIM Service Table available in the ISIM

Request: The ME performs the reading procedure with EF_{IST}.

5.2.7 P-CSCF address request

Requirement: ISIM Service n°1 and/or ISIM Service n°5 "available".

Request: The ME performs the reading procedure with $EF_{P\text{-}CSCF}$.

5.2.8 Generic Bootstrapping architecture (Bootstrap)

Requirement: ISIM Service n°2 "available".

The Terminal uses the AUTHENTICATE command in GBA security context (Bootstrapping Mode) (see 7.1.1). The response is sent to the Terminal.

After a successful GBA_U Procedure, the Terminal shall update the B-TID field and the Key Life Time field in EF_{GBABP}.

5.2.9 Generic Bootstrapping architecture (NAF Derivation)

Requirement: ISIM Service n°2 "available".

The Terminal shall first read EF_{GBABP}. The Terminal then uses the AUTHENTICATE command in GBA security context (NAF Derivation Mode) (see 7.1.1). The response is sent to the Terminal.

5.2.10 HTTP-Digest security request

Requirement: ISIM Service n°3 "available".

This HTTP-Digest security request does not apply for 3GPP and shall not be used by a terminal using a 3GPP access network or a 3GPP Interworking WLAN.

5.2.11 NAF Key Centre Address request

Requirement: Service n°2 and service n°4 "available".

Request: The ME performs the reading procedure with EF_{NAFKCA}.

5.3 Subscription related procedures

5.3.1 SM-over-IP

Requirement: Service n°8 "available".

Request: the ME performs the reading procedure with $EF_{PSISMSC}$.

Update: The ME performs the updating procedure with $EF_{PSISMSC}$.

5.3.2 Communication Control for IMS by ISIM

Requirement: ISIM Service n°9 "available".

The procedures and commands for Communication Control for IMS by ISIM are the same as Communication Control for IMS by USIM defined in TS 31.111 [31]. It is mandatory for the ME to perform the procedures if it has indicated that it supports Communication Control for IMS by USIM in the TERMINAL PROFILE command.

5.3.3 UICC access to IMS

Requirement: Service n°10 "available.

Request: The terminal performs the reading procedure with $EF_{UICCIARI}$.

The procedures and command for "UICC access to IMS" are defined in TS 31.111 [31]. An ME supporting UICC access to IMS shall perform the reading procedure with $EF_{UICCIARI}$ prior to sending a registration to the IMS.

5.3.4 From Preferred related procedures

Requirement: service n°17 is "available" in the ISIM Service Table.

Request: The ME performs the reading procedure with $EF_{FromPreferred}$. The UE then shall use the From Preferred value in the $EF_{FromPreferred}$ as described in 3GPP TS 24.607 [34] clause 4.5.2.12.

5.3.5 IMS Configuration Data related procedures

Requirement: service n°18 is "available" in the ISIM Service Table.

Request: The ME may perform the reading procedure with $EF_{IMSConfigData}$. If the ME performs the reading procedure with $EF_{IMSConfigData}$, the UE shall use the IMS Configuration Data in the $EF_{IMSConfigData}$ as described in 3GPP TS 24.229 [32] clause L.2.2.5.1D and 3GPP TS 24.229 [32] clause 6.1.1.

5.3.6 XCAP Configuration Data related procedures

Requirement: service n°19 is "available" in the ISIM Service Table.

Request: The ME may perform the reading procedure with $EF_{XCAPConfigData}$. If the ME performs the reading procedure with $EF_{XCAPConfigData}$, the UE shall use the $EF_{XCAPConfigData}$ as described in TS 24.623 [40] clause 5.2.1.3 and TS 24.623 [40] clause B.2.

5.4 MCS related procedures

Requirement: ISIM Service n°15 "available".

The MCS related procedures by ISIM are the same as MCS related procedures by USIM defined in 3GPP TS 31.102 [2].

5.5 WebRTC related procedures

Requirement: ISIM Service n°20 "available".

Request: The ME may perform the reading procedure with $EF_{WebRTCURI.}$

5.6 IMS DC Establishment indication procedures

5.6.1 IMS DC Establishment indication procedure

Requirement: Service n°22 is "available".

Request: The ME performs the reading procedure with EF_{IMSDCI}.

The ME shall follow the procedures as specified in 3GPP TS 24.186[48].

6 Security features

The security aspects of IMS are specified in 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.

6.1 User verification and file access conditions

The security architecture as defined in 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 TS 31.101 [3].
- For access to $DF_{TELECOM}$ the PIN shall be verified.
- The only valid usage qualifier is '08' which means user authentication knowledge based (PIN) as defined in ISO/IEC 7816-4 [6].

7 ISIM Commands

The commands specified in TS 31.101 [3] are supported by ISIM, with the restrictions identified in this clause.

7.1 AUTHENTICATE

7.1.1 Command description

The function can be used in several different contexts:

- an IMS AKA security context during the procedure for authenticating the ISIM to its HN and vice versa when IMS AKA authentication data are available. The function shall be used whenever an IMS context shall be established, i.e. when the terminal receives a challenge from the IMS. A cipher key and an integrity key are calculated. For the execution of the command the ISIM uses the subscriber authentication key K, which is stored in the ISIM.
- a HTTP Digest security context, when HTTP Digest authentication data are available. Digest authentication operations are described in IETF RFC 2617 [26].
- a GBA_U security context, when a GBA bootstrapping procedure is requested. In this context the function is used in two different modes:
  a) Bootstrapping Mode: during the procedure for mutual authenticating of the ISIM and the Bootstrapping Server Function (BSF) and for deriving Bootstrapped key material from the AKA run.
  b) NAF Derivation Mode: during the procedure for deriving Network Application Function (NAF) specific keys from previous bootstrapped key material.
- a Local Key Establishment security context, when a Local Key Establishment procedure is requested.

The function is related to a particular ISIM and shall not be executable unless the ISIM application has been selected and activated, and the current directory is the ISIM ADF or any subdirectory under this ADF and a successful PIN verification procedure has been performed (see clause 5).

7.1.1.1 IMS AKA security context

The ISIM first computes the anonymity key AK = $f5_K$ (RAND) and retrieves the sequence number SQN = (SQN ⊕ AK) ⊕ AK.

Then the ISIM computes XMAC = $f1_K$ (SQN || RAND || AMF) and compares this with the MAC which is included in AUTN. If they are different, the ISIM abandons the function.

Next the ISIM verifies that the received sequence number SQN is previously unused. If it is unused and its value is lower than SQN_{MS}, it shall still be accepted if it is among the last 32 sequence numbers generated. A possible verification method is described in TS 33.102 [4].

NOTE: This implies that the ISIM has to keep a list of the last used sequence numbers and the length of the list is at least 32 entries.

If the ISIM detects the sequence numbers to be invalid, this is considered as a synchronisation failure and the ISIM abandons the function. In this case the command response is AUTS, where:

- $AUTS = Conc(SQN_{MS}) \,||\, MACS$;
- $Conc(SQN_{MS}) = SQN_{MS} \oplus f5^*_K(RAND)$ is the concealed value of the counter SQN_{MS} in the ISIM; and
- $MACS = f1^*_K(SQN_{MS} \,||\, RAND \,||\, AMF)$ where:
- *RAND* is the random value received in the current user authentication request;

the AMF assumes a dummy value of all zeroes so that it does not need to be transmitted in clear in the resynchronisation message.

If the sequence number is considered in the correct range, the ISIM computes RES = $f2_K$ (RAND), the cipher key CK = $f3_K$ (RAND) and the integrity key IK = $f4_K$ (RAND) and includes these in the command response. Note that if this is more efficient, RES, CK and IK could also be computed earlier at any time after receiving RAND.

The use of AMF is HN specific and while processing the command, the content of the AMF has to be interpreted in the appropriate manner. The AMF may e.g. be used for support of multiple algorithms or keys or for changing the size of lists, see TS 33.102 [4].

7.1.1.2 GBA security context (Bootstrapping Mode)

ISIM operations in GBA security context are supported if service n°2 is "available".

The ISIM receives the RAND and AUTN*. The ISIM first computes the anonymity key AK = $f5_K$ (RAND) and retrieves the sequence number SQN = (SQN ⊕ AK) ⊕ AK.

The ISIM calculates IK = $f4_K$ (RAND) and MAC (by performing the MAC modification function described in TS 33.220 [25]). Then the ISIM computes XMAC = $f1_K$ (SQN || RAND || AMF) and compares this with the MAC previously produced. If they are different, the ISIM abandons the function.

Then the ISIM performs the remaining checking of AUTN* as in IMS security context. If the ISIM detects the sequence numbers to be invalid, this is considered as a synchronisation failure and the ISIM abandons the function. In this case the command response is AUTS, which is computed as in ISIM security context.

If the sequence number is considered in the correct range, the ISIM computes RES = $f2_K$ (RAND) and the cipher key CK = $f3_K$ (RAND).

The ISIM then derives and stores GBA_U bootstrapped key material from CK, IK values. The ISIM also stores RAND in the RAND field of EF_{GBABP}

The ISIM stores GBA_U bootstrapped key material from only one bootstrapping procedure. The previous bootstrapped key material, if present, shall be replaced by the new one. This key material is linked with the data contained in EF_{GBABP} : RAND, which is updated by the ISIM and B-TID, which shall be further updated by the ME.

NOTE: According to TS 33.220 [25], NAF-specific keys that may be stored on the ISIM are not affected by this bootstrapping operation.

RES is included in the command response after flipping the least significant bit.

Input:

- RAND, AUTN*

Output:

- RES

or

- AUTS

7.1.1.3 GBA security context (NAF Derivation Mode)

ISIM operations in GBA security context are supported if service n°2 is "available".

The ISIM receives the NAF_ID.

The ISIM performs Ks_ext_NAF and Ks_int_NAF derivation as defined in TS 33.220 [25] using the key material from the previous GBA_U bootstrapping procedure and the IMPI value from EF_{IMPI}

If no key material is available this is considered as a GBA Bootstrapping failure and the ISIM abandons the function. The status word '6985' (Conditions of use not satisfied) is returned.

Otherwise, the ISIM stores Ks_int_NAF and associated B-TID together with NAF_ID in its memory. The Ks_int_NAF keys related to other NAF_IDs, which are already stored in the ISIM, shall not be affected. The ISIM updates EF_{GBANL} as follows:

- If a record with the given NAF_ID already exists, the ISIM updates the B-TID field of this record with the B-TID value associated to the GBA_U bootstrapped key involved in this GBA_U NAF derivation procedure.
- If a record with the given NAF_ID does not exist, the ISIM uses an empty record to store the NAF_ID and the B-TID value associated to the GBA_U bootstrapped key involved in this GBA_U NAF Derivation procedure.

NOTE: According to TS 33.220 [25], the ISIM can contain several Ks_int_NAF together with the associated B-TID and NAF_ID, but there is at most one pair of Ks_int_NAF and associated B-TID stored per NAF_ID.

- In case no empty record is available the ISIM shall overwrite an existing record to store the NAF_ID and the B-TID value associated to the GBA_U bootstrapped key involved in this GBA_U NAF Derivation procedure. To determine the record to overwrite, the ISIM shall construct a list of record numbers by storing in the list first position the record number of the last used (i.e. involved in an Authentication command) or derived Ks_int_NAF and by shifting down the remaining list elements. The last record number in this list corresponds to the record to overwrite when the ISIM runs out of free records. If an existing record corresponding to a Ks_int_NAF key in use is overwritten, the application Ks_int_NAF shall not be affected.

Then, the ISIM returns Ks_ext_NAF.

Input:

- NAF_ID

Output:

- Ks_ext_NAF

7.1.1.4 HTTP-Digest security context

ISIM operations in HTTP-Digest security context are supported if service n°3 is "available".

7.1.1.5 Local Key Establishment security context (Key Derivation mode)

ISIM operations in this security context are supported if service n°2 and service n°4 are "available".

The ISIM receives the NAF_ID corresponding to the NAF Key Centre, the Terminal_ID, the Terminal_appli_ID, the UICC_appli_ID, RANDx, the Counter Limit value and the MAC as described in TS 33.110 [28].

The ISIM uses the NAF_ID to identify the Ks_int_NAF associated to the NAF Key Centre. If no valid Ks_int_NAF is available, this is considered as a Key Establishment failure and the ISIM abandons the function. The status word '6A88' (Referenced data not found) is returned.

If the Ks_local key derivation is not authorized by the local UICC policy (e.g. Terminal_appli_ID/UICC_appli_ID association not authorized or Terminal_ID value not authorized), the ISIM abandons the function. The status word '6985' (Conditions of use not satisfied) is returned.

Otherwise, the ISIM retrieves the appropriate Ks_int_NAF, derives Ks_local as described in TS 33.110 [28]. The ISIM verifies the MAC value received from the Terminal as described in TS 33.110 [28]:

- If the verification is unsuccessful, the ISIM abandons the function and returns the status word '9862' (Authentication error, incorrect MAC).
- If the verification is successful, the ISIM stores Ks_local and associated parameters Terminal_ID, Terminal_appli_ID, UICC_appli_ID, RANDx and the Ks_local Counter Limit. The ISIM returns the Local Key Establishment Operation Response TLV (indicating a successful Key Derivation operation) and a response MAC, which is derived as described in TS 33.110 [28].

The minimum number of Local keys that can be stored by the ISIM shall be defined by the service provider at the pre-issuance of the card.

In case the maximum number of Local Key was already reached or there is not enough available memory in the ISIM, the ISIM shall overwrite a Local Key and its associated data in order to store the new one. To determine the Ks_local to overwrite, the ISIM shall construct a list of Ks_local identifiers by storing in the list first position the Ks_local identifier of the last used or derived Ks_local and by shifting down the remaining list elements. The last Ks_local identifier in this list corresponds to the Ks_local to overwrite when the ISIM runs out of free memory or when the maximum number of Ks_local keys is reached. If an existing Ks_local in use is overwritten, the application using Ks_local shall not be affected.

Input:

Local Key Establishment Mode (Key Derivation mode), Counter Limit, request MAC, Key Identifier (i.e. NAF_ID, Terminal_ID, Terminal_appli_ID, UICC_appli_ID, RANDx)

Output:

- Key Derivation operation status, response MAC.

7.1.1.6 Local Key Establishment security context (Key Availability Check mode)

ISIM operations in this security context are supported if service n°2 and service n°4 are "available".

The ISIM receives a Ks_local identifier. The ISIM checks if a corresponding valid Ks_local is available. If a valid Ks_local key is available the Local Key Establishment Operation Response TLV (indicating a successful Key Availability Check operation) is returned. In case no valid Ks_local key is available the command fails and the status word '6A88' (Referenced data not found) is returned.

Input:

Local Key Establishment Mode (Key Availability Check mode), Key identifier (i.e. NAF_ID, Terminal_ID, Terminal_appli_ID, UICC_appli_ID, RANDx).

Output:

- Key Availability Check Operation Status.

7.1.2 Command parameters and data

This command can be used with an EVEN or an ODD instruction (INS) code. The EVEN instruction code can be used when the challenge data provided by the terminal is not TLV encapsulated data and the length of the challenge data provided by the terminal is less than 256 bytes.

The ODD instruction code shall be used with the security context specified in table 1, when challenge and response data is TLV encapsulated regardless of their length. Terminals and UICCs that do not support security context requiring TLV format (e.g. for Local Key Establishment), do not have to support AUTHENTICATE command with ODD instruction code.

EVEN INS code

Code	Value
CLA	As specified in TS 31.101 [3]
INS	'88'
P1	'00'
P2	See table below
Lc	See below
Data	See below
Le	'00', or maximum length of data expected in response

Parameter P2 specifies the authentication context as follows:

Coding of the reference control P2:

Coding b8-b1	Meaning
'1-------'	Specific reference data (e.g. DF specific/application dependent key)
'-XXXX---'	'0000'
'-----XXX'	Authentication context: 000 Reserved 001 IMS AKA 010 HTTP Digest 100 GBA context

All other codings are RFU.

ODD INS code

The authentication data and the authentication response data are encapsulated in BER-TLV objects structured using tag '73' for BER-TLV structured data and tag '53' otherwise.

How this command can chain successive blocks of authentication data, or authentication response data is described in TS 31 101 [3].

If P1 indicates "First block of authentication data" or "Next block of authentication data":

Input:

- Authentication data encapsulated in a BER-TLV data object.

Output:

- None.

Code	Value
CLA	As specified in TS 31.101 [3]
INS	'89'
P1	As specified in TS 31.101 [3]
P2	See table 1 below
Lc	Length of the subsequent data field
Data	Authentication related data
Le	Not present

If P1 indicates "First block of authentication response data" or "Next block of authentication response data":

Input:

- None.

Output:

- Authentication response data encapsulated in a BER-TLV data object.

Code	Value
CLA	As specified in TS 31.101 [3]
INS	'89'
P1	As specified in TS 31.101 [3]
P2	See table 1 below
Lc	Not present
Data	Not present
Le	Length of the response data

Parameter P1 is used to control the data exchange between the terminal and the UICC as defined in TS 31 101 [3].

Parameter P2 specifies the authentication context as follows:

Table 1: Coding of the reference control P2

Coding b8-b1	Meaning
'1-------'	Specific reference data (e.g. DF specific/application dependent key)
'----- XXX'	Authentication context: 110 Local Key Establishment mode

All other codings are RFU.

Command parameters/data:

7.1.2.1 IMS AKA security context

Byte(s)	Description	Length
1	Length of RAND (L1)	1
2 to (L1+1)	RAND	L1
(L1+2)	Length of AUTN (L2)	1
(L1+3) to (L1+L2+2)	AUTN	L2

The coding of AUTN is described in TS 33.102 [4]. The most significant bit of RAND is coded on bit 8 of byte 2. The most significant bit of AUTN is coded on bit 8 of byte (L1+3).

Response parameters/data, case 1, command successful:

Byte(s)	Description	Length
1	"Successful 3G authentication" tag = 'DB'	1
2	Length of RES (L3)	1
3 to (L3+2)	RES	L3
(L3+3)	Length of CK (L4)	1
(L3+4) to (L3+L4+3)	CK	L4
(L3+L4+4)	Length of IK (L5)	1
(L3+L4+5) to (L3+L4+L5+4)	IK	L5

The most significant bit of RES is coded on bit 8 of byte 3. The most significant bit of CK is coded on bit 8 of byte (L3+4). The most significant bit of IK is coded on bit 8 of byte (L3+L4+5).

Response parameters/data, case 2, synchronization failure:

Byte(s)	Description	Length
1	"Synchronisation failure" tag = 'DC'	1
2	Length of AUTS (L1)	1
3 to (L1+2)	AUTS	L1

The coding of AUTS is described in TS 33.102 [4]. The most significant bit of AUTS is coded on bit 8 of byte 3.

7.1.2.2 HTTP Digest security context

Byte(s)	Description	Length
1	Length of realm (L1)	1
2 to (L1+1)	Realm	L1
(L1+2)	Length of nonce (L2)	1
(L1+3) to (L1+L2+2)	Nonce	L2
(L1+L2+3)	Length of cnonce (L3)	1
(L1+L2+4) to (L1+L2+L3+3)	Cnonce	L3

The coding of realm, nonce and cnonce are described in IETF RFC 2617 [26].

Response parameters/data command successful:

Byte(s)	Description	Length
1	"HTTP Digest context reponse" tag = 'DB'	1
2	Length of Response(L4)	1
3 to (L4+2)	Response	L4
(L4+3)	Length of Session Key (L5)	1
(L4+4) to (L4+L5+3)	Session Key	L5

7.1.2.3 GBA security context (Bootstrapping Mode)

Byte(s)	Description	Length
1	"GBA Security Context Bootstrapping Mode" tag = 'DD'	1
2	Length of RAND (L1)	1
3 to (L1+2)	RAND	L1
(L1+3)	Length of AUTN (L2)	1
(L1+4) to (L1+L2+3)	AUTN	L2

Response parameters/data, GBA security context (Bootstrapping Mode), synchronisation failure:

Byte(s)	Description	Length
1	"Synchronisation failure" tag = 'DC'	1
2	Length of AUTS (L1)	1
3 to (L1+2)	AUTS	L1

AUTS coded as for IMS Security context.

Response parameters/data, GBA security context (Bootstrapping Mode), command successful:

Byte(s)	Description	Length
1	"Successful GBA operation" tag = 'DB'	1
2	Length of RES (L)	1
3 to (L+2)	RES	L

RES coded as for IMS Security context.

7.1.2.4 GBA security context (NAF Derivation Mode)

Byte(s)	Description	Length
1	"GBA Security Context NAF Derivation Mode" tag = 'DE'	1
2	Length of NAF_ID (L1)	1
3 to (L1+2)	NAF_ID	L1

Response parameters/data, GBA security context (NAF Derivation Mode), command successful:

Byte(s)	Description	Length
1	"Successful GBA operation" tag = 'DB'	1
2	Length of Ks_ext_NAF (L)	1
3 to (L+2)	Ks_ext_NAF	L

Coding of Ks_ext_NAF as described in TS 33.220 [25].

7.1.2.5 Local Key Establishment security context (All Modes)

The Local Key Establishment Control TLV is included in the command data to indicate the security context mode. The Local Key Establishment Control TLV is also included in the response data to indicate the operation status.

Table 2: Coding of the Local Key Establishment Control TLV

Tag Value	Length	Value / Meaning
'80'	Coded according to ISO/IEC 8825-1 [20]	Local Key Establishment context: '01': Key Derivation mode '02': Key Availability Check mode Operation Status: 'DB': Successful Operation

7.1.2.5.1 Local Key Establishment security context (Key Derivation mode)

Command parameters/data:

Byte(s)	Description	Coding	Length
1	Key Derivation Data Object tag ('73')	As defined in TS 31.101 [3] for BER-TLV data object	1
2 to A+1 bytes (A ≤ 4)	Key Derivation Data Object length (L)	As defined in TS 31.101 [3] for BER-TLV data object	A
A+2 to (A+L+1)	Key Derivation Data Object		L

- Key Derivation Data Object content: The TLVs defined in table 3 are included in the Key Derivation Data Object.

Table 3: Coding of the Key Derivation Data Object

Description	Value	M/O	Length (bytes)
Local Key Establishment Control TLV	Coded as defined in clause 7.1.2.5. The value field shall be set to '01'	M	B
Counter Limit tag	'81'	M	1
Length	C	M	Note 1
Counter Limit	Coded as defined in TS 33.110 [28]	M	C
Request MAC tag	'82'	M	1
Length	D	M	Note 1
Request MAC	Coded as defined in TS 33.110 [28]	M	D (see Note 3)
Key Identifier tag	'A0'	M	1
Length	E (see Note 2)	M	Note 1
NAF_ID tag	'83'	M	1
Length	F	M	Note 1
NAF_ID	Coded as defined in TS 33.220 [25]	M	F
Terminal_ID tag	'84'	M	1
Length	G	M	Note 1
Terminal_ID	Coded as defined in TS 33.110 [28]	M	G
Terminal_appli_ID tag	'85'	M	1
Length	H	M	Note 1
Terminal_appli_ID	Coded as defined in TS 33.110 [28]	M	H
UICC_appli_ID tag	'86'	M	1
Length	I	M	Note 1
UICC_appli_ID	Coded as defined in TS 33.110 [28]	M	I
RANDx tag	'87'	M	1
Length	J	M	Note 1
RANDx	Coded as defined in TS 33.110 [28]	M	J (see Note 4)

Note 1: The length is coded according to ISO/IEC 8825-1 [20]
Note 2: The Key Identifier TLV is a constructed TLV containing the following primitive TLVs: NAF_ID, Terminal_ID, Terminal_appli_ID, UICC_appli_ID and RANDx. E is the length of the constructed Key Identifier value.
Note 3: The most significant bit of the request MAC is coded on bit 8 of the first byte following the MAC Length.
Note 4: The most significant bit of the RANDx is coded on bit 8 of the first byte following the RANDx Length.

Response parameters/data, Local Key Establishment security context (Key Derivation mode), command successful:

Byte(s)	Description	Coding	Length
1	Key Derivation Operation Response Data Object tag ('73')	As defined in TS 31.101 [3] for BER-TLV data object	1
2 to A1+1 bytes (A1 ≤ 4)	Key Derivation Operation Response Data Object length (L1)	As defined in TS 31.101 [3] for BER-TLV data object	A1
A1+2 to (A1+L1+1)	Key Derivation Operation Response Data Object		L1

- Key Derivation Operation Response Data Object content: The TLVs defined in table 4 are included in the Key Derivation Operation Response Data Object.

Table 4: Coding of the Key Derivation Operation Response Data Object

Description	Value	M/O	Length (bytes)
Local Key Establishment Control TLV	Coded as defined in clause 7.1.2.5. The value field shall be set to 'DB'	M	B
Response MAC tag	'82'	M	1
Length	C	M	Note 1
Response MAC	Coded as defined in TS 33.110 [28]	M	C (see Note 2)
Note 1: The length is coded according to ISO/IEC 8825-1 [20] Note 2: The most significant bit of the response MAC is coded on bit 8 of the first byte following the MAC length.			

7.1.2.5.2 Local Key Establishment security context (Key Availability Check mode)

Command parameters/data:

Byte(s)	Description	Coding	Length
1	Key Availability Check Data Object tag ('73')	As defined in TS 31.101 [3] for BER-TLV data object	1
2 to 1+A bytes (A ≤ 4)	Key Availability Check Data Object length (L)	As defined in TS 31.101 [3] for BER-TLV data object	A
A+2 to (A+L+1)	Key Availability Check Data Object		L

- Key Availability Check Data Object content: The TLVs defined in table 5 are included in the Key Availability Check Data Object.

Table 5: Coding of the Key Availability Check Data Object

Description	Value	M/O	Length (bytes)
Local Key Establishment Control TLV	Coded as defined in clause 7.1.2.5. The value field shall be set to '02'	M	B
Key Identifier TLV	Coded as defined in clause 7.1.2.5.1	M	C

Response parameters/data, Local Key Establishment security context (Key Availability Check mode), command successful:

Byte(s)	Description	Coding	Length
1	Key Availability Check Operation Response Data Object tag ('73')	As defined in TS 31.101 [3] for BER-TLV data object	1
2 to 1+A1 bytes (A1 ≤ 4)	Key Availability Check Operation Response Data Object length (L1)	As defined in TS 31.101 [3] for BER-TLV data object	A1
A1+2 to (A1+L1+1)	Key Availability Check Operation Response Data Object		L1

- Key Availability Check Operation Response Data Object content: The TLV defined in table 6 is included in the Key Availability Check Operation Response Data Object.

Table 6: Coding of the Key Availability Check Operation Response Data Object

Description	Value	M/O	Length (bytes)
Local Key Establishment Control TLV	Coded as defined in clause 7.1.2.5. The value field shall be set to 'DB'	M	B

7.1.3 Status Conditions Returned by the ISIM

Status of the card after processing of the command is coded in the status bytes SW1 and SW2. This clause specifies coding of the status bytes in the following tables.

7.1.3.1 Security management

SW1	SW2	Error description
'98'	'62'	- Authentication error, incorrect MAC
'98'	'64'	- Authentication error, security context not supported

7.1.3.2 Status Words of the Commands

The following table shows for each command the possible status conditions returned (marked by an asterisk *).

Commands and status words

Status Words	AUTHENTICATE
90 00	*
91 XX	*
93 00	
98 50	
98 62	*
98 64	*
62 00	*
62 81	
62 82	
62 83	
62 F1	*
62 F3	*
63 CX	
63 F1	*
64 00	*
65 00	*
65 81	*
67 00	*
67 XX – (see note)	*
68 00	*
68 81	*
68 82	*
69 81	
69 82	*
69 83	
69 84	*
69 85	*
69 86	
6A 80	
6A 81	*
6A 82	
6A 83	
6A 86	*
6A 87	
6A 88	*
6B 00	*
6E 00	*
6F 00	*
6F XX – (see note)	*
NOTE: Except SW2 = '00'.	

7.2 GET CHALLENGE

The GET CHALLENGE command is optional for the ISIM application.

8 Void

Annex A (informative): EF changes via Data Download or USAT applications

This annex defines if changing the content of an EF by the network (e.g. by sending an SMS) or by a USAT Application is advisable. Updating of certain EFs "over the air" could result in unpredictable behaviour of the UE; these are marked "Caution" in the table below. Certain EFs are marked "No"; under no circumstances should "over the air" changes of these EFs be considered.

File identification	Description	Change advised
'6F02'	IMS private user identity	Caution (note 1)
'6F03'	Home Network Domain Name	Caution (note 1)
'6F04'	IMS public user identity	Caution (note 1)
'6FAD'	Administrative Data	Caution
'6F06'	Access Rule Reference	Caution
'6F07'	ISIM Service Table	Caution
'6F09'	P-CSCF address	Caution (note 1)
'6FD5'	GBA Bootstrapping parameters	Caution
'6FD7'	GBA NAF List	Caution
'6FDD'	NAF Key Centre Address	Caution
'6F3C'	Short messages	Yes
'6F42'	SMS parameters	Yes
'6F43'	SMS status	Yes
'6F47'	Short message status reports	Yes
'6FE5'	Public Service Identity of the SM-SC	Yes
'6FE7'	UICC IARI	Caution (note 2)
'6FF7'	From Preferred	Yes
'6FF8'	IMSConfigData	Caution (note 1)
'6FFC'	XCAP Configuration Data	Yes
'6FFA'	WebRTC URI	Yes
'6FFE'	MuD and MiD configuration data	Yes
'6F0A'	Access Control to GBA_U_API	Yes
'6F0B'	IMS DC Establishment Indication	Yes

NOTE 1: If EF_{IMPI}, EF_{IMPU}, EF_{DOMAIN}, P-CSCF or IMSConfigData are changed, the UICC should issue a REFRESH command.

NOTE 2: If $EF_{UICCIARI}$ is changed, the UICC shall issue a REFRESH command as defined in TS 31.111 [31]. The ME shall read the updated list of IARIs associated with active applications installed on the UICC.

Annex B (informative): Tags defined in 31.103

Tag	Name of Data Element	Usage
'80'	NAF_ID	EF_{GBANL}
'80'	NAI TLV data object	EF_{IMPI}
'80'	P-CSCF TLV data object	$EF_{P\text{-}CSCF}$
'80'	URI TLV data object	EF_{IMPU}, EF_{DOMAIN}, $EF_{WebRTCURI}$
'80'	XCAP_conn_params_policy TLV TAG	$EF_{XCAPConfigData}$
'80'	IMS configuration data encoding	$EF_{IMSConfigData}$
'80'	MuD_and_MiD_configuration_data encoding	$EF_{MuDMiDConfigData}$
'81'	IMS configuration data	$EF_{IMSConfigData}$
'81'	B-TID	EF_{GBANL}
'81'	MuD_and_MiD_configuration_data	$EF_{MuDMiDConfigData}$
'A0'	XCAP_conn_params_policy part tag The following tags are encapsulated within 'A0' '81' AccessForXCAP Tag '82' Number of XCAP connection parameters policy part TLV's Tag 'A1' XCAP connection parameters policy part tag	$EF_{XCAPConfigData}$
'A1'	XCAP connection parameters policy part tag The following tags are encapsulated within 'A1' '81' Access Tag '82' Application name Tag '83' Provider ID Tag '84' URI Tag '85' XCAP Authentication User Name Tag '86' XCAP Authentication password Tag '87'…XCAP Authentication type Tag '88'…Address type Tag '89'…Address Tag '8A'…PDP Authentication type Tag '8B'…PDP Authentication Name Tag '8C'…PDP Authentication Secret Tag	$EF_{XCAPConfigData}$
'DB'	Successful IMS authentication	Response to AUTHENTICATE"IMS AKA security context"
'DB'	HTTP Digest Context response	Response to AUTHENTICATE "HTTP Digest security context"
'DB'	Successful GBA operation	Response to AUTHENTICATE "GBA security context"
'DC'	Synchronisation failure	Response to AUTHENTICATE "IMS AKA security context" or "GBA security context (Bootstrapping Mode)"
'DD'	GBA Security Context Bootstrapping Mode	AUTHENTICATE "GBA security context"
'DE'	GBA Security Context NAF Derivation Mode	AUTHENTICATE "GBA security context"

NOTE: the value 'FF' is an invalid tag value. For ASN.1 tag assignment rules see ISO/IEC 8825-1 [20]

Annex C (informative): Suggested contents of the EFs at pre-personalization

If EFs have an unassigned value, it may not be clear from the main text what this value should be. This annex suggests values in these cases.

File Identification	Description	Value
'6F02'	IMS private user identity	'8000FF…FF'
'6F03'	Home Network Domain Name	'8000FF…FF'
'6F04'	IMS public user identity	'8000FF…FF'
'6FAD'	Administrative Data	Operator dependent
'6F06'	Access Rule Reference	Card issuer/operator dependent
'6FD5'	GBA Bootstrapping parameters	'FF…FF'
'6F07'	ISIM Service Table	Operator dependent
'6F09'	P-CSCF address	Operator dependent
'6FD7'	GBA NAF List	'FF…FF'
'6FDD'	NAF Key Centre Address	'FF…FF'
'6FE7'	UICC IARI	Operator dependent
'6FF7'	From Preferred	'00'
'6FF8'	IMSConfigData	Operator dependent
'6FFC'	XCAP Configuration Data	Operator dependent
'6FFA'	WebRTC URI	Operator dependent
'6FFE'	MuD and MiD Configuration Data	Operator dependent
'6F0A'	Access Control to GBA_U_API	Operator dependent
'6F0B'	IMS DC Establishment Indication	Operator dependent

Annex D (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
'6F02'	'02'	IMS private user identity
'6F03'	'05'	Home Network Domain Name
'6F04'	'04'	IMS public user identity
'6FAD'	'03'	Administrative Data
'6F06'	'06'	Access Rule Reference
'6F07'	'07'	ISIM Service Table

All other SFI values are reserved for future use.

Annex E (informative): ISIM Application Session Activation / Termination

The purpose of this annex is to illustrate the different Application Session procedures.

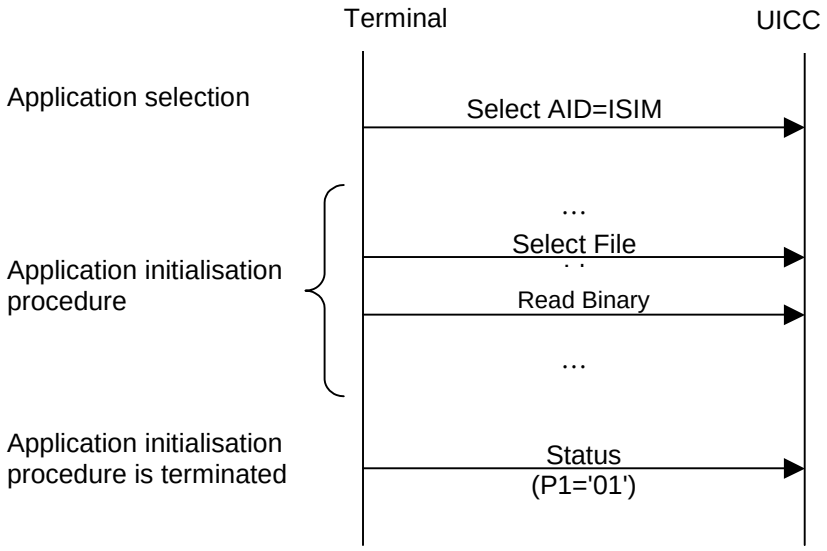


Figure E.1: ISIM Application Session Activation procedure

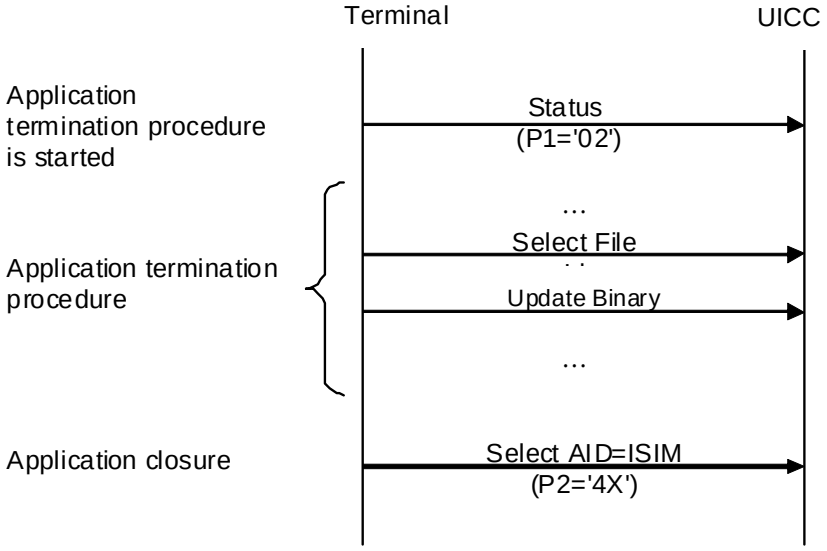


Figure E.2: ISIM Application Session Termination procedure

Annex F (informative): Change History

The table below indicates all CRs that have been incorporated into the present document since it was initially approved.

TSG #	TSG TD#	CR	Rev	Cat	Subject/Comment	New
TP-16	TP-020124	-	-	-	Initial version for information and approval in one step Comment: T#16 approved the specification to be part of Rel-5. The only changes to v1.0.0 are in the references clause for the reference in [16]	1.0.0
TP-17	TP-020211	001	-	F	Corrections	5.1.0
TP-18	TP-020281	002	-	F	Replace reference to TS 31.110 by reference to ETSI TS 101 220	6.0.0
TP-18	TP-020281	003	-	F	Management of last selected ISIM	
TP-18	TP-020281	004		D	Gather all 3GPP-specific card platform requirements into TS 31.101, and remove them from TS 31.103. NOTE: This CR created Rel-6 of TS 31.103.	
TP-19	TP-030019	006		F	Alignment with the Stage 2 terminology	6.1.0
TP-20	TP-030122	008		A	Clarification that the home operator's network domain name is a SIP URI.	6.2.0
TP-23	TP-040025	012			Essential corrections to remove Session Keys	6.3.0
TP-23	TP-040025	014			Creation of an ISIM Service Table	
TP-23	TP-040067	013			New EF for P-CSCF Addresses in ISIM	
TP-24	TP-040102	015		F	Clarification that the P-CSCF address shall not be used by a 3GPP terminal accessing a Interworking WLAN	6.4.0
TP-25	TP-040182	017		B	GBAU ME-ISIM interface	6.5.0
TP-25	TP-040182	016		B	New 3GPP2 IMS authentication context in ISIM	6.5.0
TP-26	TP-040257	019		B	Storage of the lifetime of the GBA_U bootstrapped keys	6.6.0
TP-26	TP-040257	021		F	Correction of non specific references	6.6.0
TP-27	TP-050019	022		A	Reservation of file IDs under ADF ISIM	6.7.0
TP-27	TP-050019	024		F	Completion of GBA_U-related procedures	6.7.0
TP-27	TP-050019	025		F	Storage of NAF-keys identifiers in GBA_U	6.7.0
CT-28	TP-050136	027		A	ISO/IEC 7816-series revision	6.8.0
CT-29	CP-050330	029	1	A	Default Record for EFIMPU	6.9.0
CT-29	CP-050335	030		F	Corrections of EFIST Service No. referencing	6.9.0
CT-29	CP-050335	031		F	Changes in Application Protocol due to the use of ISIM Service Table	6.9.0
CT-30	CP-050492	035		F	Subscription related procedures	6.10.0
CT-30	CP-050492	033		F	Encoding of IMPI, IMPU and Domain	6.10.0
CT-32	CP-060243	0036		F	Add missing EF in ISIM file structure	7.0.0
CT-32	CP-060243	0037		F	Update of the table summarizing the tags defined in 31.103	7.0.0
CT-33	CP-060386	0040	1		Correction of ISIM Service Table	7.1.0
CT-33	CP-060386	0043	1		Coding of P2	7.1.0
CT-36	CP-070294	0045	1	A	HTTP-Digest security request	7.2.0
CT-36	CP-070291	0048	-	A	Correction of coding of home network domain name in EF-DOMAIN	7.2.0
CT-36	CP-070465	0050	-	A	GBA NAF Keys storage policy	7.2.0
2007-06	-	-	-	-	MCC correction to CR0048 implementation (reference to [9])	7.2.1
CT-37	CP-070620	0051	2	B	Key Establishment mechanism: alignment with TS 33.110	7.3.0
CT-41	CP-080584	0055	1	A	Authentication of GBA	7.4.0
CT-41	CP-080585	0053	1	B	Introduction of support for IMS local breakout	8.0.0
-------	-	-	-	-	- correction of change history - correction of formatting in file structure (clause 4.3) - update of front cover/copyright/logos for LTE	8.0.1
CT-43	CP-090453	0057	-	A	IMS public user identity for emergency registration	8.1.0
CT-46	CP-091011	0065	1	F	References update	8.2.0
CT-46	CP-091012	0063	1	F	Correction to application session termination	9.0.0
--	--	--	--	--	Corrupted clauses numbering fixed	9.0.1
CT-49	CP-100585	0067	1	A	Introduction of a DF_TELECOM EF to support Public Service Identity for SMS over IP	9.1.0
CT-50	CP-100824	0068	-	B	Addition of CALL CONTROL indicator in the IST	10.0.0
CT-51	CP-110241	0071	1	A	Introduction of Data Download via SMS-PP service indication in EF IST	10.1.0
CT-51	CP-110306	0072	2	B	Introduction of the IARI list in the ISIM	10.1.0
SP-57					Automatic upgrade to Rel-11	11.0.0
CT-58	CP-120870	0080	1	F	Update of reference to ASN.1 coding specification	11.1.0
CT-58					Sanity check according to C6-120554 agreed at C6 #66.	11.1.0
CT-60	CP-130363	0081	1	C	Add support for 98 64 status words for AUTHENTICATE command	12.0.0
CT-63	CP-140163	0093		A	Correction of SMS storage procedures for ISIM	12.1.0
CT-64	CP-140424	0086	2	A	New UICC service in IST for URI support	12.2.0
CT-68	CP-150381	0094	1	B	URI support for SMS indicator in ISIM	13.0.0
CT-68	CP-150394	0095	2	B	Support of Enhanced IMS Call Control by ISIM	13.0.0
CT-72	CP-160350	0099		B	Addition of MCPTT configuration parameters	13.1.0
CT-74	CP-160789	0101	3	B	URI support for SMS-PP DOWNLOAD indicator in IST	14.0.0

CT-74	CP-160795	0105	1	B	Support of OIP OIR Policy Note: reference to 3GPP TS 24.417 not added during implementation as not used in the CR.	14.0.0
CT-74	CP-160820	0102	4	B	Default EPS bearer context usage restriction policy configuration	14.0.0
CT-75	CP-170166	0075		F	Geolocalization API document aligment	14.1.0
					Implementation error (Version updated)	14.1.1
CT-76	CP-171162	0112	1	B	New Emerg-request timer defined with configurable values	14.2.0
CT-76	CP-171162	0107	5	B	XCAP configuration parameters	14.2.0
CT-76	CP-171166	0108	1	B	Estimated P-CSCF recover time node	14.2.0
CT-77	CP-172066	0113	2	B	WebRTC Web Server Function discovery	15.0.0
CT-78	CP-173143	0109r4	4	B	Registration handling when VoPS not supported node	15.1.0
CT-78	CP-173135	0119	1	A	Correction of file ID for EFXCAPConfigData	15.1.0
CT78	CP-173136	0120	1	A	Propagation of MCPTT fixes to Rel-15	15.1.0
CT-79	CP-180128	0123	1	A	Removal of Estimated_P-CSCF_Recover_Time timer	15.2.0
CT-79	CP-180131	0124	1	B	Configuration parameter for handover between WLAN and EPS	15.2.0
CT-81	CP-182187	0126	2	B	Mission Critical Services configuration data update to ISIM	15.3.0
CT-82	CP-183142	0128	-	F	Default QoS flow usage restriction policy	15.4.0
CT-82	CP-183141	0129	2	F	New Timer for emergency call attempt in non-3GPP access	15.4.0
CT-82	CP-183141	0130	1	F	Correction on implementation of CR0125	15.4.0
2019-03	CP-190044	0132	-	A	Fix omission of SMS_Over_IP_Networks_Indication in EFIMSConfigData	15.5.0
2020-01					5G logo updated in a cover page as agreed in CT#86	15.5.1
2020-03	CP-200089	0133	1	B	Configuration file for MuD and MiD services	16.0.0
2020-09	CP-202130	0134	1	A	Update of spec. reference	16.1.0
2021-03	CP-210084	0136	-	B	Configuration of Handover parameters	17.0.0
2024-03	CP-240149	0141	1	B	Add EF of Access Control to GBA_U_APIs for the ISIM	18.0.0
2024-03	CP-240149	0140	1	B	Add EF of IMS Data Channel configuration to the ISIM	18.0.0
2024-06	CP-241215	0143		F	Correction of FID issues	18.1.0
2024-06	CP-241220	0142	2	C	Update EF of IMS Data Channel configuration on the ISIM	18.1.0
2024-09	CP-242087	0144	-	F	Correction of FIDs in Annex A and B	18.2.0
2025-10	-	-	-	-	Update to Rel-19 version (MCC)	**19.0.0**

History

Document history		
V19.0.0	October 2025	Publication