ETSI TS 131 103 V7.6.0 (2010-01)

Technical Specification

Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Characteristics of the IP Multimedia Services Identity Module (ISIM) application (3GPP TS 31.103 version 7.6.0 Release 7)

GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

Reference

RTS/TSGC-0631103v760

Keywords

GSM, UMTS

ETSI

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

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

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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

ETSI

Intellectual Property Rights

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

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

Foreword

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

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

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

Contents

Foreword

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

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

Version x.y.z

where:

    x   the first digit:

        1   presented to TSG for information;

        2   presented to TSG for approval;

        3   or greater indicates TSG approved document under change control.

    y   the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

    z   the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

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

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

1 Scope

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

The present document specifies:

- specific command parameters;

- file structures;

- contents of EFs (Elementary Files);

- security functions;

- application protocol to be used on the interface between UICC (ISIM) and Terminal.

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

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

2 References

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

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1]   3GPP TS 21.111: "USIM and IC Card Requirements".

[2]   3GPP TS 31.102: "Characteristics of the USIM Application".

[3]   3GPP TS 31.101: "UICC-Terminal Interface, Physical and Logical Characteristics".

[4]   3GPP TS 33.102: "3G Security; Security Architecture".

[5]   3GPP TS 33.103: "3G Security; Integration Guidelines".

[6]   ISO/IEC 7816-4: "Identification cards - Integrated circuit cards,Part 4: Organization, security and commands for interchange".

[7]   Void.

[8]   Void.

[9]   3GPP TS 23.003: "Numbering, Addressing and Identification".

[10]   Void.

[11]   Void.

[12]   3GPP TS 25.101: "UE Radio Transmission and Reception (FDD)".

[13]   3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[14]   3GPP TS 33.203: "3G security; Access security for IP-based services".

[15]   3GPP TS 24.228: "Signalling flows for the IP multimedia call control based on SIP and SDP; Stage 3".

[16]   IETF RFC 3261: "SIP: Session Initiation Protocol".

[17]   3GPP TS 23.038: "Alphabets and language-specific information".

[18]   ISO 639 (1988): "Code for the representation of names of languages".

[19]   3GPP TS 51.011 Release 4: "Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface".

[20]   ISO/IEC 8825(1990): "Information technology - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)" Second Edition.

[21]   3GPP TS 22.101: "Service aspects; Service principles".

[22]   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".

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
$\oplus$	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
ICC	Integrated Circuit Card
ID	IDentifier
IK	Integrity Key
IM	IP Multimedia
IMPI	IM Private Identity
IMPU	IM PUblic identity
IMS	IP Multimedia Subsystem
ISIM	IM Services Identity Module
K	long-term secret Key shared between the ISIM and the AuC
KSI	Key Set Identifier
LI	Language Indication
LSB	Least Significant Bit
MAC	Message Authentication Code
MF	Master File
MSB	Most Significant Bit
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
XRES	eXpected user RESponse

3.4 Coding Conventions

The following coding conventions apply to the present document.

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

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

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

4 Files

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

For an overview containing all files see figure 4.1.

4.1 Contents of the EFs at the MF level

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

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

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

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

4.2.1 Void

4.2.2 EF$_{IMPI}$ (IMS private user identity)

This EF contains the private user identity of the user.

Identifier: '6F02'		Structure: transparent		Mandatory
SFI: "02"				
File size: X bytes		Update activity: low		

Access Conditions:
    READ   PIN
    UPDATE   ADM
    DEACTIVATE   ADM
    ACTIVATE ADM				

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

- NAI

    Contents:

    - Private user identity of the user.

    Coding:

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

4.2.3 EF_{DOMAIN} (Home Network Domain Name)

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

Identifier: '6F03'	Structure: transparent		Mandatory
SFI: "05"			
File size: X bytes		Update activity: low	
Access Conditions: READ PIN UPDATE ADM DEACTIVATE ADM ACTIVATE ADM			
Bytes	Description	M/O	Length
1 to X	Home Network Domain Name TLV data object	M	X bytes

- URI

   Contents:

- Home Network Domain Name.

   Coding:

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

4.2.4 EF_{IMPU} (IMS public user identity)

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

Identifier: '6F04'	Structure: linear fixed		Mandatory
SFI: "04"			
Record length: X bytes		Update activity: low	
Access Conditions: READ PIN UPDATE ADM DEACTIVATE ADM ACTIVATE ADM			
Bytes	Description	M/O	Length
1 to X	URI TLV data object	M	X bytes

- URI

   Contents:

- SIP URI by which other parties know the subscriber.

   Coding:

- For contents and syntax of URI TLV data object values see IETF RFC 3261 [16]. The URI shall be encoded to an octet string according to UTF-8 encoding rules as specified in IETF RFC 3629 [27]. The tag value of the URI TLV data object shall be '80'.

4.2.5 EF$_{AD}$ (Administrative Data)

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

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

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

Access Conditions:
    READ   ALW
    UPDATE   ADM
    DEACTIVATE   ADM
    ACTIVATE ADM				

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

- UE operation mode:

    Contents:

    - mode of operation for the UE

    Coding:

    - Initial value

        - '00' normal operation.

        - '80' type approval operations.

        - '01' normal operation + specific facilities.

        - '81' type approval operations + specific facilities.

        - '02' maintenance (off line).

- Additional information:

    Coding:

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

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

RFU (see TS 31.101)
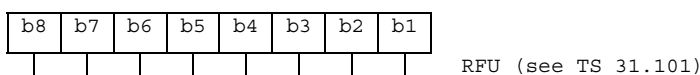
4.2.6 EF_{ARR} (Access Rule Reference)

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

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:

```
┌────┬────┬────┬────┬────┬────┬────┬────┐
│ b8 │ b7 │ b6 │ B5 │ b4 │ b3 │ b2 │ b1 │
└────┴────┴────┴────┴────┴────┴────┴────┘
                                    └── Service n°1
                               └─────── Service n°2
                          └──────────── Service n°3
                     └───────────────── Service n°4
                └────────────────────── Service n°5
           └─────────────────────────── Service n°6
      └──────────────────────────────── Service n°7
 └───────────────────────────────────── Service n°8
```

Second byte:

```
┌────┬────┬────┬────┬────┬────┬────┬────┐
│ b8 │ b7 │ b6 │ B5 │ b4 │ b3 │ b2 │ b1 │
└────┴────┴────┴────┴────┴────┴────┴────┘
                                    └── Service n°9
                               └─────── Service n°10
                          └──────────── Service n°11
                     └───────────────── Service n°12
                └────────────────────── Service n°13
           └─────────────────────────── Service n°14
      └──────────────────────────────── Service n°15
 └───────────────────────────────────── Service n°16
```
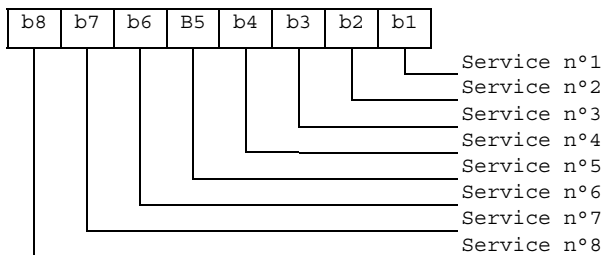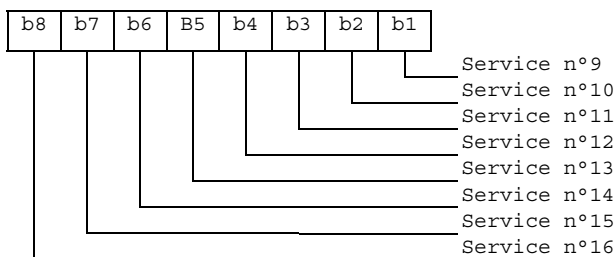
etc.

4.2.8 EF$_{P-CSCF}$ (P-CSCF Address)

If service n°1 is "available", this file shall be present.

This EF does not apply for 3GPP and shall not be used by a terminal using a 3GPP access network or a 3GPP Interworking WLAN.

NOTE: The current 3GPP procedures for P-CSCF discovery provide a flexible way for the UE to discover the P-CSCF address(es). Procedures include both GPRS PDP context based solution and a generic DHCP based approach that can be used for other access technologies.

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
0x00	FQDN
0x01	IPv4
0x02	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 0x00, 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 [13].

- 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 [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 [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].

4.3 ISIM file structure

This subclause contains a figure depicting the file structure of the ADF$_{ISIM}$. ADF$_{ISIM}$ shall be selected using the AID and information in EF$_{DIR}$.
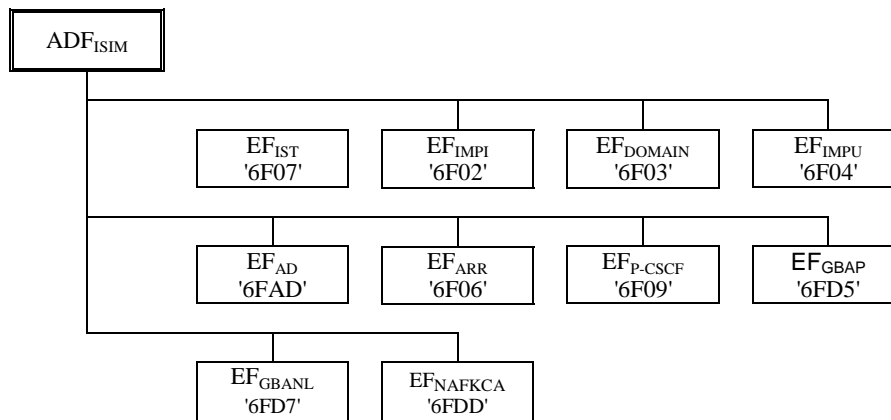

Figure 1: File identifiers and directory structures of ISIM

5 Application protocol

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

The procedures listed in subclause "ISIM management procedures" are required for execution of the procedures in the subsequent subclause "ISIM security related procedures". The procedures authentication procedure, IMPI request, IMPU request and SIPdomain request, which are listed in subclause "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 subclause " 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 subclause 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 subclause 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 "available".

Request: The ME performs the reading procedure with EF_{P-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 Derviation 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$_{NAFKCA}$.

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 referenceas 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 $SQN = (SQN \oplus AK) \oplus AK$.

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 $SQN = (SQN \oplus AK) \oplus AK$.

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
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 dependant 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 dependant 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 codings 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 [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 section 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 [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 section 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 [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 section 7.1.2.5. The value field shall be set to '02'	M	B
Key Identifier TLV	Coded as defined in section 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 section 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 subclause 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

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	*
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 behavior 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)
'6F03'	Home Network Domain Name	Caution (note)
'6F04'	IMS public user identity	Caution (note)
'6FAD'	Administrative Data	Caution
'6F06'	Access Rule Reference	Caution
"6F07"	ISIM Service Table	Caution
"6F09"	P-CSCF address	Caution (note)
'6FD5"	GBA Bootstrapping parameters	Caution
'6FD7"	GBA NAF List	Caution
'6FDD"	NAF Key Centre Address	Caution
NOTE: If EF_{IMPI}, EF_{IMPU}, EF_{DOMAIN} or P-CSCF are changed, the UICC should issue a REFRESH command.			

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$_{P-CSCF}$
'80'	URI TLV data object	EF$_{IMPU}$, EF$_{DOMAIN}$
'81'	B-TID	EF$_{GBANL}$
'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 [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 dependant
'6F06'	Access Rule Reference	Card issuer/operator dependant
'6FD5"	GBA Bootstrapping parameters	"FF…FF"
"6F07"	ISIM Service Table	Operator dependant
"6F09"	P-CSCF address	Operator dependant
"6FD7"	GBA NAF List	"FF…FF"
"6FDD"	NAF Key Centre Address	'FF…FF'

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.
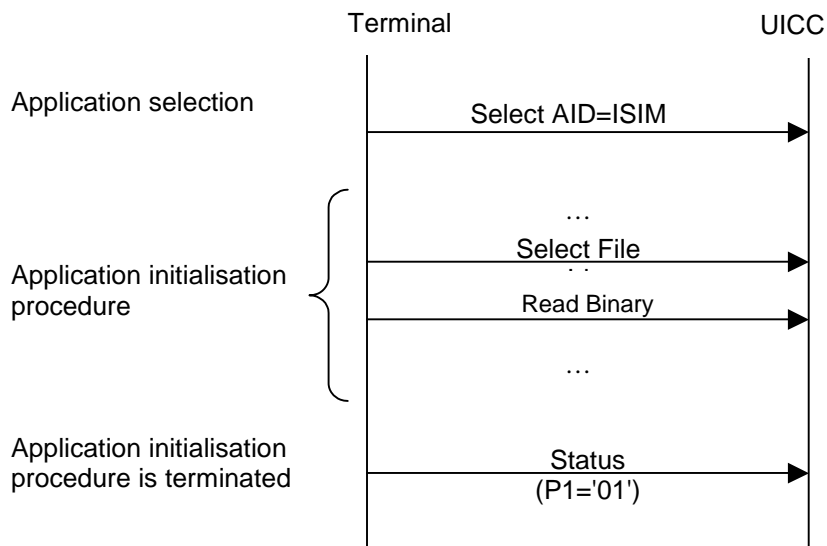
Figure E.1: ISIM Application Session Activation procedure
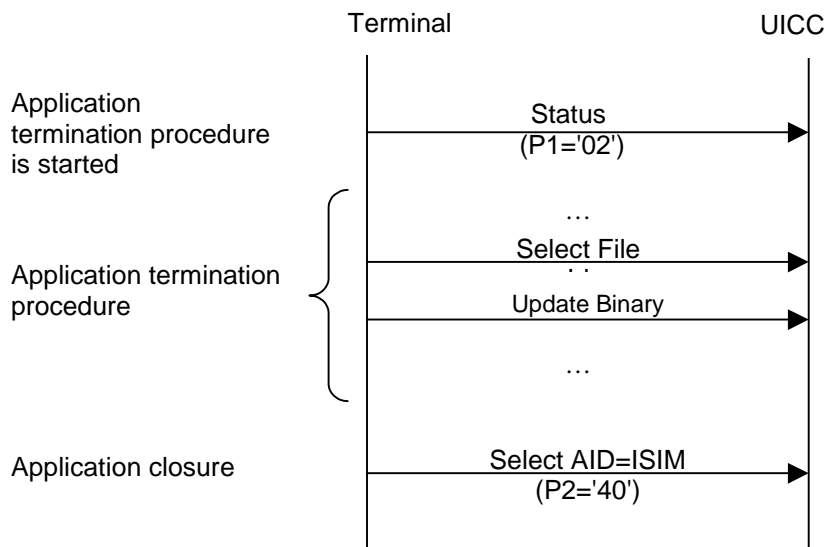
Figure E.2: ISIM Application Session Termination procedure

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#	WG 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	T3-050126	022		A	Reservation of file IDs under ADF ISIM	6.7.0
TP-27	TP-050019	T3-050182	024		F	Completion of GBA_U-related procedures	6.7.0
TP-27	TP-050019	T3-050185	025		F	Storage of NAF-keys identifiers in GBA_U	6.7.0
CT-28	TP-050136	C6-050416	027		A	ISO/IEC 7816-series revision	6.8.0
CT-29	CP-050330	C6-050731	029	1	A	Default Record for EFIMPU	6.9.0
CT-29	CP-050335	C6-050693	030		F	Corrections of EFIST Service No. referencing	6.9.0
CT-29	CP-050335	C6-050694	031		F	Changes in Application Protocol due to the use of ISIM Service Table	6.9.0
CT-30	CP-050492	C6-050885	035		F	Subscription related procedures	6.10.0
CT-30	CP-050492	C6-050904	033		F	Encoding of IMPI, IMPU and Domain	6.10.0
CT-32	CP-060243	C6-060282	0036		F	Add missing EF in ISIM file structure	7.0.0
CT-32	CP-060243	C6-060319	0037		F	Update of the table summarizing the tags defined in 31.103	7.0.0
CT-33	CP-060386	C6-060511	0040	1		Correction of ISIM Service Table	7.1.0
CT-33	CP-060386	C6-060514	0043	1		Coding of P2	7.1.0
CT-36	CP-070294	C6-070314	0045	1	A	HTTP-Digest security request	7.2.0
CT-36	CP-070291	C6-070317	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	C6-070418	0051	2	B	Key Establishment mechanism: alignment with TS 33.110	7.3.0
CT-41	CP-080584	C6-080416	0055	1	A	Authentication of GBA	7.4.0
CT-43	CP-090453	C6-090173	0056	-	F	IMS public user identity for emergency registration	7.5.0
CT-46	CP-090988	C6-090478	0064	1	F	References update	7.6.0

History

Document history		
V7.1.0	September 2006	Publication
V7.2.1	June 2007	Publication
V7.3.0	October 2007	Publication
V7.4.0	October 2008	Publication
V7.5.0	July 2009	Publication
V7.6.0	January 2010	Publication