ETSI TS 131 103 V5.3.0 (2003-03)

Technical Specification

**Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
Characteristics of the ISIM application
(3GPP TS 31.103 version 5.3.0 Release 5)**

Reference
RTS/TSGT-0331103v530

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, send your comment to:
editor@etsi.org

Copyright Notification

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).

All published ETSI deliverables shall include information which directs the reader to the above source of information.

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.

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 (1995): "Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 4: Interindustry commands for interchange".

[7] ISO/IEC 7816-5 (1994): "Identification cards - Integrated circuit(s) cards with contacts - Part 5: Numbering system and registration procedure for application identifiers".

[8] ITU-T Recommendation T.50: "International Reference Alphabet (IRA) (Formerly International Alphabet No. 5 or IA5) - Information technology - 7-bit coded character set for information interchange

[8a] ISO 646 (1983): "Information processing - ISO 7-bits coded characters set for information interchange".

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

[10] ISO/IEC 7816-9 (2000): "Identification cards - Integrated circuit(s) cards with contacts - Part 9: Additional interindustry commands and security attributes".

[11] ISO/IEC 7816-6 (1996): "Identification cards - Integrated circuit(s) cards with contacts - Part 6: Interindustry data elements".

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

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

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

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

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

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

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

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

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

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

[22] ETSI TS 102 223: "Smart cards; Card Application Toolkit (CAT)".

[23] ETSI TS 101 220: "Smart cards; ETSI numbering system for telecommunication application providers".

[24] IETF RFC 2486: "The Network Access Identifier"

3 Definitions, symbols, abbreviations and coding conventions

3.1 Definitions

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

ISIM: application residing on the UICC, an IC card specified in 3GPP TS 31.101 [3]
In particular, 3GPP TS 31.101 [3] specifies the application independent properties of the UICC/terminal interface such as the physical characteristics and the logical structure

The AID of ISIM is defined in 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
CK	Cipher Key
DF	Dedicated File
EF	Elementary File
FFS	For Further Study
HE	Home Environment
HN	Home Network
ICC	Integrated Circuit Card
ID	IDentifier
IK	Integrity Key
IM	IP Multimedia
IMPI	IM Private Identity
IMPU	IM PUblic identity
IMS	IP Multimedia Subsystem
ISIM	IM Services Identity Module
K	long-term secret Key shared between the ISIM and the AuC
KSI	Key Set Identifier
LI	Language Indication
LSB	Least Significant Bit
MAC	Message Authentication Code
MF	Master File
MSB	Most Significant Bit
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 ISO/IEC 7816-6 [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.

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

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

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

For an overview containing all files see figure 4.1.

4.1 Contents of the EFs at the MF level

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

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

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.

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

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

Identifier: '6F08'	Structure: transparent	Mandatory
SFI: '01'		
File size: 33 bytes	Update activity: high	

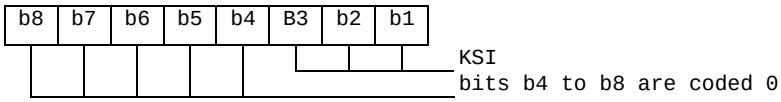
Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

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

- Key Set Identifier KSI.

  Coding:



- Ciphering key CK.

  Coding:

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

- Integrity key IK.

  Coding:

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

4.2.2 EF_{IMPI} (IMS private 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 coding of NAI TLV data object values see IETF RFC 2486 [24]. 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	URI TLV data object	M	X bytes

- URI

  Contents:

  - Home Network Domain Name.

  Coding:

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

4.2.4 EF_{IMPU} (IMS public user identity)

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

Identifier: '6F04'	Structure: linear fixed	Mandatory
SFI: '04'		
Record length: X bytes	Update activity: low	
Access Conditions: READ PIN UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

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

- URI

  Contents:

  - SIP URI by which other parties know the subscriber.

Coding:

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

4.2.5 EF_{AD} (Administrative Data)

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

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

Identifier: '6FAD'	Structure: transparent	Mandatory
SFI: '03'		
File size: 3+X bytes	Update activity: low	
Access Conditions: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

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

- UE operation mode:

  Contents:

  - mode of operation for the UE

  Coding:

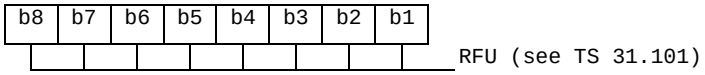
  - Initial value
    - '00' normal operation.
    - '80' type approval operations.
    - '01' normal operation + specific facilities.
    - '81' type approval operations + specific facilities.
    - '02' maintenance (off line).

- Additional information:

  Coding:

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

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



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 7816-9 [10]. 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.

4.3 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}.

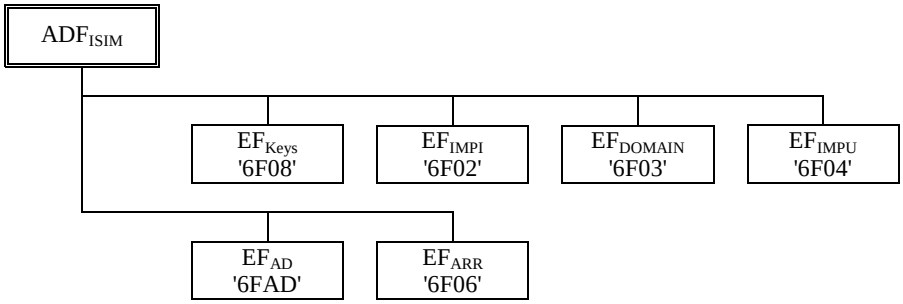


Figure 1: File identifiers and directory structures of ISIM

5 Application protocol

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

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

- An ISIM Application command/response pair is a sequence consisting of a command and the associated response.

- An ISIM Application procedure consists of one or more ISIM Application command/response pairs, which are used to perform all, or part of an application-oriented task. A procedure shall be considered as a whole that is to say that the corresponding task is achieved if and only if the procedure is completed. The Terminal shall ensure that, when operated according to the manufacturer's manual, any unspecified interruption of the sequence of command/response pairs, which realise the procedure, leads to the abortion of the procedure itself.

- An ISIM session is the interval of time starting at the completion of the ISIM initialisation procedure and ending either with the start of the ISIM session termination procedure, or at the first instant the link between the UICC and the Terminal is interrupted.

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

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

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

5.1 ISIM management procedures

5.1.1 Initialisation

5.1.1.1 ISIM application selection

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

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

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

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 3GPP 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.
- Cipher key and integrity key 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 3GPP 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.

The Terminal then runs all the procedures which are necessary to transfer the following subscriber related information to the ISIM:

- Cipher Key and Integrity Key update.

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 3GPP 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 3GPP 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 3GPP 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).

After a Successful AUTHENTICATE command, the Terminal shall perform Cipher and Integrity key update procedure.

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 Cipher and Integrity key

Request: The Terminal performs the reading procedure with EF_{Keys}.

Update: The Terminal performs the updating procedure with EF_{Keys}.

6 Security features

The security aspects of IMS are specified in 3GPP TS 33.203 [14]. This clause gives information related to security features supported by the ISIM to enable the following:

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

6.1 User verification and file access conditions

The ISIM application uses 2 PINs for user verification, PIN and PIN2. PIN2 is used only in the ADF. The PIN and PIN2 are mapped into key references as defined in 3GPP TS 31.101 [3]. Each key reference is associated with a usage qualifier as defined in ISO/IEC7816-9 [10]. The PIN status is indicated in the PS_DO, which is part of the FCP response when an ADF/DF is selected. The coding of the PS_DO is defined in 3GPP TS 31.101 [3].

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

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

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

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

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

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

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

7 ISIM Commands

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

7.1 AUTHENTICATE

7.1.1 Command description

The function is used during the procedure for authenticating the ISIM to its HN and vice versa. In addition, 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.

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).

The function shall be used whenever an IMS context shall be established, i.e. when the terminal receives a challenge from the IMS.

7.1.1.1 IMS 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 3GPP 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 3GPP TS 33.102 [4].

7.1.2 Command parameters and data

Code	Value
CLA	As specified in 3GPP 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)
'-XXXXXX-'	'000000'
'-------X'	Authentication context: 0 Reserved 1 3G IMS context

All other codings are RFU.

Command parameters/data:

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

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	
63 CX	
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 UICC Characteristics

8.1 Voltage classes

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

8.2 File Control Parameters (FCP)

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

8.2.1 Minimum application clock frequency

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

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

This annex defines if changing the content of an EF by the network (e.g. by sending an SMS), or by a CAT Application [22], 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
'6F08'	Ciphering and Integrity Keys for IMS	No
'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
NOTE: If EF_{IMPI}, EF_{IMPU} or EF_{DOMAIN} are changed, the UICC should issue a CAT REFRESH command [22].		

Annex B (informative): Tags defined in 31.103

Tag	Name of Data Element	Usage
'80'	URI TLV data object	IMPI, IMPU, DOMAIN
'DB'	Successful IMS authentication	Response to AUTHENTICATE
'DC'	Synchronisation failure	Response to AUTHENTICATE

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
'6F08'	Ciphering and Integrity Keys for IMS	'07FF…FF'
'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

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
'6F08'	'01'	Ciphering and Integrity Keys for IMS
'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

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.

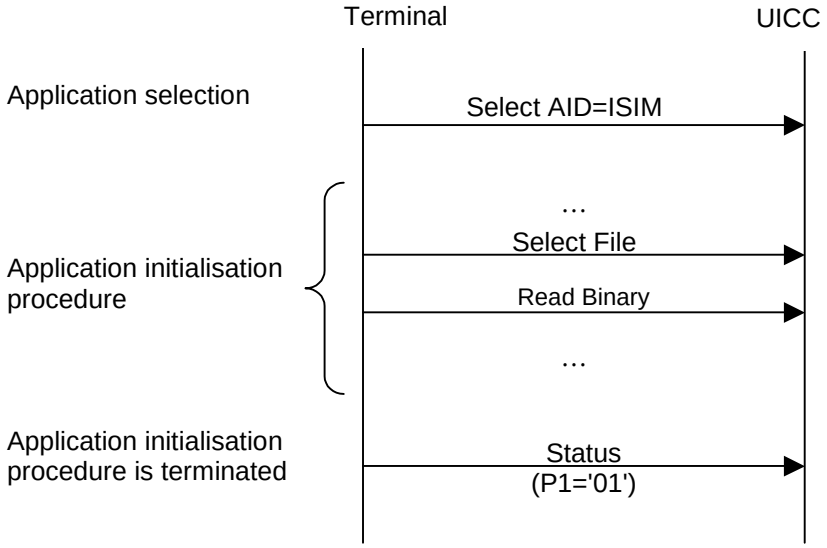


Figure E.1: ISIM Application Session Activation procedure

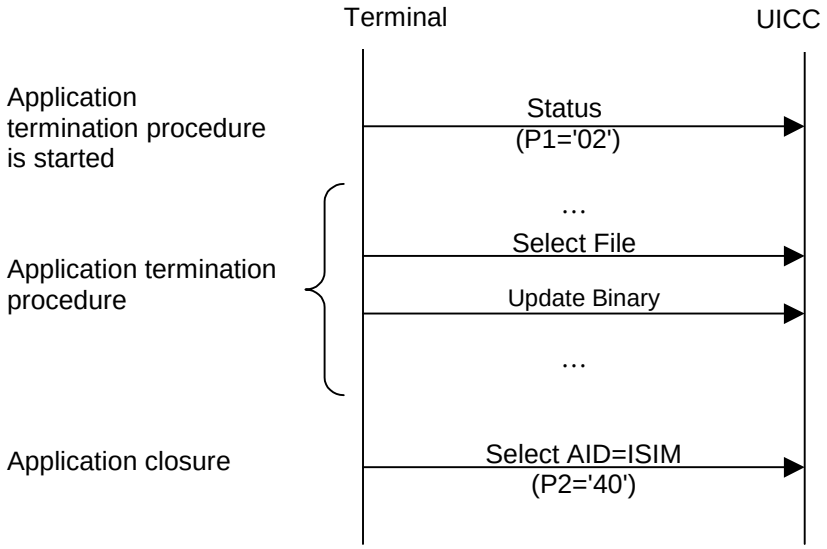


Figure E.2: ISIM Application Session Termination procedure

Annex F (informative): Change history

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

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**Old**	**New**
2002-06	TP-16	TP-020124				Initial version for information and approval in one step		1.0.0
						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]		5.0.0
2002-09	TP-17	TP-020211	001		F	Corrections	5.0.0	5.1.0
2002-12	TP-18	TP-020281	002		F	Replace reference to TS 31.110 by reference to ETSI TS 101 220	5.1.0	5.2.0
			003		F	Management of last selected ISIM		
2003-03	TP-19	TP-030019	005		F	Alignment with the Stage 2 terminology	5.2.0	5.3.0

History

Document history		
V5.0.0	June 2002	Publication
V5.1.0	September 2002	Publication
V5.2.0	December 2002	Publication
V5.3.0	March 2003	Publication