3GPP TSG SA WG3 Security — S3#20 **S3-010580**

27 - 30 November, 2001

Sophia Antipolis, France

Source : **Gemplus**

Subject : **ISIM Application**

The following document is a draft TS describing the ISIM characteristics. It was proposed as a framework for discussion in the T3 meeting in Kyoto, 5-7 november 2001 and should form the basis of the specification of the ISIM. The version presented here is slightly modified, taking into account some preliminary remarks.

There are still some open issues to be solved, before the ISIM can be clearly specified, amongst which:

- In TS 33.203 the ISIM is responsible for handling the keys etc. tailored to the IM CN SS. In TS 23.228 and TS 24.228 however, the USIM seems to be given this role. In S2, there are discussions going on about access independence for IMS and thus defining an ISIM independent from the USIM.
  It is most likely that this latter option will be chosen.

- A Service profile is attached to one or more public ID's and to one Private ID. In the case of access independence, i.e. obtaining access to the same service via different terminals, each with an ISIM, these ISIMs should bare the same private Identity. Is this allowed?

- It is not defined yet if the algorithms and keys used for IMS are different than the ones defined in the USIM

- Are there other functions that can be allocated to the ISIM, like phonebook, 'call control', operator preferences, ISIM Application Toolkit, generation of Call-ID, etc.?

In any case, this document can be discussed and serve as a basis for the R5 specification of the ISIM.

3GPP TS xx.xxx V0.0.0 (2001-06)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Terminals;
Characteristics of the ISIM Application
(Release 5)

Keywords

UMTS, ISIM

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

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 3G TS 31.101 [3]. In particular, 3G TS 31.101 [3] specifies the application independent properties of the UICC/terminal interface such as the physical characteristics and the logical structure.

1 Scope

The present document defines the ISIM application for 3G telecom network operation.
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 ME.

This is to ensure interoperability between an ISIM and an ME 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 ME is only specified where these are reflected over the interface.
The present document does not specify any of the security algorithms which may be used.

[Editor's note: a better terminology should be used for ME, as the ISIM can be used in either the mobile equipment or any other terminal equipment connecting to the IMS]

2 References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) 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 Architecture".

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

[6] ISO/IEC 7816-4 (1995): "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 Alphabet No. 5". (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 FCD 7816-9 (1999): "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] TS 23.228: “IP Multimedia (IM) Subsystem – Stage 2”.

[14] TS 33.203: “ Access security for IP-based services”

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

[16] IETF 2543bis2: “SIP: Session Initiation Protocol” (ietf-sip-rfc2543bis-02.txt)

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

[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): "Specification of Basic Encoding Rules for Abstract Syntax Notation One" Second Edition.

3 Definitions, symbols, abbreviations and coding conventions

3.1 Definitions

For the purposes of the present document, the following and definition applies.
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
AAA	Authentication Authorisation Accounting
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
CSCF	Call State Control Function
DF	Dedicated File

EF	Elementary File
FFS	For Further Study
HE	Home Environment
HN	Home Network
HSS	Home Subscriber Server
ICC	Integrated Circuit Card
ID	IDentifier
IK	Integrity key
IM	IP Multimedia
IMPI	IM Private Identity
IMPU	IM Public Identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
ISIM	IM Services Identity Module
K	ISIM Individual key
KSI	Key Set Identifier
LI	Language Indication
LSB	Least Significant Bit
MAC	Message authentication code
MAC	Message Authentication Code
MAC-A	MAC used for authentication and key agreement
MAC-I	MAC used for data integrity of signalling messages
MCC	Mobile Country Code
ME	Mobile Equipment
MF	Master File
MMI	Man Machine Interface
MSB	Most Significant Bit
NEV	NEVer
PIN	Personal Identification Number
PL	Preferred Languages
PS	Packet Switched
PS_DO	PIN Status Data Object
RAND	Random challenge
RAND_{MS}	Random challenge stored in the ISIM
RES	User response
RFU	Reserved for Future Use
RST	Reset
SA	Security Association
SDP	Session Description Protocol
SE	Security Environment
SEG	Security Gateway
SFI	Short EF Identifier
SGSN	Serving GPRS Support Node
SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol
SN	Serving Network
SQN	Sequence number
SRES	Signed RESponse calculated by an ISIM
SW	Status Word
TLV	Tag Length Value
UA	User Agent
UAC	UA Client
UAS	UA Server
UE	User Equipment
UICC	UMTS IC Card
ISIM	Universal Subscriber Identity Module
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 Contents of the Files

This clause specifies the EFs for the 3G session defining access conditions, data items and coding. A data item is a part of an EF which represents a complete logical entity, e.g. the alpha tag in an EF_{ADN} record.

EFs or data items having an unassigned value, or, which during the 3G session, are cleared by the ME, 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 3G 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 figures 4.1 and 4.2.

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 3G TS 31.101 [3].

4.1.1 EF_{DIR}

This EF contains the Application Identifier (AID) and the Application Label as mandatory elements.

The ISIM application can only be selected by means of the AID selection. The EF_{DIR} entry shall not contain a path object for application selection.

It is recommended that the application label does not contain more than 32 bytes.

Contents:

- according to 3G TS 31.101 [3].

Coding:

- according to 3G TS 31.101 [3].

4.1.2 EF_{ICCID} (ICC Identity)

This EF provides a unique identification number for the ICC.

Contents:

according to 3G TS 31.101 [3].

Coding:

according to 3G TS 31.101 [3].

4.1.3 EF_{ARR} (Access Rule Reference)

This EF contains the access rules for access to the EFs under the master file including this EF. This file is mandatory for the ISIM application.

Contents:

- according to 3G TS 31.101 [3].

Coding:

- according to 3G 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.

4.2.1 EF$_{IMS-ST}$ (IMS Service table)

This EF indicates which IMS services are available. If a service is not indicated as available in the USIM, the ME shall not select this service.

Identifier: 'xxxx'	Structure: transparent	Conditional (see Note)
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
etc.			
X	Services (8X-7) to (8X)	O	1 byte
NOTE:This file is mandatory if and only if DF$_{IMS}$ is present.			

-Services

Contents: Service n°1 : SIP domain URI

Coding:

the coding rules of the USIM Service Table apply to this table.

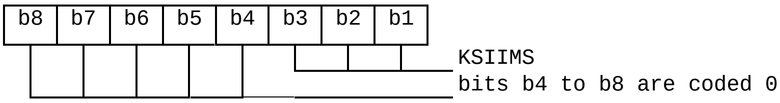
4.2.2 EF$_{KeysIMS}$ (Ciphering and Integrity Keys for IP Multimedia System)

This EF contains the ciphering key CKIMS, the integrity key IKIMS and the key set identifier KSIIMS for the IP Multimedia Subsystem.

Identifier: 'xxxx'	Structure: transparent	Mandatory
SFI: 'yy'		
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 KSIIMS	M	1 byte
2 to 17	Ciphering key CKIMS	M	16 bytes
18 to 33	Integrity key IKIMS	M	16 bytes

- Key Set Identifier KSIIMS.
  Coding:



- Ciphering key CKIMS.
  Coding:
  - the least significant bit of CKIMS is the least significant bit of the 17th byte. The most significant bit of CKIMS is the most significant bit of the 2nd byte.
- Integrity key IKIMS.
  Coding:
  - the least significant bit of IKIMS is the least significant bit of the 33rd byte. The most significant bit of IKIMS is the most significant bit of the 18th byte.

4.2.3 EF$_{IMPI}$ (IMS PRIVATE IDENTIFIER)

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

Identifier: ’xxxx’	Structure: transparent		Conditional (see Note)
SFI: ‘yy’			
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	M	X bytes
NOTE:This file is mandatory if and only if DF$_{IMS}$ is present.			

- URI

  Contents:

  - Private SIP URI of the user.

  Coding:

  according to RFC 2543 [16]. Unused bytes shall be set to ‘FF’.

4.2.4 EF$_{DOMAIN}$ (SIP DOMAIN URI)

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

Identifier: 'xxxx'	Structure: transparent		Optional
SFI: ‘yy’			
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	M	X bytes

- URI

  Contents:

  - Request-URI.

  Coding:

  - according to RFC 2543 [16] . Unused bytes shall be set to ‘FF’.

4.2.5 EF$_{IMPU}$ (IMS PUBLIC IDENTIFIER OF USER)

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

Identifier: 'xxxx'	Structure: linear fixed	Conditional (see note)

SFI: ‘yy’			
Record length: X bytes		Update activity: low	
Access Conditions: READ PIN UPDATE PIN/ADM (fixed during administrative management) DEACTIVATE ADM ACTIVATE ADM			
Bytes	Description	M/O	Length
1 to X	URI	M	X bytes
NOTE:This file is mandatory if and only if DF_{IMS} is present.			

- URI
  Contents:
  - SIP URI by which other parties know the subscriber.

  Coding:
  - according to RFC 2543 [16]. Unused bytes shall be set to ‘FF’.

4.2.51 $\text{EF}_{\text{START-HFN}}$ (Initialisation values for Hyperframe number)

This EF contains the values of $\text{START}_{\text{IMS}}$ and $\text{START}_{\text{IMS}}$ of the bearers that were protected by the keys in $\text{EF}_{\text{KEYSIMS}}$ at release of the last IMS session. These values are used to control the lifetime of the keys (see 3G TS 33.102 [3]).

Identifier: 'XXXX'	Structure: transparent		Mandatory
SFI: 'yy'			
File size: 3 bytes		Update activity: high	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM			
Bytes	Description	M/O	Length
1 to 3	$\text{START}_{\text{IMS}}$	M	3 bytes

- $\text{START}_{\text{IMS}}$
  Contents: Initialisation value for Hyperframe number – IMS domain.
  Coding: The LSB of $\text{START}_{\text{IMS}}$ is stored in bit 1 of byte 3. Unused nibbles are set to 'F'.

4.2.52 $\text{EF}_{\text{THRESHOLD}}$ (Maximum value of START)

This EF contains the maximum value of $\text{START}_{\text{IMS}}$. This value is used to control the lifetime of the keys (see 3G TS 33.102 [3]).

Identifier: 'XXXX'	Structure: transparent		Mandatory
SFI: 'yy'			
File size: 3 bytes		Update activity: low	
Access Conditions: READ PIN UPDATE ADM DEACTIVATE ADM ACTIVATE ADM			
Bytes	Description	M/O	Length
1 to 3	Maximum value of $\text{START}_{\text{IMS}}$.	M	3 bytes

- Maximum value of $\text{START}_{\text{IMS}}$.
  Coding: As for $\text{EF}_{\text{START-IMS}}$.

4.7 Files of ISIM

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}.

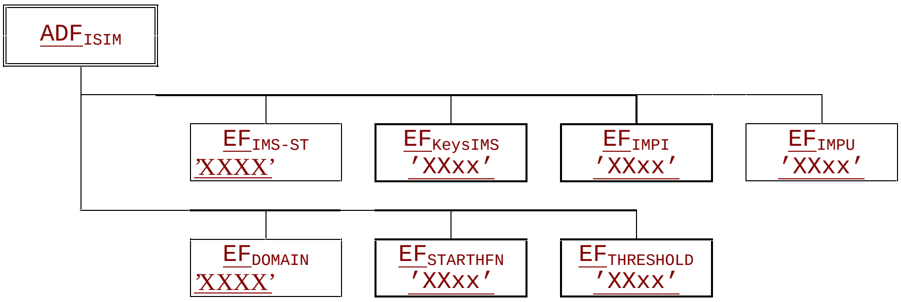


Figure 4.2: File identifiers and directory structures of ISIM

5 Application protocol

When involved in 3G administrative management operations, the ISIM interfaces with appropriate equipment. These operations are outside the scope of this standard.
When involved in 3G network operations the ISIM interfaces with an ME with which messages are exchanged. A message can be a command or a response.

[Editor’s note: a better terminology should be used for ME, as the ISIM can be used in either the mobile equipment or any other terminal equipment connecting to the IMS]

- 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 ME 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 IMS session of the ISIM in the IMS application is the interval of time starting at the completion of the ISIM initialisation procedure and ending either with the start of the 3G session termination procedure, or at the first instant the link between the UICC and the ME is interrupted.

During the 3G network operation phase, the ME plays the role of the master and the ISIM plays the role of the slave.
The ISIM shall execute all 3G commands or 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 network 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

After UICC activation (see 3G TS 31.101 [3]), the ME selects a USIM application. If no EF_{DIR} file is found or no USIM applications are listed in the EF_{DIR} file, the ME then tries to select the GSM application as specified in TS 51.011 [19].

If neither USIM nor GSM application is present on the UICC, or only after having selected either one, the ME shall select an ISIM application, if an ISIM application is listed in the EF_{DIR} file.
After a successful ISIM application selection, the selected ISIM (AID) is stored on the UICC. This application is referred to as the last selected application. The last selected application shall be available on the UICC after a deactivation followed by an activation of the UICC.
If an ISIM application is selected using partial DF name, the partial DF name supplied in the command shall uniquely identify an ISIM application. Furthermore if an ISIM application is selected using a partial DF name as specified in 3G TS 31.101 [3] indicating in the SELECT command the last occurrence the UICC shall select the ISIM application stored as the last 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 ME runs the user verification procedure. If the procedure is not performed successfully, the ISIM initialisation stops.
The ME performs the administrative information request.
If all these procedures have been performed successfully then an IMS session can start. In all other cases IMS session shall not start.
Afterwards, the ME runs the following procedures if the ME supports the related feature:

- Cipher key and integrity key request for CS- and/or PS-mode.

- Depending on the further services that are supported by both the ME and the ISIM the corresponding EFs have to be read.

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

5.1.2 Session termination

5.1.2.1 IMS session termination

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

The 3G session is terminated by the ME as follows.
The ME shall indicate to the ISIM by sending a particular STATUS command that the termination procedure is starting.
The ME 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 ME has already updated any of the subscriber related information during the IMS session, and the value has not changed until IMS session termination, the ME may omit the respective update procedure.

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

5.1.3 ISIM application closure

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

5.1.9 UICC presence detection

The ME checks for the presence of the UICC according to 3G TS 31.101 [3].

5.2 ISIM security related procedures

5.2.1 Authentication algorithms computation

The ME selects an ISIM application and uses the AUTHENTICATE command (see 7.1.1). The response is sent to the ME (in case of the T=0 protocol when requested by a subsequent GET RESPONSE command).
After a Successful AUTHENTICATE command, the ME shall perform Cipher and Integrity key update procedure.

5.2.2 IMS UserIdentifiers request

The ME performs the reading procedure with $EF_{IMPI,}$ EF_{IMPU} and the EF_{IMS-ST}. Depending if Service n°1 is present, the ME continues the readin procedure with EF_{DOMAIN}.

5.2.6 Cipher and Integrity key

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

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

6 Security features

The security aspects of IMS are specified in 3G 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 Authentication and key agreement procedure

This subclause gives an overview of the authentication mechanism and cipher and integrity key generation which are invoked by the network. For the specification of the corresponding procedures across the ISIM/ME interface see clause 5.

The mechanism achieves mutual authentication by the user and the network showing knowledge of a secret key K which is shared between and available only to the ISIM and the HSS in the user's HN. In addition, the ISIM and the HN keep track of counters SQN_{ISIM} and SQN_{HSS} respectively to support network authentication. SQN_{HSS} is a counter in the HSS, individual for each user and SQN_{ISIM} denotes the highest sequence number the ISIM has ever accepted.

When the SN/P-CSCSF initiates an authentication and key agreement, it selects the next authentication vector and sends the parameters RAND and AUTN (authentication token) to the user. Each authentication token consists of the following components: a sequence number SQN, an Authentication Management Field (AMF) and a message authentication code MAC over the RAND, SQN and AMF.

The ISIM checks whether AUTN can be accepted and, if so, produces a response RES which is sent back to the SN/ P-CSCSF. The SN/ P-CSCSF compares the received RES with XRES. If they match the SN/ P-CSCSF considers the authentication and key agreement exchange to be successfully completed. The ISIM also computes CK and IK. The established keys CK and IK will be used by the ME to perform ciphering and integrity functions.

A permanent secret key K is used in this procedure. This key K has a length of 128 bits and is stored within the ISIM for use in the algorithms described below. Also more than one secret key K can be stored in the ISIM. The active key to be used by the algorithms is signalled within the AMF field in the AUTN.

6.2 Cryptographic Functions

The names and parameters of the cryptographic functions supported by the ISIM are defined in 3G TS 33.102 [4]. These are:

- f1: a message authentication function for network authentication used to compute XMAC;
- f1*: a message authentication function for support to re-synchronisation with the property that no valuable information can be inferred from the function values of f1* about those of f1, ... , f5, f5* and vice versa;
- f2: a message authentication function for user authentication used to compute SRES;
- f3: a key generating function to compute the cipher key CK;
- f4: a key generating function to compute the integrity key IK;
- f5: a key generating function to compute the anonymity key AK (optional);
- f5*: a key generating function to compute AK in re-synchronisation procedures with the property that no valuable information can be inferred from the function values of f5* about those of f1, f1*, f2, ... , f5 and vice versa.

These cryptographic functions may exist either discretely or combined within the ISIM.

6.4 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 3G 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 3G 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 ME 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 3G TS 31.101 [3] applies to the ISIM application with the following definitions and additions.

- The ISIM application shall use key reference '01' as PIN and key reference '81' as PIN2. For access to DFTelecom the PIN shall be verified. Access with PIN2 is limited to the ISIM application.
- 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 31.101 [3].
- Every file in the ISIM application shall have a reference to an access rule stored in EF_{ARR}.
- A multi-application capability UICC (from the security context point of view) shall support the referenced format using SEID as defined in 3G TS 31.101 [3].
- A multi-application capability UICC (from the security context point of view) shall support the replacement of an ISIM application PIN with the Universal PIN, key reference '01', as defined in 3G TS 31.101 [3]. Only the Universal PIN is allowed as a replacement.
- A terminal shall support the use of level 1 and level 2 user verification requirements as defined in 3G TS 31.101 [3].
- A terminal shall support the replacement of an ISIM application PIN with the Universal PIN, key reference '01', as defined in 3G TS 31.101 [3].
- A terminal shall support the security attributes defined using tag's '8C', 'AB' and '8B' as defined in 3G TS 31.101 [3]. In addition both the referencing methods indicated by tag '8B' shall be supported as defined in 3G TS 31.101 [3].

Disabling of PIN2 is allowed. This is, however, not the case if PIN2 is mapped to the CHV2 of a GSM application.

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 3G TS 31.101 [3].

7 ISIM Commands

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 in the IMS ~~context:~~

~~-~~ ~~a 3G security context~~context, when ~~3G~~ IMS authentication vectors (RAND, CK, IK, AUTN) are available:

- Either, the IMS client is connected to the IMS via a 3G network~~-~~(i.e. the UE is located in the UTRAN), or~~-~~via any other means (PSTN, WLAN…) supporting the connection to the IMS.~~in a GSM radio access network which is connected to a 3G or 3G capable VLR/SGSN), or~~

7.1.1.1 3G security context

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

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

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

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

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

$AUTS = Conc(SQN_{MS}) \| MACS;$

$Conc(SQN_{MS}) = SQN_{MS} \oplus f5^*_K(RAND)$ is the concealed value of the counter SQN_{MS} in the ISIM; and.

$MACS = f1^*_K(SQN_{MS} \| RAND \| AMF)$ where:

RAND is the random value received in the current user authentication request;

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

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

The use of AMF is HN specific and while processing the command, the content of the AMF has to be interpreted in the appropriate manner. The AMF may e.g. be used for support of multiple algorithms or keys or for changing the size of lists, see 3G TS 33.102 [4].

7.1.2 Command parameters and data

Code	Value
CLA	As specified in 3G 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~~-~~x’	’0000000’

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

7.2 Void

7.3 Status Conditions Returned by the UICC

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.

7.3.1 Security management

SW1	SW2	Error description
'98'	'62'	- Authentication error, incorrect MAC

7.3.2 Status Words of the Commands

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

Commands and status words

Status Words	AUTHENTICATE
90 00	*
91 XX	*
93 00	
98 50	
98 62	*
~~98 64~~	~~*~~
62 00	*
62 81	
62 82	
62 83	
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'.	

7.4 VERIFY command

The VERIFY command is used to verify the user as defined in 3G TS 31.101 [3]. For the ISIM application during a 3G session the parameter P2 is restricted to the following values.

- '01' indicating verification of the PIN;

- '81' indicating verification of PIN2.

NOTE For administrative purposes any level 5 or level 6 value as specified in 3G TS 31.101 [3] may be used.

After 3 unsuccessful verification attempts, not necessarily in the same session the PINs blocked. The blocked status is indicated in the response to the VERIFY command (0 attempts left) see 3G TS 31.101 [3].

8 UICC Characteristics

8.1 Voltage classes

A UICC holding an ISIM application shall support at least two consecutive voltage classes as defined in 3G 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 3G TS 31.101 [3]. This section also specifies values for data objects in the FCP information where there is no exact value given in 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 3G 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 3G 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): Tags defined in XX.XXX

Tag	Name of Data Element	Usage
’DB’	Successful 3G 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 B (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
‘XXXX’	Ciphering and integrity keys for packet switched domain	'07FF…FF'
‘XXXX’	SIP Domain URI	‘00FF…FF’
‘XXXX’	SIP Private Identifier	‘00FF…FF’
‘XXXX’	SIP Public Identifier	‘00FF…FF’

Annex C (normative): List of SFI Values

This annex lists SFI values assigned in this specification.

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

File Identification	SFI	Description
'XXXX'	'yy'	Cyphering and Integrity keys for IMS
'XXXX'	'yy'	IMS Service table
'XXXX'	'yy'	SIP Domain URI
'XXXX'	'yy'	SIP Private Identifier
'XXXX'	'yy'	SIP Public Identifier

All other SFI values are reserved for future use.

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

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

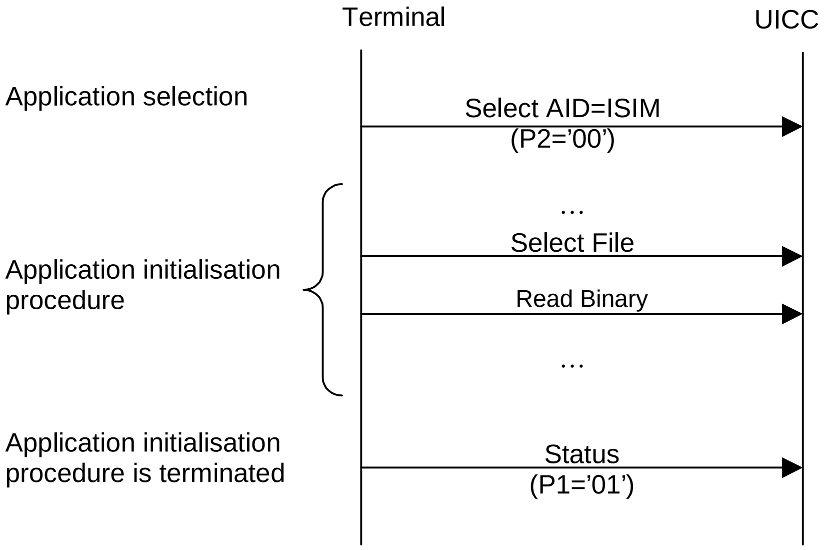


Figure I.1 ISIM Application Session Activation procedure

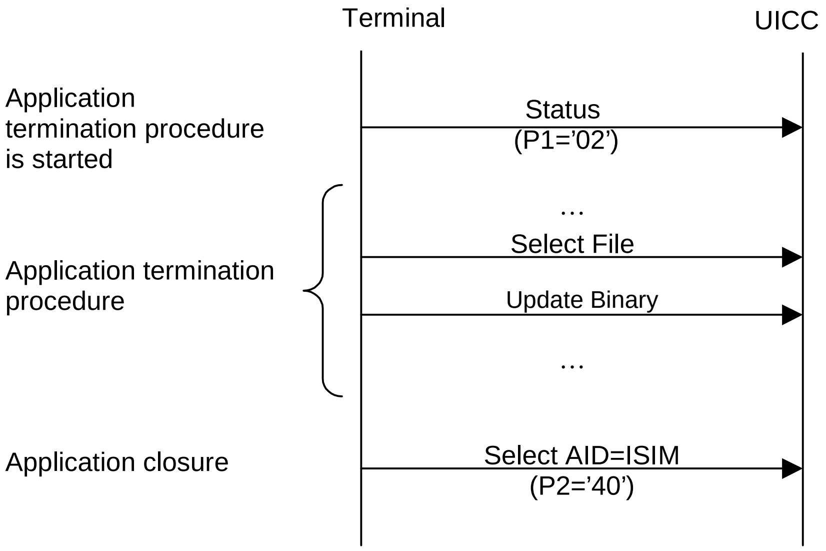


Figure I.2 ISIM Application Session Termination procedure

Annex E (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