3GPP TSG-T (Terminals) Meeting #23
Phoenix, USA
10 - 12 March, 2004

TP-040025

Agenda Item: 5.3.3

Source: T3

Title: CRs to TS 31.103: Characteristics of the IP Multimedia Services Identity Module (ISIM) application

Document for: Approval

This document contains the following change requests that are approved by 3GPP TSG T3 and forwarded to 3GPP TSG T#23 for approval:

Spec	CR	Rev	Phase	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
31.103	011	-	Rel-5	CR 31.103 Rel-5: Essential corrections to remove Session Keys	F	5.5.0	5.6.0	T3-040136
31.103	012	-	Rel-6	CR 31.103 Rel-6: Essential corrections to remove Session Keys	A	6.2.0	6.3.0	T3-040137
31 103	014	-	Rel-6	Creation of an ISIM Service Table	F	6.2.0	6.3.0	T3-040128

3GPP TSG-T WG3 Meeting #30 ***T3-040128***
Sophia-Antipolis, France, 9-13 February 2004

CR-Form-v7

CHANGE REQUEST

⌘ **TS 31 103 CR 014** ⌘**rev** **-** ⌘ Current version: **6.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Creation of an ISIM Service Table
Source:	⌘	T3
Work item code:	⌘	ISIM
Date:	⌘	13/02/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	An ISIM service table is needed for introduction of optional EFs in the ISIM
Summary of change:	⌘	A new EF IST is introduced, with the appropriate procedures
Consequences if not approved:	⌘	It would not be possible to introduce optional EFs in further releases

Clauses affected:	⌘	4.2.X (New Section)

Other specs affected:	⌘	Y	N		⌘
			X	Other core specifications	
			X	Test specifications	
			X	O&M Specifications	

Other comments: ⌘

4.2.y 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: '6Fzz'	Structure: transparent	Optional
SFI: 'tt'		
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°y: RFU

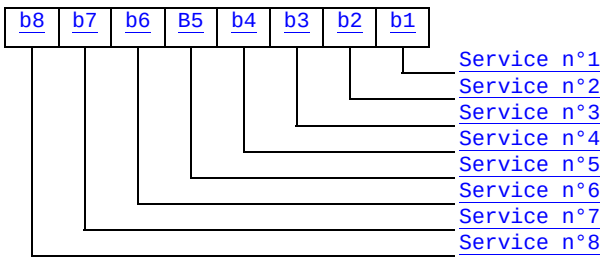
The EF shall contain at least one byte. Further bytes may be included, but if the EF includes an optional byte, then it is mandatory for the EF to also contain all bytes before that byte. Other services are possible in the future and will be coded on further bytes in the EF. The coding falls under the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

Coding:

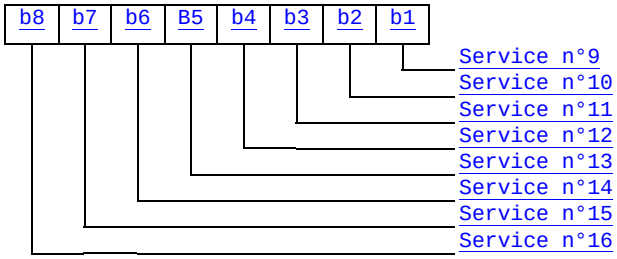
1 bit is used to code each service:
bit = 1: service available;
bit = 0: service not available.

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

First byte:



Second byte:


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.

4.3 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}.

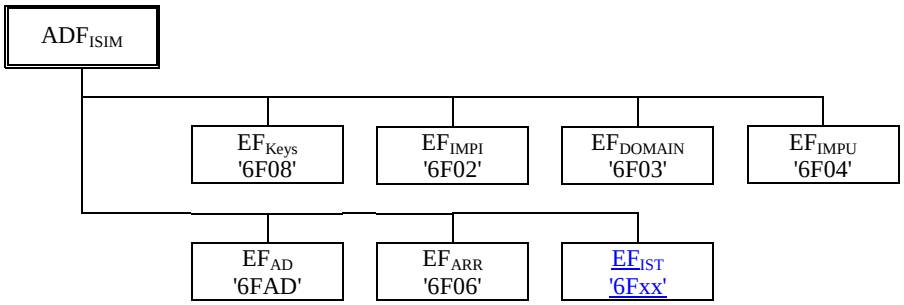


Figure 1: File identifiers and directory structures of ISIM

5.1.1.2 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.
- ISIM Service Table request. If the ISIM Service Table is not present, the terminal shall assume that no optional services are available.

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.

5.2.x ISIM Service Table request

Requirement: ISIM Service Table available in the ISIM

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

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
'6Fxx'	ISIM Service Table	Caution
NOTE: If EF_{IMPI}, EF_{IMPU} or EF_{DOMAIN} are changed, the UICC should issue a CAT REFRESH command [22].		

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
'6Fxx'	ISIM Service Table	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
‘6Fxx’	‘tt’	ISIM Service Table

All other SFI values are reserved for future use.

3GPP TSG-T3 Meeting #30
Sophia, France, 9-13.02.2004

T3-040136

CR-Form-v7

CHANGE REQUEST

⌘ **31.103** **CR** **011** ⌘ **rev** **-** ⌘ Current version: **5.5.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ [X] ME [X] Radio Access Network [X] Core Network [ ]

Title:	⌘	CR 31.103 Rel-5: Essential corrections to remove Session Keys
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	11/02/2004
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)

Reason for change:	⌘	Implement the SA3 requirements documented in T3-020321 (S3-020314)
Summary of change:	⌘	SA3 has identified that Session Keys do not need to be stored. Therefore EFKEYS and all references to it are removed.
Consequences if not approved:	⌘	Incorrect implementation.

Clauses affected:	⌘	

		Y	N		
Other specs Affected:	⌘		N	Other core specifications	⌘
			N	Test specifications	
			N	O&M Specifications	

Other comments:	⌘	

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

4.2.1 VoidEF$_{Keys}$ (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.

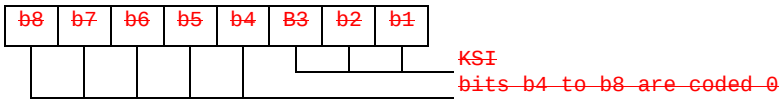
Identifier: '6F08'	Structure: transparent	Mandatory
SFI: '01'		
File size: 33 bytes	Update activity: high	

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.

[….]

4.3 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$_{DIR}$.

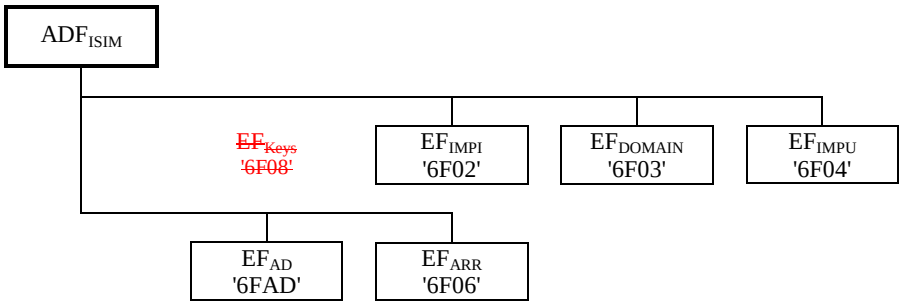


Figure 1: File identifiers and directory structures of ISIM

[….]

5.1 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 VoidCipher and Integrity key

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

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

[….]

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 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.

3GPP TSG-T3 Meeting #30
Sophia, France, 9-13.02.2004

T3-040137

CR-Form-v7

CHANGE REQUEST

⌘ **31.103** **CR** **012** ⌘ **rev** **-** ⌘ Current version: **6.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ [X] ME [X] Radio Access Network [X] Core Network [ ]

Title:	⌘	CR 31.103 Rel-6: Essential corrections to remove Session Keys
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	11/02/2004
Category:	⌘	**A**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)

Reason for change:	⌘	Implement the SA3 requirements documented in T3-020321 (S3-020314)
Summary of change:	⌘	SA3 has identified that Session Keys do not need to be stored. Therefore EFKEYS and all references to it are removed.
Consequences if not approved:	⌘	Incorrect implementation.

Clauses affected:	⌘	

		Y	N			
Other specs Affected:	⌘		N	Other core specifications	⌘	
			N	Test specifications		
			N	O&M Specifications		

Other comments:	⌘	

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

4.2.1 VoidEF$_{Keys}$ (Ciphering and Integrity Keys for IMS)

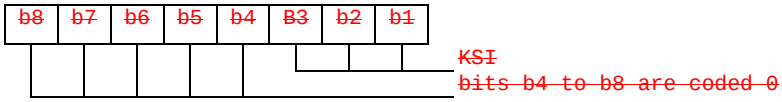
This EF contains the ciphering key CK, the integrity key IK and the key set identifier KSI for the IP Multimedia Subsystem.

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.

[….]

4.3 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$_{DIR}$.

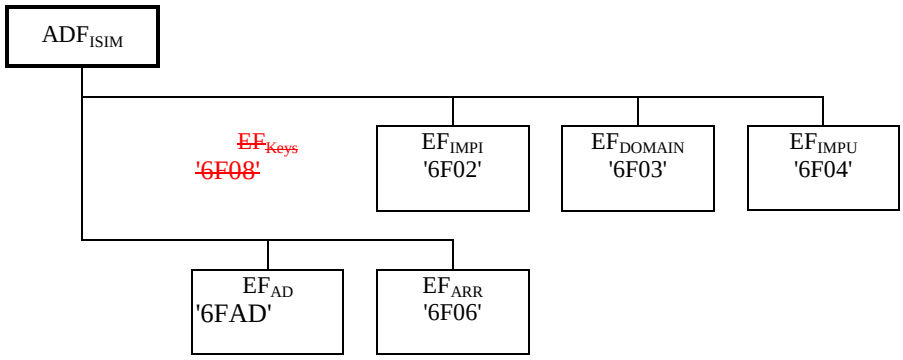


Figure 1: File identifiers and directory structures of ISIM

[….]

5.1 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 Void~~Cipher and Integrity key~~

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

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

[….]

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 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.