3GPP TSG-T (Terminals) Meeting #27
Tokyo, Japan, 9-11 March 2005

TP-050018

Agenda Item: 6.3.3

Source: T3

Title: CRs to TS 31.102

Document for: Approval

This document contains the following change requests that are approved by 3GPP TSG T3 and forwarded to 3GPP TSG T#27 for approval:

Doc-2nd-Level	Spec	CR	Rev	Rel	Subject	Cat	Ver-old	Ver-new	WI
T3-050201	31.102	250	2	Rel-6	Enable multiple Terminal Profile downloads in UST	F	6.8.0	6.9.0	TEI6
T3-050111	31.102	260		Rel-5	Correction of example MMS Issuer/User Connectivity Parameters	F	5.11.0	5.12.0	TEI5
T3-050112	31.102	261		Rel-6	Background colours not unique	F	6.8.0	6.9.0	TEI6
T3-050137	31.102	262		Rel-5	Oddities Service Numbers in EF_UST	F	5.11.0	5.12.0	TEI5
T3-050161	31.102	263	1	Rel-6	Correction due to inclusion of EHPLMN in wrong release	F	6.8.0	6.9.0	TEI6
T3-050189	31.102	264	1	Rel-7	Correction to overcome IMSI number space limitation – inclusion of EHPLMN	F	6.9.0	7.0.0	TEI7
T3-050171	31.102	265		Rel-6	Completion of GBA_U-related procedures	F	6.8.0	6.9.0	TEI6
T3-050184	31.102	266		Rel-6	Storage of NAF-keys identifiers in GBA_U	F	6.8.0	6.9.0	TEI6
T3-050143	31.102	267		Rel-6	VGCS/VBS security - alignment with 43.020	F	6.8.0	6.9.0	TEI6
T3-050166	31.102	268		Rel-6	MBMS security - alignment with TS 33.246	F	6.8.0	6.9.0	TEI6
T3-050169	31.102	269		Rel-7	Clarification on ADM access condition	F	6.9.0	7.0.0	TEI7
T3-050170	31.102	270		Rel-6	Collection of essential corrections	F	6.8.0	6.9.0	TEI6

3GPP TSG T WG3 Meeting #35 **T3-050111**
Barcelona, Spain, 8th – 11th February 2005

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.102** **CR** **260** ⌘ **rev** **-** ⌘ Current version: **5.11.0** ⌘

*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:	⌘	Correction of example MMS Issuer/User Connectivity Parameters
Source:	⌘	T3
Work item code:	⌘	TEI-5 ***Date:*** ⌘ 08/02/2005
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:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change:	⌘	Incorrect length coding in coding example of MMS connectivity parameter. CR 223 agreed during T#24 Plenary (TP-040101 / T3-040289) was not complete implemented in the specification
Summary of change:	⌘	Changed the incorrect length coding of MMS connectivity parameter
Consequences if not approved:	⌘	Misinterpretation of the coding example for MMS Issuer/User Connectivity Parameters and therefore there is a high risk of wrong implementation in the Mobiles and/or UICCs

Clauses affected:	⌘	Annex J.2

		Y	N		
Other specs Affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	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.

Annex J (informative): Example of MMS coding

This annex gives an example for the coding of MMS User Preferences, while the MMS User Information Preference parameters are coded according to the WAP implementation of MMS.

[…]

J.2 Coding Example for MMS Issuer/User Connectivity Parameters

0xAB MMS Connectivity Parameters Tag

0x81 0x~~9F~~88 (Length = "136") (Length bytes greater than 127 are coded onto 2 bytes according to ISO/IEC 8825 [35])

0x80 MMS Implementation Tag

0x01 (Length = "1")

0x01 (MMS implementation information = "WAP"; 1 Byte)

0x81 MMS Relay/Server Tag

0x17 (Length = "23")

0x68 0x74 0x74 0x70 0x3A 0x2F 0x2F 0x6D 0x6D 0x73 0x2D 0x6F 0x70 0x65 0x72 0x61 0x74 0x6F 0x72 0x2E 0x63 0x6F 0x6D
(MMS Relay/Server information = "http://mms-operator.com"; 23 characters; 23 Bytes)

0x82 Interface to Core Network and Bearer Tag

0x32 (Length = "50")

0x10 0xAA (bearer = "GSM-CSD"; 2 Bytes)

0x08 0x2B 0x34 0x39 0x35 0x33 0x34 0x31 0x39 0x30 0x36 0x00
(address = "+495341906", 12 Bytes)

0x09 0x87 (type of address = "E164"; 2 Bytes)

0x25 0xC5 (speed = "autobauding"; 2 Bytes)

0x0A 0x90 (call type = "ANALOG_MODEM"; 2 Bytes)

0x0C 0x9A (authentication type = "PAP"; 2 Bytes)

0x0D 0x64 0x75 0x6D 0x6D 0x79 0x5F 0x6E 0x61 0x6D 0x65 0x00
(authentication id = "dummy_name"; 12 Bytes)

0x0E 0x64 0x75 0x6D 0x6D 0x79 0x5F 0x70 0x61 0x73 0x73 0x77 0x6F 0x72 0x64 0x00
(authentication pw = "dummy_password"; 16 Bytes)

0x83 Gateway Tag

0x36 (Length = "54")

0x20 0x31 0x37 0x30 0x2E 0x31 0x38 0x37 0x2E 0x35 0x31 0x2E 0x33 0x00
(address = "170.187.51.3"; 14 Bytes)

0x21 0x85 (type of address = "IPv4"; 2 Bytes)

0x23 0x39 0x32 0x30 0x33 0x00 (port = "9203"; 6 Bytes)

0x24 0xCB (service = "CO-WSP"; 2 Bytes)

0x19 0x9C (authentication type = "HTTP BASIC"; 2 Bytes)

0x1A 0x64 0x75 0x6D 0x6D 0x79 0x5F 0x6E 0x61 0x6D 0x65 0x00
(authentication id = "dummy_name"; 12 Bytes)

0x1B 0x64 0x75 0x6D 0x6D 0x79 0x5F 0x70 0x61 0x73 0x73 0x77 0x6F 0x72 0x64 0x00
(authentication pw = "dummy_password"; 16 Bytes)

3GPP TSG T WG3 Meeting #35
Barcelona, Spain, 8th – 11th February 2005

T3-050112
(revised from T3-050037)

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.102** **CR** **261** ⌘ **rev** **-** ⌘ Current version: **6.8.0** ⌘

*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:	⌘	Background colours not unique
Source:	⌘	T3
Work item code:	⌘	TEI-6
Date:	⌘	08/02/2005
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:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change:	⌘	Different background colours for EF's in figure 4.2 "File identifiers and directory structures of USIM"
Summary of change:	⌘	Modified background colours in the figure, having an unique classification of the EF's to the corresponding directory.
Consequences if not approved:	⌘	Possible interpretation of EF's to a wrong directory under the USIM.

Clauses affected:	⌘	4.7			
		Y	**N**		
Other specs Affected:	⌘		**X**	Other core specifications	⌘
			X	Test specifications	
			X	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:

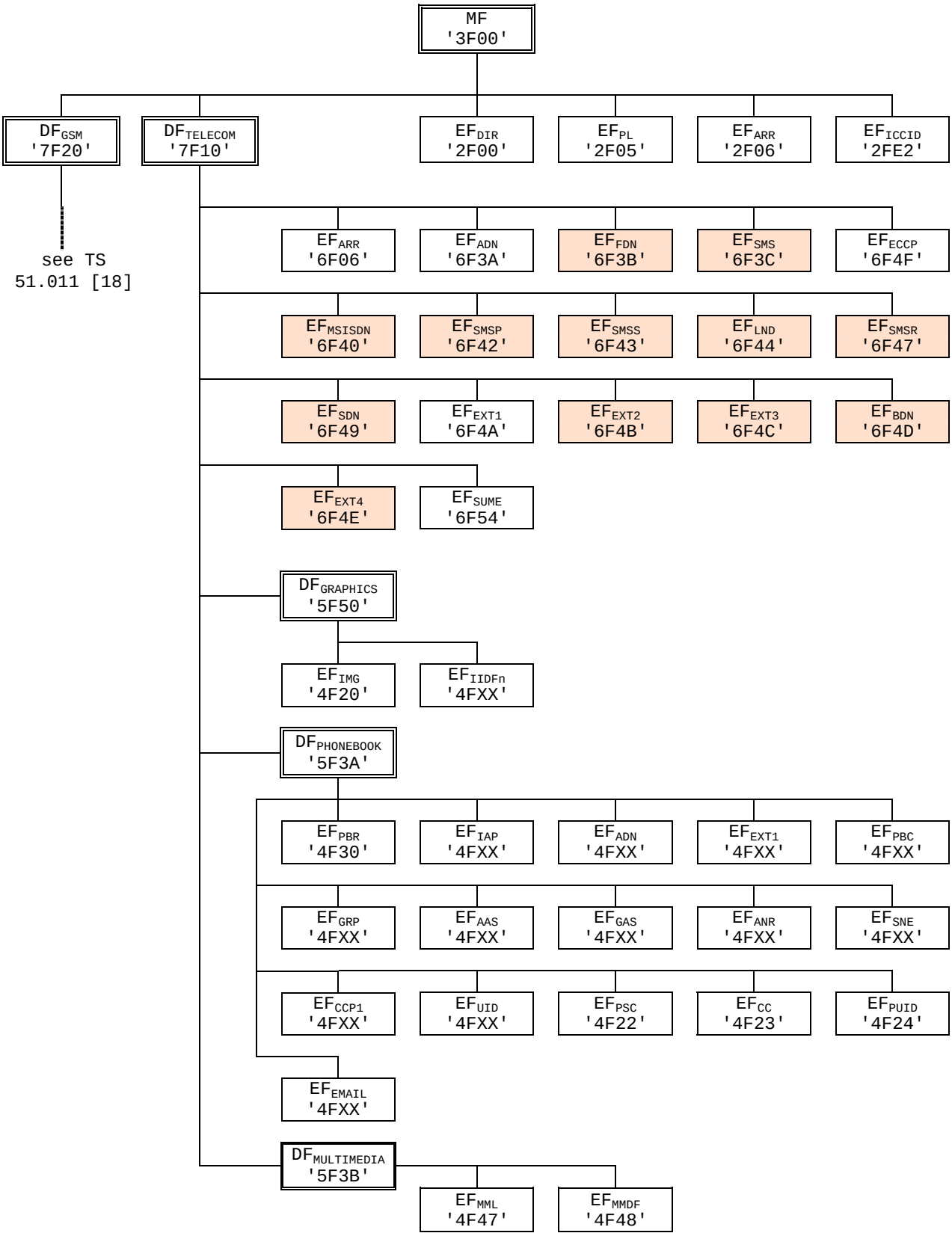
1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

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.

4.7 Files of USIM

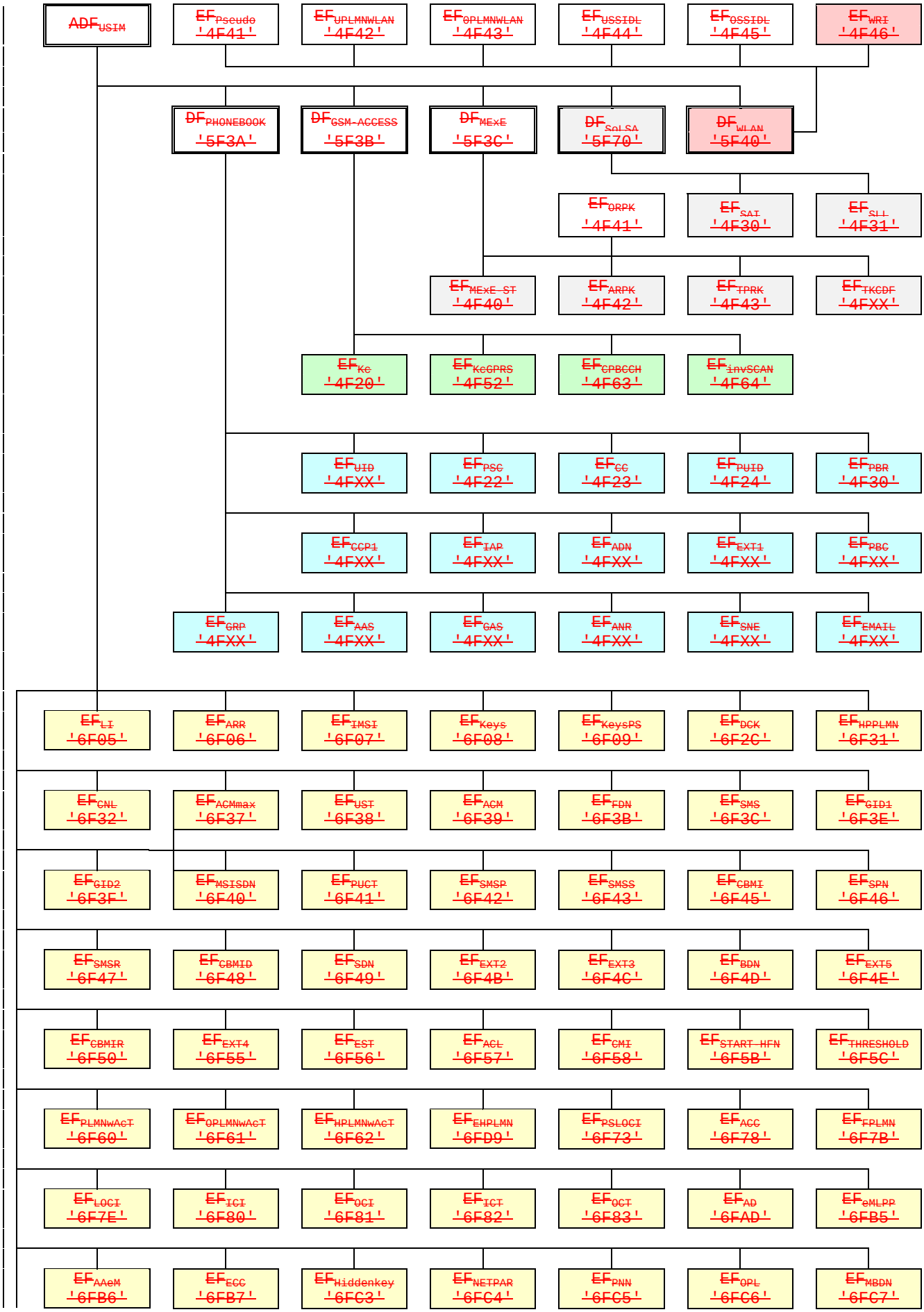
This clause contains two figures depicting the file structure of the UICC and the ADF_{USIM}. ADF_{USIM} shall be selected using the AID and information in EF_{DIR}.



NOTE 1: Files under $DF_{TELECOM}$ with shaded background are defined in TS 51.011 [18].

NOTE 2: The value '6F65' under ADFUSIM was used in earlier versions of this specification, and should not be re-assigned in future versions.

Figure 4.1: File identifiers and directory structures of UICC


ADF USIM
EF Pseudo '4F41'
EF UPLMNWLAN '4F42'
EF OPLMNWLAN '4F43'
EF USSIDL '4F44'
EF OSSIDL '4F45'
EF WRI '4F46'
DF PHONEBOOK '5F3A'
DF GSM-ACCESS '5F3B'
DF MExE '5F3C'
DF SoLSA '5F70'
DF WLAN '5F40'
EF ORPK '4F41'
EF SAI '4F30'
EF SLI '4F31'
EF MExE-ST '4F40'
EF ARPK '4F42'
EF TPRK '4F43'
EF TKCDF '4FXX'
EF Kc '4F20'
EF KcGPRS '4F52'
EF CPBCCH '4F63'
EF invSCAN '4F64'
EF UID '4FXX'
EF PSC '4F22'
EF CC '4F23'
EF PUID '4F24'
EF PBR '4F30'
EF CCP1 '4FXX'
EF IAP '4FXX'
EF ADN '4FXX'
EF EXT1 '4FXX'
EF PBC '4FXX'
EF GRP '4FXX'
EF AAS '4FXX'
EF GAS '4FXX'
EF ANR '4FXX'
EF SNE '4FXX'
EF EMAIL '4FXX'
EF LI '6F05'
EF ARR '6F06'
EF IMSI '6F07'
EF Keys '6F08'
EF KeysPS '6F09'
EF DCK '6F2C'
EF HPPLMN '6F31'
EF CNL '6F32'
EF ACMmax '6F37'
EF UST '6F38'
EF ACM '6F39'
EF FDN '6F3B'
EF SMS '6F3C'
EF GID1 '6F3E'
EF GID2 '6F3F'
EF MSISDN '6F40'
EF PUCT '6F41'
EF SMSP '6F42'
EF SMSS '6F43'
EF CBMI '6F45'
EF SPN '6F46'
EF SMSR '6F47'
EF CBMID '6F48'
EF SDN '6F49'
EF EXT2 '6F4B'
EF EXT3 '6F4C'
EF BDN '6F4D'
EF EXT5 '6F4E'
EF CBMIR '6F50'
EF EXT4 '6F55'
EF EST '6F56'
EF ACL '6F57'
EF CMI '6F58'
EF START-HFN '6F5B'
EF THRESHOLD '6F5C'
EF PLMNwAcT '6F60'
EF OPLMNwAcT '6F61'
EF HPLMNwAcT '6F62'
EF EHPLMN '6FD9'
EF PSLOCI '6F73'
EF ACC '6F78'
EF FPLMN '6F7B'
EF LOCI '6F7E'
EF ICI '6F80'
EF OCI '6F81'
EF ICT '6F82'
EF OCT '6F83'
EF AD '6FAD'
EF eMLPP '6FB5'
EF AAeM '6FB6'
EF ECC '6FB7'
EF Hiddenkey '6FC3'
EF NETPAR '6FC4'
EF PNN '6FC5'
EF OPL '6FC6'
EF MBDN '6FC7'

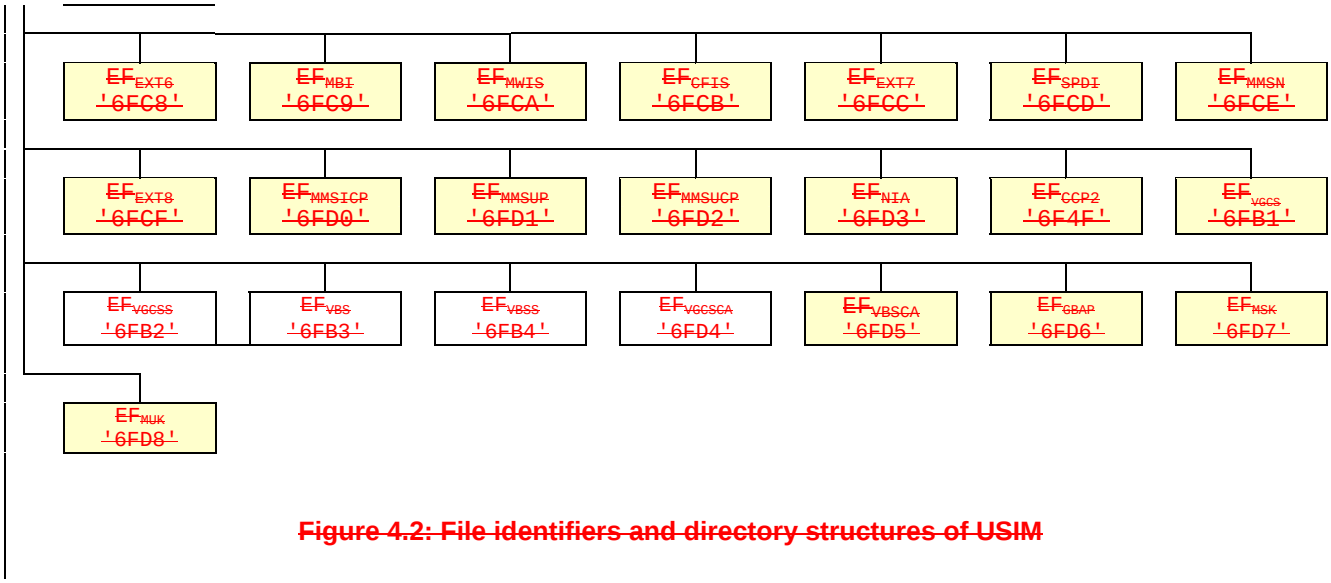
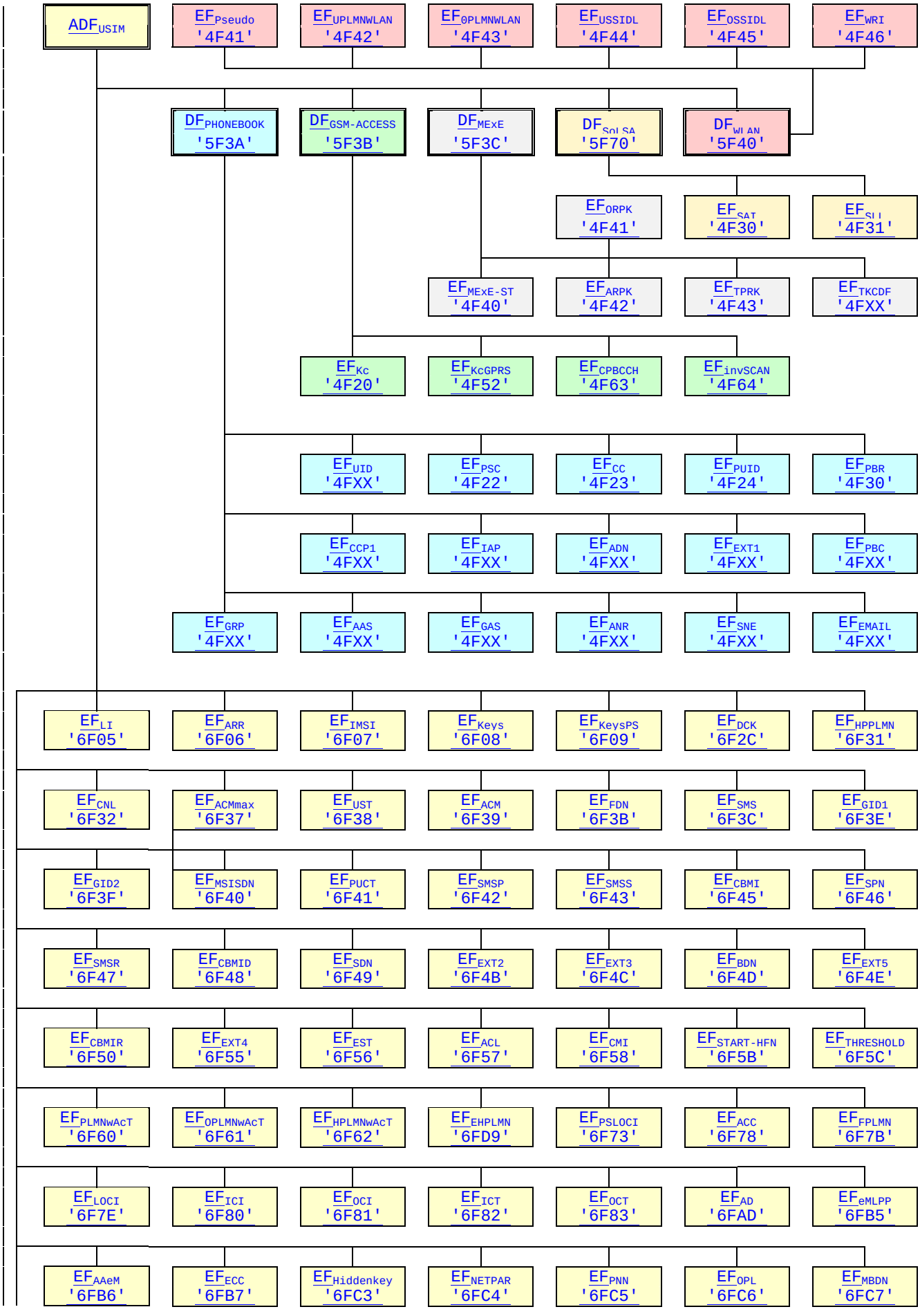


Figure 4.2: File identifiers and directory structures of USIM


ADF USIM
EF Pseudo '4F41'
EF UPLMNWLAN '4F42'
EF 0PLMNWLAN '4F43'
EF USSIDL '4F44'
EF OSSIDL '4F45'
EF WRI '4F46'
DF PHONEBOOK '5F3A'
DF GSM-ACCESS '5F3B'
DF MExE '5F3C'
DF SoLSA '5F70'
DF WLAN '5F40'
EF ORPK '4F41'
EF SAT '4F30'
EF SLL '4F31'
EF MExE-ST '4F40'
EF ARPK '4F42'
EF TPRK '4F43'
EF TKCDF '4FXX'
EF Kc '4F20'
EF KcGPRS '4F52'
EF CPBCCH '4F63'
EF invSCAN '4F64'
EF UID '4FXX'
EF PSC '4F22'
EF CC '4F23'
EF PUID '4F24'
EF PBR '4F30'
EF CCP1 '4FXX'
EF IAP '4FXX'
EF ADN '4FXX'
EF EXT1 '4FXX'
EF PBC '4FXX'
EF GRP '4FXX'
EF AAS '4FXX'
EF GAS '4FXX'
EF ANR '4FXX'
EF SNE '4FXX'
EF EMAIL '4FXX'
EF LI '6F05'
EF ARR '6F06'
EF IMSI '6F07'
EF Keys '6F08'
EF KeysPS '6F09'
EF DCK '6F2C'
EF HPPLMN '6F31'
EF CNL '6F32'
EF ACMmax '6F37'
EF UST '6F38'
EF ACM '6F39'
EF FDN '6F3B'
EF SMS '6F3C'
EF GID1 '6F3E'
EF GID2 '6F3F'
EF MSISDN '6F40'
EF PUCT '6F41'
EF SMSP '6F42'
EF SMSS '6F43'
EF CBMI '6F45'
EF SPN '6F46'
EF SMSR '6F47'
EF CBMID '6F48'
EF SDN '6F49'
EF EXT2 '6F4B'
EF EXT3 '6F4C'
EF BDN '6F4D'
EF EXT5 '6F4E'
EF CBMIR '6F50'
EF EXT4 '6F55'
EF EST '6F56'
EF ACL '6F57'
EF CMI '6F58'
EF START-HFN '6F5B'
EF THRESHOLD '6F5C'
EF PLMNwAcT '6F60'
EF OPLMNwAcT '6F61'
EF HPLMNwAcT '6F62'
EF EHPLMN '6FD9'
EF PSLOCI '6F73'
EF ACC '6F78'
EF FPLMN '6F7B'
EF LOCI '6F7E'
EF ICI '6F80'
EF OCI '6F81'
EF ICT '6F82'
EF OCT '6F83'
EF AD '6FAD'
EF eMLPP '6FB5'
EF AAeM '6FB6'
EF ECC '6FB7'
EF Hiddenkey '6FC3'
EF NETPAR '6FC4'
EF PNN '6FC5'
EF OPL '6FC6'
EF MBDN '6FC7'

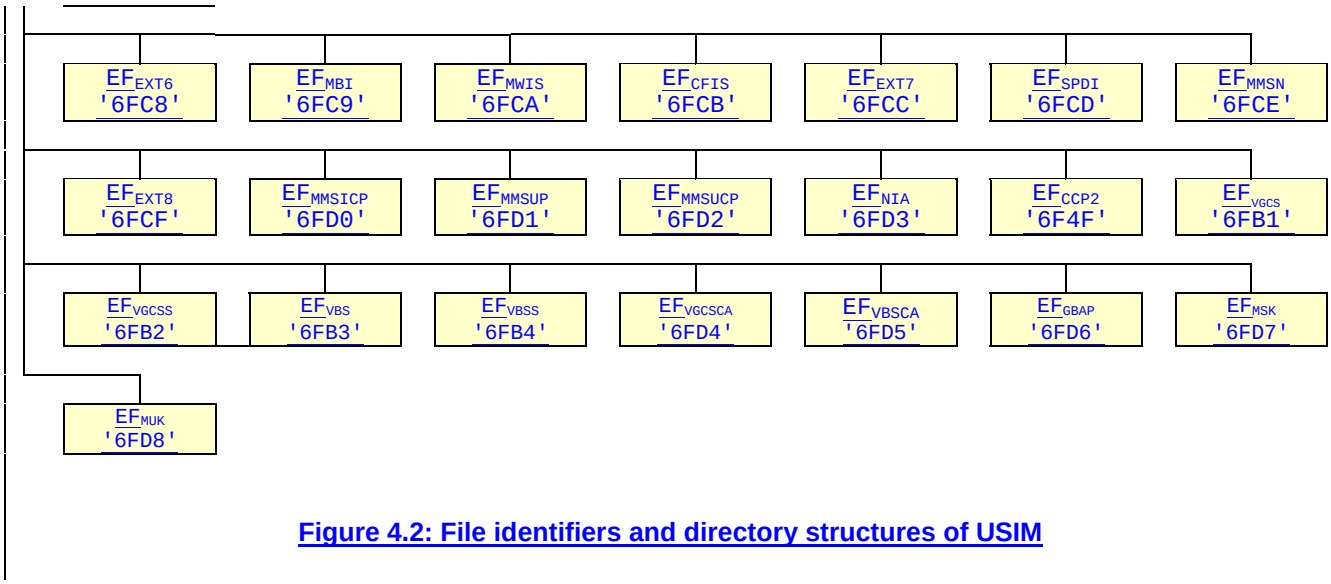


Figure 4.2: File identifiers and directory structures of USIM

3GPP TSG T WG3 Meeting #35
Barcelona, Spain, 8th – 11th February 2005

T3-050137
(revised from T3-050035)

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.102** **CR** **262** ⌘ **rev** **-** ⌘ Current version: **5.11.0** ⌘

*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:	⌘	Oddity signed Service Numbers in EF_UST
Source:	⌘	T3
Work item code:	⌘	TEI-5
Date:	⌘	09/02/2005
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:
Ph2 (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)
Rel-7 (Release 7)

Reason for change:	⌘	The Service numbers for VGCS Group Identifier List and VBS Group Identifier List should be Service n° 57 and Service n° 58 and not Service n°XX and n°YY. This is an result of an incorrect implemented CR.
Summary of change:	⌘	Modified oddity signed Service Number in EF_UST
Consequences if not approved:	⌘	Oddity signed service numbers in USIM Service table

Clauses affected:	⌘	4.2.8

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

Other comments: ⌘ All other releases of the specification are correct implemented.

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.

4.2.8 EF_{UST} (USIM Service Table)

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

Identifier: '6F38'	Structure: transparent	Mandatory
SFI: '04'		
File size: X bytes, X >= 1	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

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

-Services

Contents:		
	Service n°1:	Local Phone Book
	Service n°2:	Fixed Dialling Numbers (FDN)
	Service n°3:	Extension 2
	Service n°4:	Service Dialling Numbers (SDN)
	Service n°5:	Extension3
	Service n°6:	Barred Dialling Numbers (BDN)
	Service n°7:	Extension4
	Service n°8:	Outgoing Call Information (OCI and OCT)
	Service n°9:	Incoming Call Information (ICI and ICT)
	Service n°10:	Short Message Storage (SMS)
	Service n°11:	Short Message Status Reports (SMSR)
	Service n°12:	Short Message Service Parameters (SMSP)
	Service n°13:	Advice of Charge (AoC)
	Service n°14:	Capability Configuration Parameters (CCP)
	Service n°15:	Cell Broadcast Message Identifier
	Service n°16:	Cell Broadcast Message Identifier Ranges
	Service n°17:	Group Identifier Level 1
	Service n°18:	Group Identifier Level 2
	Service n°19:	Service Provider Name
	Service n°20:	User controlled PLMN selector with Access Technology
	Service n°21:	MSISDN
	Service n°22:	Image (IMG)
	Service n°23:	Support of Localised Service Areas (SoLSA)
	Service n°24:	Enhanced Multi-Level Precedence and Pre-emption Service
	Service n°25:	Automatic Answer for eMLPP
	Service n°26:	RFU
	Service n°27:	GSM Access
	Service n°28:	Data download via SMS-PP
	Service n°29:	Data download via SMS-CB
	Service n°30:	Call Control by USIM
	Service n°31:	MO-SMS Control by USIM
	Service n°32:	RUN AT COMMAND command
	Service n°33:	shall be set to '1'
	Service n°34:	Enabled Services Table
	Service n°35:	APN Control List (ACL)
	Service n°36:	Depersonalisation Control Keys
	Service n°37:	Co-operative Network List
	Service n°38:	GSM security context
	Service n°39:	CPBCCH Information
	Service n°40:	Investigation Scan
	Service n°41:	MExE
	Service n°42:	Operator controlled PLMN selector with Access Technology
	Service n°43:	HPLMN selector with Access Technology
	Service n°44:	Extension 5
	Service n°45:	PLMN Network Name
	Service n°46:	Operator PLMN List
	Service n°47:	Mailbox Dialling Numbers
	Service n°48:	Message Waiting Indication Status
	Service n°49:	Call Forwarding Indication Status
	Service n°50:	Reserved and shall be ignored
	Service n°51:	Service Provider Display Information
	Service n°52	Multimedia Messaging Service (MMS)
	Service n°53	Extension 8
	Service n°54	Call control on GPRS by USIM
	Service n°55	MMS User Connectivity Parameters
	Service n°56	Network's indication of alerting in the MS (NIA)
	Service n°57~~xx~~	VGCS Group Identifier List (EF_{VGCS} and EF_{VGCSS})
	Service n°58~~yy~~	VBS Group Identifier List (EF_{VBS} and EF_{VBSS})

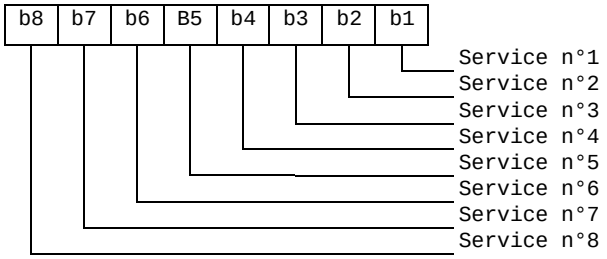
The EF shall contain at least one byte. Further bytes may be included, but if the EF includes an optional byte, then it is mandatory for the EF to also contain all bytes before that byte. Other services are possible in the future and will be coded on further bytes in the EF. The coding falls under the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

Coding:

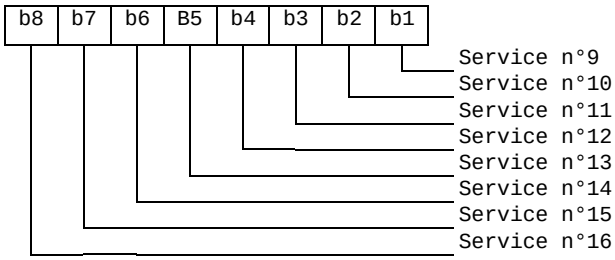
1 bit is used to code each service:
bit = 1: service available;
bit = 0: service not available.

- Service available means that the USIM has the capability to support the service and that the service is available for the user of the USIM unless the service is identified as "disabled" in EF_{EST}.
  Service not available means that the service shall not be used by the USIM user, even if the USIM has the capability to support the service.

First byte:



Second byte:



etc.

3GPP TSG-T3 #34
Barcelona, Spain, 8-11 February 2005

Tdoc ⌘T3-050143

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.102** **CR** 267 ⌘**rev** **-** ⌘ Current version: **6.8.0** ⌘

*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:	⌘	VGCS/VBS security: alignment with 43.020
Source:	⌘	T3
Work item code:	⌘	TEI6
Date:	⌘	09/02/05
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:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change:	⌘	The terminology used for the definition of the VGCS/VBS security context is not inline with TS 43.068. In fact, the octets 2-5 of the Descriptive group or broadcast call reference information element contain a group reference part (coded on 27 bits) and a service flag (coded on 1 bit to indicate the type of service: VGCS/VBS). TS 43.068 uses "Group_Id" to indicate part of octets 2-5 of the group reference part while TS 31.102 uses "Group_Id" to indicate the complete octets 2-5 of the group reference part. Add a note on Group_Id variable length.
Summary of change:	⌘	Rename the Group_ID field in section 7.1.2.2. Introduction of a clarification in section 7.1.1.3.
Consequences if not approved:	⌘	Misinterpretation of the VGCS/VBS terminology.

Clauses affected:	⌘	2, 7.1.1.3, 7.1.2.2

	Y	N		
Other specs affected: ⌘		X	Other core specifications	⌘
		X	Test specifications	
		X	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.

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 22.011: "Service accessibility".

[3] 3GPP TS 22.024: "Description of Charge Advice Information (CAI)".

[4] 3GPP TS 22.030: "Man-Machine Interface (MMI) of the User Equipment (UE)".

[5] 3GPP TS 23.038: "Alphabets and language".

[6] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)".

[7] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[8] 3GPP TS 22.067: "enhanced Multi Level Precedence and Pre-emption service (eMLPP) - Stage 1".

[9] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".

[10] 3GPP TS 24.011: "Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".

[11] 3GPP TS 31.101: "UICC-Terminal Interface, Physical and Logical Characteristics".

[12] 3GPP TS 31.111: "USIM Application Toolkit (USAT)".

[13] 3GPP TS 33.102: "3GPP Security; Security Architecture".

[14] 3GPP TS 33.103: "3GPP Security; Integration Guidelines".

[15] 3GPP TS 22.086: "Advice of charge (AoC) Supplementary Services - Stage 1".

[16] 3GPP TS 23.041: "Technical realization of Cell Broadcast (CB)".

[17] 3GPP TS 02.07: "Mobile Stations (MS) features".

[18] 3GPP TS 51.011 Release 4: "Specification of the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface".

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

[20] ISO/IEC 7816-4 (1995): "Identification cards - Integrated circuit(s) cards with contacts, Part 4: Interindustry commands for interchange".

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

[22] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

[23] 3GPP TS 23.073: "Support of Localised Service Area (SoLSA); Stage 2".

[24] 3GPP TS 22.101: "Service aspects; service principles".

[25] 3GPP TS 23.003: "Numbering, Addressing and Identification".

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

[27] 3GPP TS 22.022: "Personalisation of Mobile Equipment (ME); Mobile functionality specification".

[28] 3GPP TS 44.018 "Mobile Interface Layer3 Specification, Radio Resource control protocol"

[29] 3GPP TS 23.022: "Functions related to Mobile Station (MS) in idle mode and group receive mode".

[30] 3GPP TS 23.057: "Mobile Execution Environment (MExE);Functional description; Stage 2".

[31] 3GPP TS 23.122: "NAS Functions related to Mobile Station (MS) in idle mode"

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

[33] 3GPP TS 25.101: "UE Radio Transmission and Reception (FDD)"

[34] 3GPP TS 45.005: "Radio Transmission and Reception"

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

[36] 3GPP TS 23.097: "Multiple Subscriber Profile (MSP)"

[37] Void.

[38] 3GPP TS 23.140: “Multimedia Messaging Service (MMS); Functional description; stage 2”.

[39] ETSI TS 102 222 Release 6:"Administrative commands for telecommunications applications "

[40] 3GPP TS 24.234: “3GPP System to WLAN Interworking; UE to Network protocols;Stage 3”

[41] 3GPP TS 33.234: "3G Security; Wireless Local Area Network (WLAN) interworking security"

[42] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic bootstrapping architecture"

[43] 3GPP TS 33.246: "Security of Multimedia Broadcast/Multicast Service"

[44] 3GPP TS 43.020: "Technical Specification Group Services and system Aspects; Security related network functions"

[45] X.S0016-000-A v1.0: "3GPP2 Multimedia Messaging System MMS Specification Overview, Revision A"

[xx] 3GPP TS 43.068: "Technical Specification Group Core Network; Voice Group Call Service (VGCS); Stage 2"

7.1.1.3 VGCS/VBS security context

USIM operation in a VGCS/VBS security context is supported if Service n°64 or Service n°65 are "available".

The USIM computes the Short Term Key (VSTK) associated with a particular VGCS/VBS Group Identifier (Group_Id). For this computation, the USIM uses the- Voice Group (for VGCS) or Broadcast Group (for VBS) Key (V_Ki) identified by ~~the~~ their respective Group_Id and Master Group Key Identifier (VK_I-d). The USIM retrieves the Group_Id and the service flag (VGCS or VBS) from the received Voice Service Identifier (VService_Id).

NOTE: The Group_Id has a variable length according to TS 43.068 [xx].

The USIM shall first search if the Group_Id corresponds to a stored VGCS Group Identifier in EF_{VGCS} or a stored VBS Group Identifier in EF_{VBS}.

Then, the USIM shall retrieve the V_Ki corresponding to the given Group_Id and VK_Id.

Then the USIM uses V_Ki and VSTK_RAND as input parameters for the A8_V key derivation function (as defined in 3GPP TS 43.020 [44]) in order to compute and returns VSTK.

Input:

- VService~~Group~~_Id, VK_Id, VSTK_RAND

Output:

- VSTK.

7.1.2.2 VGCS/VBS security context

Byte(s)	Description	Length
1	Length of VService_Id~~VGCS_ID (L1)~~	1
2 to 5	VService~~Group~~_Id	4
6	Length of VK_Id	1
7	VK_Id	1
8	Length of VSTK_RAND (L1)	1
9 to L1+8	VSTK_RAND	L1

~~Group~~VService_Id is coded in the same way as the octets 2-5 in the Descriptive group or broadcast call reference information element as defined in TS 24.008 [9].
The coding of VK_Id is as follows:

Coding of VK_Id

Coding b8-b1	Meaning
'00000001'	Corresponds to the 1st group key
'00000010'	Corresponds to the 2nd group key

The coding of VSTK_RAND is described in TS 43.020 [44].

Response parameters/data, VGCS/VBS security context, command successful:

Byte(s)	Description	Length
1	"Successful VGCS/VBS operation" tag = 'DB'	1
2	Length of VSTK (16)	1
3 to 18	VSTK	16

3GPP TSG-T3 Meeting #34
Barcelona, Spain, 8th – 11th February 2005

Tdoc ⌘T3-050161

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.102** **CR** **263** ⌘ **rev** **-** ⌘ Current version: **6.8.0** ⌘

*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:	⌘	Correction due to inclusion of EHPLMN in wrong release
Source:	⌘	T3
Work item code:	⌘	TEI6
Date:	⌘	10/02/2005
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:
Ph2 (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)
Rel-7 (Release 7)

Reason for change:	⌘	The feature EHPLMN feature was incorrectly introduced into Release 6, rather than Release 7, of TS 31.102. SA1 and CN1 introduced these changes into Rel-7.
Summary of change:	⌘	Remove changes made to introduce the new file EF_{EHPLMN} and procedures related to the usage of the data field
Consequences if not approved:	⌘	Misalignment of specifications

Clauses affected:	⌘	3.1, 4.2.8, 4.2.xx, 4.7, 5.1.1.2, 5.2.yy, 5.3.zz, Annex A, Annex E

Other specs affected:	Y	N		
⌘		X	Other core specifications	⌘
		X	Test specifications	
		X	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.

3 Definitions, symbols, abbreviations and coding conventions

3.1 Definitions

For the purposes of the present document, the following definition applies.

ADM: access condition to an EF which is under the control of the authority which creates this file

~~**EHPLMN**: represents the Equivalent HPLMNs for network selection purposes. The usage of EHPLMNs is defined in TS 23.122 [31].~~

======== Next modification==========

4.2.8 EF_{UST} (USIM Service Table)

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

Identifier: '6F38'	Structure: transparent	Mandatory
SFI: '04'		
File size: X bytes, X >= 1	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

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

-Services

Contents:	Service n°1:	Local Phone Book
	Service n°2:	Fixed Dialling Numbers (FDN)
	Service n°3:	Extension 2
	Service n°4:	Service Dialling Numbers (SDN)
	Service n°5:	Extension3
	Service n°6:	Barred Dialling Numbers (BDN)
	Service n°7:	Extension4
	Service n°8:	Outgoing Call Information (OCI and OCT)
	Service n°9:	Incoming Call Information (ICI and ICT)
	Service n°10:	Short Message Storage (SMS)
	Service n°11:	Short Message Status Reports (SMSR)
	Service n°12:	Short Message Service Parameters (SMSP)
	Service n°13:	Advice of Charge (AoC)
	Service n°14:	Capability Configuration Parameters (CCP)
	Service n°15:	Cell Broadcast Message Identifier
	Service n°16:	Cell Broadcast Message Identifier Ranges
	Service n°17:	Group Identifier Level 1
	Service n°18:	Group Identifier Level 2
	Service n°19:	Service Provider Name
	Service n°20:	User controlled PLMN selector with Access Technology
	Service n°21:	MSISDN
	Service n°22:	Image (IMG)
	Service n°23:	Support of Localised Service Areas (SoLSA)
	Service n°24:	Enhanced Multi-Level Precedence and Pre-emption Service
	Service n°25:	Automatic Answer for eMLPP
	Service n°26:	RFU
	Service n°27:	GSM Access
	Service n°28:	Data download via SMS-PP
	Service n°29:	Data download via SMS-CB
	Service n°30:	Call Control by USIM
	Service n°31:	MO-SMS Control by USIM
	Service n°32:	RUN AT COMMAND command
	Service n°33:	shall be set to '1'
	Service n°34:	Enabled Services Table
	Service n°35:	APN Control List (ACL)
	Service n°36:	Depersonalisation Control Keys
	Service n°37:	Co-operative Network List
	Service n°38:	GSM security context
	Service n°39:	CPBCCH Information
	Service n°40:	Investigation Scan
	Service n°41:	MExE
	Service n°42:	Operator controlled PLMN selector with Access Technology
	Service n°43:	HPLMN selector with Access Technology
	Service n°44:	Extension 5
	Service n°45:	PLMN Network Name
	Service n°46:	Operator PLMN List
	Service n°47:	Mailbox Dialling Numbers
	Service n°48:	Message Waiting Indication Status
	Service n°49:	Call Forwarding Indication Status
	Service n°50:	Reserved and shall be ignored
	Service n°51:	Service Provider Display Information
	Service n°52	Multimedia Messaging Service (MMS)
	Service n°53	Extension 8
	Service n°54	Call control on GPRS by USIM
	Service n°55	MMS User Connectivity Parameters
	Service n°56	Network's indication of alerting in the MS (NIA)
	Service n°57	VGCS Group Identifier List (EF_{VGCS} and EF_{VGCSS})
	Service n°58	VBS Group Identifier List (EF_{VBS} and EF_{VBSS})
	Service n°59	Pseudonym
	Service n°60	User Controlled PLMN selector for WLAN access
	Service n°61	Operator Controlled PLMN selector for WLAN access
	Service n°62	User controlled WSID list
	Service n°63	Operator controlled WSID list
	Service n°64	VGCS security
	Service n°65	VBS security
	Service n°66	WLAN Reauthentication Identity
	Service n°67	Multimedia Messages Storage
	Service n°68	Generic Bootstrapping Architecture (GBA)

Service n°69	MBMS security
Service n°70	Data download via USSD and USSD application mode
~~Service n°71~~	~~Equivalent HPLMN~~

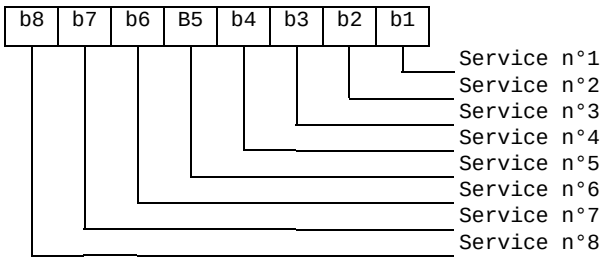
The EF shall contain at least one byte. Further bytes may be included, but if the EF includes an optional byte, then it is mandatory for the EF to also contain all bytes before that byte. Other services are possible in the future and will be coded on further bytes in the EF. The coding falls under the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

Coding:

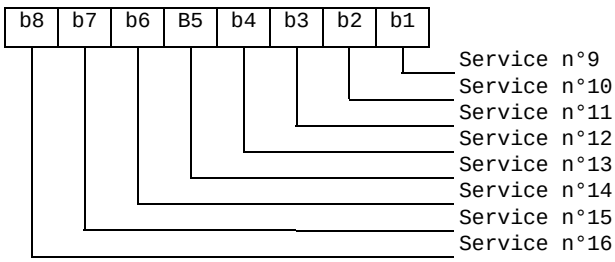
1 bit is used to code each service:
bit = 1: service available;
bit = 0: service not available.

- Service available means that the USIM has the capability to support the service and that the service is available for the user of the USIM unless the service is identified as "disabled" in EF_{EST}.
  Service not available means that the service shall not be used by the USIM user, even if the USIM has the capability to support the service.

First byte:



Second byte:



etc.

========== Next Modification ==========

4.2.82 Void~~EF$_{EHPLMN}$ (Equivalent HPLMN)~~

~~If service n°71 is "available", this file shall be present.~~

~~This EF contains the coding for n EHPLMNs. The usage of EHPLMN is defined in 23.122 [31]. This data field shall not contain the HPLMN code derived from the IMSI as an EHPLMN entry.~~

Identifier: '6FD9'	Structure: transparent	Optional
SFI: 'xx'		
File size: 3*n (where n ≥1)	Update activity: low	

Access Conditions:
READ PIN
UPDATE ADM
DEACTIVATE ADM
ACTIVATE ADM

Bytes	Description	M/O	Length
1 to 3	1st EHPLMN (highest priority)	M	3 bytes
4 to 6	2nd EHPLMN	O	3 bytes
:	:		
(3n-2) to (3n)	nth EHPLMN (lowest priority)	O	3 bytes

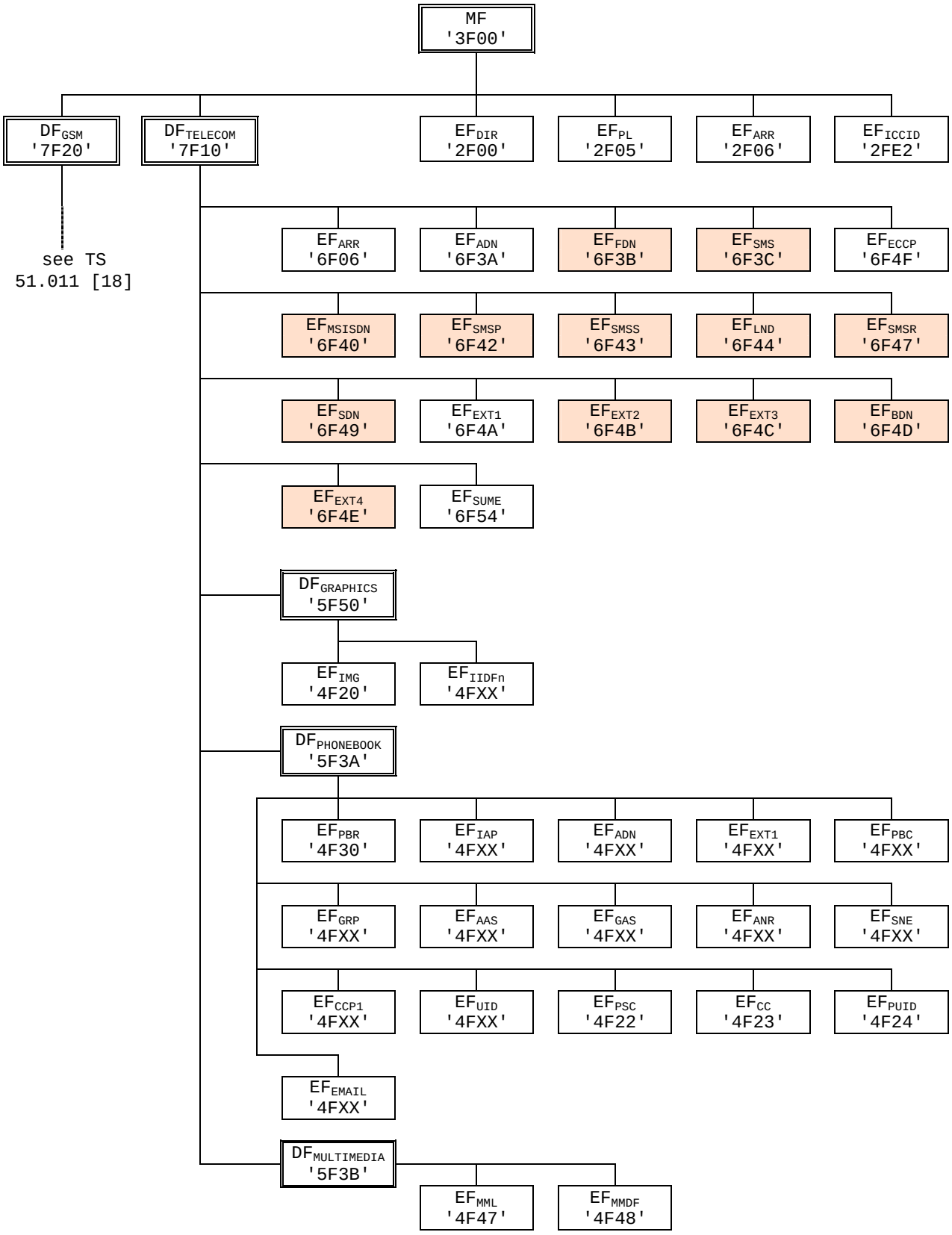
EHPLMN
Contents:
Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).
Coding:
according to TS 24.008 [9].

Unused entries shall be set to 'FF FF FF'

========== Next Change ==========

4.7 Files of USIM

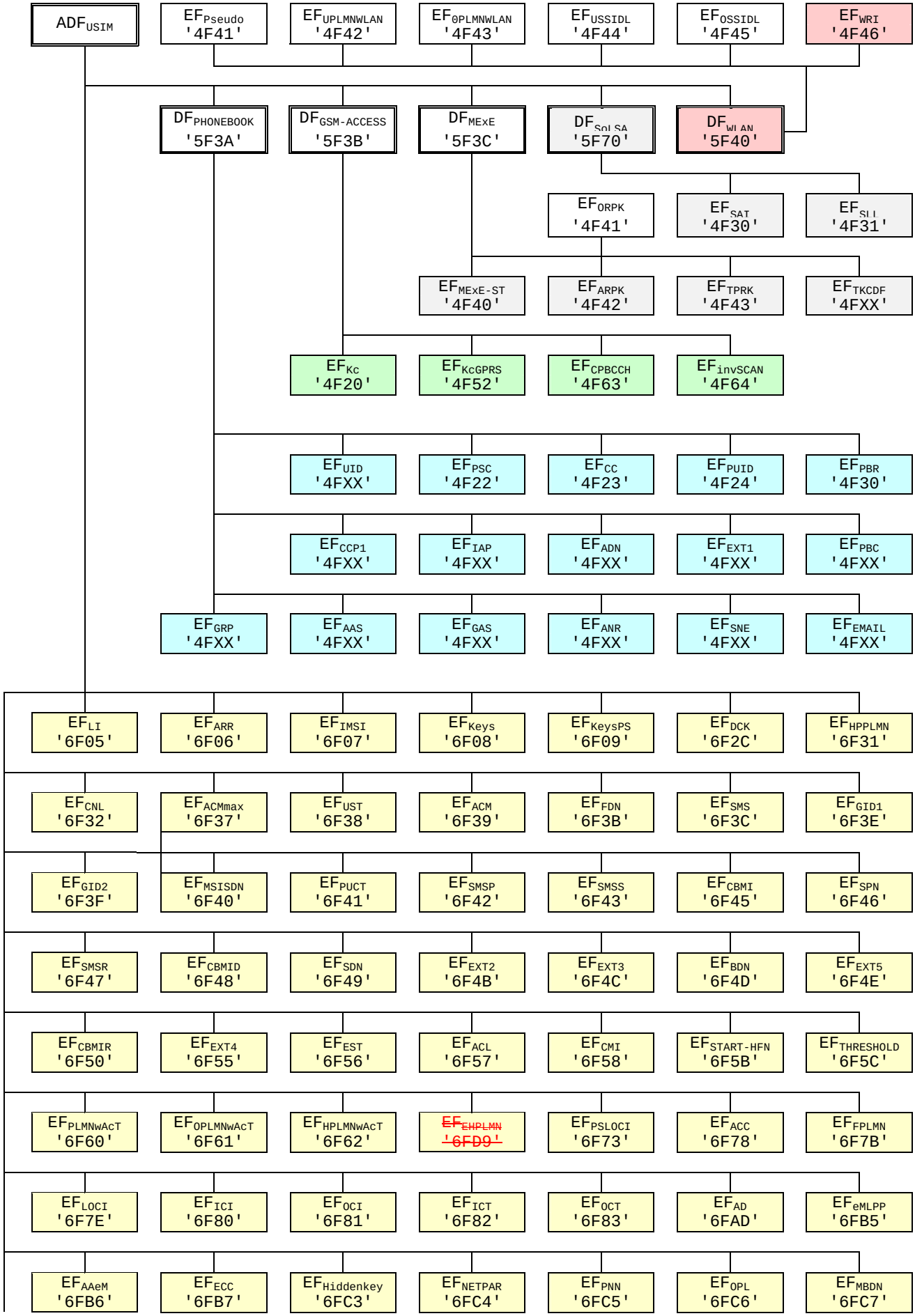
This clause contains two figures depicting the file structure of the UICC and the ADF_{USIM}. ADF_{USIM} shall be selected using the AID and information in EF_{DIR}.



NOTE 1: Files under $DF_{TELECOM}$ with shaded background are defined in TS 51.011 [18].

NOTE 2: The value '6F65' under ADFUSIM was used in earlier versions of this specification, and should not be re-assigned in future versions.

Figure 4.1: File identifiers and directory structures of UICC


ADF USIM
EF Pseudo '4F41'
EF UPLMNWLAN '4F42'
EF 0PLMNWLAN '4F43'
EF USSIDL '4F44'
EF OSSIDL '4F45'
EF WRI '4F46'
DF PHONEBOOK '5F3A'
DF GSM-ACCESS '5F3B'
DF MExE '5F3C'
DF SoLSA '5F70'
DF WLAN '5F40'
EF ORPK '4F41'
EF SAT '4F30'
EF SLI '4F31'
EF MExE-ST '4F40'
EF ARPK '4F42'
EF TPRK '4F43'
EF TKCDF '4FXX'
EF Kc '4F20'
EF KcGPRS '4F52'
EF CPBCCH '4F63'
EF invSCAN '4F64'
EF UID '4FXX'
EF PSC '4F22'
EF CC '4F23'
EF PUID '4F24'
EF PBR '4F30'
EF CCP1 '4FXX'
EF IAP '4FXX'
EF ADN '4FXX'
EF EXT1 '4FXX'
EF PBC '4FXX'
EF GRP '4FXX'
EF AAS '4FXX'
EF GAS '4FXX'
EF ANR '4FXX'
EF SNE '4FXX'
EF EMAIL '4FXX'
EF LI '6F05'
EF ARR '6F06'
EF IMSI '6F07'
EF Keys '6F08'
EF KeysPS '6F09'
EF DCK '6F2C'
EF HPPLMN '6F31'
EF CNL '6F32'
EF ACMmax '6F37'
EF UST '6F38'
EF ACM '6F39'
EF FDN '6F3B'
EF SMS '6F3C'
EF GID1 '6F3E'
EF GID2 '6F3F'
EF MSISDN '6F40'
EF PUCT '6F41'
EF SMSP '6F42'
EF SMSS '6F43'
EF CBMI '6F45'
EF SPN '6F46'
EF SMSR '6F47'
EF CBMID '6F48'
EF SDN '6F49'
EF EXT2 '6F4B'
EF EXT3 '6F4C'
EF BDN '6F4D'
EF EXT5 '6F4E'
EF CBMIR '6F50'
EF EXT4 '6F55'
EF EST '6F56'
EF ACL '6F57'
EF CMI '6F58'
EF START-HFN '6F5B'
EF THRESHOLD '6F5C'
EF PLMNwAcT '6F60'
EF OPLMNwAcT '6F61'
EF HPLMNwAcT '6F62'
EF EHPLMN '6FD9'
EF PSLOCI '6F73'
EF ACC '6F78'
EF FPLMN '6F7B'
EF LOCI '6F7E'
EF ICI '6F80'
EF OCI '6F81'
EF ICT '6F82'
EF OCT '6F83'
EF AD '6FAD'
EF eMLPP '6FB5'
EF AAeM '6FB6'
EF ECC '6FB7'
EF Hiddenkey '6FC3'
EF NETPAR '6FC4'
EF PNN '6FC5'
EF OPL '6FC6'
EF MBDN '6FC7'

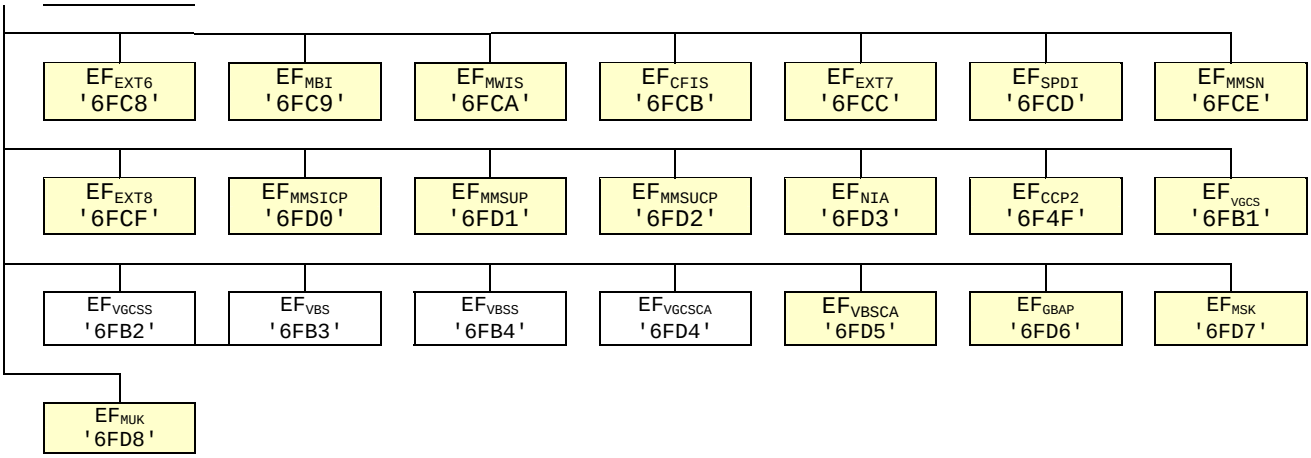


Figure 4.2: File identifiers and directory structures of USIM

========== Next Modification ==========

5.1.1.2 USIM initialisation

The ME requests the emergency call codes. For service requirements, see TS 22.101 [24].

The ME requests the Language Indication. The preferred language selection shall always use the EF_{LI} in preference to the EF_{PL} at the MF unless any of the following conditions applies:

- if the EF_{LI} has the value 'FFFF' in its highest priority position, then the preferred language selection shall be the language preference in the EF_{PL} at the MF level according the procedure defined in TS 31.101[11];
- if the ME does not support any of the language codes indicated in EF_{LI}, or if EF_{LI} is not present, then the language selection shall be as defined in EF_{PL} at the MF level according the procedure defined in TS 31.101[11];
- if neither the languages of EF_{LI} nor EF_{PL} are supported by the terminal, then the terminal shall use its own internal default selection.

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

The ME performs the administrative information request.

The ME performs the USIM Service Table request.

The ME performs the Enabled Services Table Request.

In case FDN is enabled, an ME which does not support FDN shall allow emergency calls but shall not allow MO-CS calls and MO-SMS.

If BDN is enabled, an ME which does not support Call Control shall allow emergency calls but shall not allow MO-CS calls.

If ACL is enabled, an ME which does not support ACL shall not send any APN to the network.

If all these procedures have been performed successfully then 3G session shall start. In all other cases 3G session shall not start.

Afterwards, the ME runs the following procedures if the ME and the USIM support the related services:

- IMSI request;
- Access control information request;
- Higher Priority PLMN search period request;

~~- EHPLMN request;~~

- HPLMN selector with Access Technology request;
- User controlled PLMN selector with Access Technology request;
- Operator controlled PLMN selector with Access Technology request;
- GSM initialisation requests;
- Location Information request for CS-and/or PS-mode;
- Cipher key and integrity key request for CS- and/or PS-mode;
- Forbidden PLMN request;
- Initialisation value for hyperframe number request;
- Maximum value of START request;
- CBMID request;
- Depending on the further services that are supported by both the ME and the USIM the corresponding EFs have to be read.

After the USIM initialisation has been completed successfully, the ME is ready for a 3G session and shall indicate this to the USIM by sending a particular STATUS command.

========== Next Modification ==========

5.2.24 Void~~EHPLMN request~~

~~Requirement: Service n°yy "available".~~

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

========== Next Modification ==========

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

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

File identification	Description	Change advised
'2F00'	Application directory	Caution
'2F05'	Preferred languages	Yes
'2F06'	Access rule reference	Caution
'2FE2'	ICC identification	No
'4F20'	Image data	Yes
'4F20'	GSM Ciphering key Kc	No
'4FXX'	Image Instance data Files	Yes
'4FXX'	Unique identifier	Yes
'4F22'	Phone book synchronisation counter	Yes
'4F23'	Change counter	Yes
'4F24'	Previous unique identifier	Yes
'4F30'	Phone book reference file	Yes
'4FXX'	Capability configuration parameters 1	Yes
'4F30'	SoLSA Access Indicator	Caution
'4F31'	SoLSA LSA List	Caution
'4FXX'	LSA Descriptor files	Caution
'4F52'	GPRS Ciphring key KcGPRS	No
'4F63'	CPBCCH Information	No
'4F64'	Investigation Scan	Caution
'4FXX'	Additional number alpha string	Yes
'4FXX'	Additional number	Yes
'4FXX'	Second name entry	Yes
'4FXX'	Grouping information alpha string	Yes
'4FXX'	Phone book control	Yes
'4FXX'	E-mail addresses	Yes
'4FXX'	Index administration phone book	Yes
'4FXX'	Extension 1	Yes
'4FXX'	Abbreviated dialling numbers	Yes
'4FXX'	Grouping file	Yes
'4F41'	Pseudonym	Caution
'4F42'	User controlled PLMN selector for WLAN	No
'4F43'	Operator controlled PLMN selector for WLAN	Caution
'4F44'	User controlled WSID List	No
'4F45'	Operator controlled WSID List	Caution
'4F46'	WLAN Reauthentication Identity	No
'4F47'	Multimedia Messages List	Yes
'4F48'	Multimedia Messages Data File	Yes
'6F05'	Language indication	Yes
'6F06'	Access rule reference (under ADF_{USIM} and $DF_{TELECOM}$)	Caution
'6F07'	IMSI	Caution (Note 1)
'6F08'	Ciphering and integrity keys	No
'6F09'	Ciphering and integrity keys for packet switched domain	No
'6F2C'	De-personalization Control Keys	Caution
'6F31'	Higher Priority PLMN search period	Caution
'6F32'	Co-operative network list	Caution
'6F37'	ACM maximum value	Yes
'6F38'	USIM service table	Caution
'6F39'	Accumulated call meter	Yes
'6F3B'	Fixed dialling numbers	Yes
'6F3C'	Short messages	Yes
'6F3E'	Group identifier level 1	Yes
'6F3F'	Group identifier level 2	Yes

File identification	Description	Change advised
	Continued….	

File identification	Description	Change advised
'6F40'	MSISDN storage	Yes
'6F41'	PUCT	Yes
'6F42'	SMS parameters	Yes
'6F43'	SMS status	Yes
'6F45'	CBMI	Caution
'6F46'	Service provider name	Yes
'6F47'	Short message status reports	Yes
'6F48'	CBMID	Yes
'6F49'	Service Dialling Numbers	Yes
'6F4B'	Extension 2	Yes
'6F4C'	Extension 3	Yes
'6F4D'	Barred dialling numbers	Yes
'6F4E'	Extension 5	Yes
'6F4F'	Capability configuration parameters 2	Yes
'6F50'	CBMIR	Yes
'6F54'	SetUp Menu Elements	Yes
'6F55'	Extension 4	Yes
'6F56'	Enabled services table	Caution
'6F57'	Access point name control list	Yes
'6F58'	Comparison method information	Yes
'6F5B'	Initialisation value for Hyperframe number	Caution
'6F5C'	Maximum value of START	Yes
'6F60'	User controlled PLMN selector with Access Technology	No
'6F61'	Operator controlled PLMN selector with Access Technology	Caution
'6F62'	HPLMN selector with Access Technology	Caution
'6F73'	Packet switched location information	Caution
'6F78'	Access control class	Caution
'6F7B'	Forbidden PLMNs	Caution
'6F7E'	Location information	No (Note 1)
'6F80'	Incoming call information	Yes
'6F81'	Outgoing call information	Yes
'6F82'	Incoming call timer	Yes
'6F83'	Outgoing call timer	Yes
'6FAD'	Administrative data	Caution
'6FB1'	Voice Group Call Service	Yes
'6FB2'	Voice Group Call Service Status	Yes
'6FB3'	Voice Broadcast Service	Yes
'6FB4'	Voice Broadcast Service Status	Yes
'6FB5'	Enhanced Multi Level Pre-emption and Priority	Yes
'6FB6'	Automatic Answer for eMLPP Service	Yes
'6FB7'	Emergency Call Codes	Caution
'6FC3'	Key for hidden phone book entries	No
'6FC4'	Network Parameters	No
'6FC5'	PLMN Network Name	Yes
'6FC6'	Operator Network List	Yes
'6FC7'	Mailbox Dialling Numbers	Yes
'6FC8'	Extension 6	Yes
'6FC9'	Mailbox Identifier	Caution
'6FCA'	Message Waiting Indication Status	Caution
'6FCB'	Call Forwarding Indication Status	Caution
'6FCC'	Extension 7	Yes
'6FCD'	Service Provider Display Information	Yes
'6FCE'	MMS Notification	Yes
'6FCF'	Extension 8	Yes
'6FD0'	MMS Issuer Connectivity Parameters	Yes
'6FD1'	MMS User Preferences	Yes
'6FD2'	MMS User Connectivity Parameters	Yes
'6FD3'	Network's indication of alerting (NIA)	Caution
'6FD4'	Voice Group Call Service Ciphering Algorithm	Yes
'6FD5'	Voice Broadcast Service Ciphering Algorithm	Yes
'6FD6'	GBA Bootstrapping parameters	Caution
'6FD7'	MBMS Service Keys List	Caution

File identification	Description	Change advised
'6FD8'	MBMS User Key	Caution
~~'6FD9'~~	~~EHPLMN~~	~~Caution~~
NOTE1: If EF_{IMSI} is changed, the UICC should issue REFRESH as defined in TS 31.111 and update EF_{LOCI} accordingly.		

========== Next Modification ==========

Annex E (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
'2F00'	Application directory	Card issuer/operator dependant
'2F05'	Preferred languages	'FF…FF'
'2F06'	Access rule reference	Card issuer/operator dependant
'2FE2'	ICC identification	operator dependant
'4F20'	Image data	'00FF...FF'
'4F20'	GSM Ciphering key Kc	'FF...FF07'
'4FXX'	Image instance data files	'FF…FF'
'4FXX'	Unique identifier	'0000'
'4F22'	Phone book synchronisation counter	'00000000'
'4F23'	Change counter	'0000'
'4F24'	Previous unique identifier	'0000'
'4F30'	Phone book reference file	Operator dependant
'4F30'	SoLSA Access Indicator	'00FF...FF'
'4F31'	SoLSA LSA List	'FF...FF'
'4FXX'	LSA Descriptor files	'FF…FF'
'4FXX'	Capability configuration parameters 1	'FF…FF'
'4F52'	GPRS Ciphring key KcGPRS	'FF...FF07'
'4F63'	CPBCCH Information	'FF..FF'
'4F64'	Investigation PLMN scan	'00'
'4FXX'	E-mail addresses	'FF…FF'
'4FXX'	Additional number alpha string	'FF…FF'
'4FXX'	Second name entry	'FF…FF'
'4FXX'	Abbreviated dialling numbers	'FF...FF'
'4FXX'	Grouping file	'00…00'
'4FXX'	Grouping information alpha string	'FF…FF'
'4FXX'	Phone book control	'0000'
'4FXX'	Index administration phone book	'FF…FF'
'4FXX'	Additional number	'FF…FF'
'4FXX'	Extension 1	'00FF...FF'
'4F41'	Pseudonym	'00FF…FF'
'4F42'	User Controlled PLMN selector for WLAN	'FF…FF'
'4F43'	Operator Controlled PLMN selector for WLAN	Operator dependant
'4F44'	User Controlled WSID list	'00FF…FF'
'4F45'	Operator controlled WSID list	Operator dependant
'4F46'	WLAN Reauthentication Identity	'FF…FF'
'4F47'	Multimedia Messages List	'FF…FF'
'4F48'	Multimedia Messages Data File	'FF…FF'
'6F05'	Language indication	'FF…FF'
'6F06'	Access rule reference (under ADF_{USIM} and $DF_{TELECOM}$)	Card issuer/operator dependant
'6F07'	IMSI	Operator dependant
'6F08'	Ciphering and integrity keys	'07FF…FF'
'6F09'	Ciphering and integrity keys for packet switched domain	'07FF…FF'
'6F2C'	De-personalization control keys	'FF…FF'
'6F31'	Higher Priority PLMN search period	'FF'
'6F32'	Co-operative network list	'FF…FF'
'6F37'	ACM maximum value	'000000' (see note 1)
'6F38'	USIM service table	Operator dependant
'6F39'	Accumulated call meter	'000000'
'6F3B'	Fixed dialling numbers	'FF...FF'
'6F3C'	Short messages	'00FF...FF'
'6F3E'	Group identifier level 1	Operator dependant
'6F3F'	Group identifier level 2	Operator dependant
'6F40'	MSISDN storage	'FF...FF'
'6F41'	PUCT	'FFFFFF0000'
'6F42'	SMS parameters	'FF...FF'
'6F43'	SMS status	'FF...FF'
'6F45'	CBMI	'FF...FF'
'6F46'	Service provider name	Operator dependant
'6F47'	Short message status reports	'00FF…FF'
'6F48'	CBMID	'FF...FF'
'6F49'	Service Dialling Numbers	'FF...FF'

'6F4B'	Extension 2	'00FF...FF'
'6F4C'	Extension 3	'00FF...FF'

Continued....

File Identification	Description	Value
'6F4D'	Barred Dialling Numbers	'FF...FF'
'6F4E'	Extension 5	'00FF...FF'
'6F4F'	Capability configuration parameters 2	'FF...FF'
'6F50'	CBMIR	'FF...FF'
'6F54'	SetUp Menu Elements	Operator dependant
'6F55'	Extension 4	'00FF...FF'
'6F56'	Enabled services table	Operator dependant
'6F57'	Access point name control list	'00FF…FF'
'6F58'	Comparison method information	'FF…FF'
'6F5B'	Initialisation value for Hyperframe number	'F0 00 00 F0 00 00'
'6F5C'	Maximum value of START	Operator dependant
'6F60'	User controlled PLMN selector with Access Technology	'FFFFFF0000..FFFFFF0000'
'6F61'	Operator controlled PLMN selector with Access Technology	'FFFFFF0000..FFFFFF0000'
'6F62'	HPLMN selector with Access Technology	'FFFFFF0000..FFFFFF0000'
'6F73'	Packet switched location information	'FFFFFFFF FFFFFF xxxxxx 0000 FF 01' (see note 2)
'6F78'	Access control class	Operator dependant
'6F7B'	Forbidden PLMNs	'FF...FF'
'6F7E	Location information	'FFFFFFFF xxxxxx 0000 FF 01' (see note 2)
'6F80'	Incoming call information	'FF…FF 000000 00 01FFFF'
'6F81'	Outgoing call information	'FF…FF 000000 01FFFF'
'6F82'	Incoming call timer	'000000'
'6F83'	Outgoing call timer	'000000'
'6FAD'	Administrative data	Operator dependant
'6FB1'	Voice Group Call Service	Operator dependant
'6FB2'	Voice Group Call Service Status	Operator dependant
'6FB3'	Voice Broadcast Service	Operator dependant
'6FB4'	Voice Broadcast Service Status	Operator dependant
'6FB5'	EMLPP	Operator dependant
'6FB6'	AaeM	'00'
'6FB7'	Emergency call codes	Operator dependant
'6FC3'	Key for hidden phone book entries	'FF…FF'
'6FC4'	Network Parameters	'FF…FF'
'6FC5'	PLMN Network Name	Operator dependant
'6FC6'	Operator Network List	Operator dependant
'6FC7'	Mailbox Dialling Numbers	Operator dependant
'6FC8'	Extension 6	'00 FF...FF'
'6FC9'	Mailbox Identifier	Operator dependant
'6FCA'	Message Waiting Indication Status	'00 00 00 00 00'
'6FCB'	Call Forwarding Indication Status	'xx 00 FF...FF'
'6FCC'	Extension 7	'00 FF...FF'
'6FCD'	Service Provider Display Information	
'6FCE'	MMS Notification	'00 00 00 FF…FF'
'6FCF'	Extension 8	'00FF...FF'
'6FD0'	MMS Issuer Connectivity Parameters	'FF…FF'
'6FD1'	MMS User Preferences	'FF…FF'
'6FD2'	MMS User Connectivity Parameters	'FF…FF'
'6FD3'	Network's Indication of Alerting (NIA)	'FF...FF'
'6FD4'	Voice Group Call Service Ciphering Algorithm	'00…00'
'6FD5'	Voice Broadcast Service Ciphering Algorithm	'00…00'
'6FD6'	GBA Bootstrapping parameters	'FF…FF'
'6FD7'	MBMS Service Keys List	'FF…FF'
'6FD8'	MBMS User Key	'FF…FF'
~~'6FD9'~~	~~EHPLMN~~	~~'FF…FF' or xxxxxx (see Note 2)~~

NOTE 1: The value '000000' means that ACMmax is not valid, i.e. there is no restriction on the ACM. When assigning a value to ACMmax, care should be taken not to use values too close to the maximum possible value 'FFFFFF', because the INCREASE command does not update EF_{ACM} if the units to be added would exceed 'FFFFFF'. This could affect the call termination procedure of the Advice of Charge function.

NOTE 2: xxxxxx stands for any valid MCC and MNC, coded according to TS 24.008 [9].

3GPP TSG-T3 #34
Barcelona, Spain, 8-11 February 2005

Tdoc ⌘T3-050166

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.102** **CR** 268 ⌘**rev** **-** ⌘ Current version: **6.8.0** ⌘

*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:	⌘	MBMS security: alignment with TS 33.246
Source:	⌘	Axalto, Gemplus
Work item code:	⌘	TEI
Date:	⌘	9/02/2005
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:
Ph2 *(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)*
Rel-7 *(Release 7)*

Reason for change:	⌘	SP #26 has approved several CRs that impact the MBMS functionality specified in TS 31.102. The following changes has been applied to TS 33.246: • Network ID was renamed to Key Domain ID • MSK ID was redefined in TS 33.246, combining former MSK and Key Group IDs. • In the MSK update procedure, the MIKEY message has been updated to contain the whole MUK_ID, which includes the NAF_ID. Therefore it is no longer necessary to include the NAF_ID in the parameters of the AUTHENTICATE command, for the MSK update procedure. • Update the description of the MSK update procedure, to reflect the modifications that were adopted by SA3. • Update the type of EF_{MUK}, to reflect the fact that an ME can connect to several BM-SCs (one MUK per BM-SC is needed)
Summary of change:	⌘	The changes described above are reflected in TS 31.102
Consequences if not approved:	⌘	Discrepancies between TS 33.246 rel-6 and TS 31.102 rel-6.

Clauses affected:	⌘	4.2.80, 4.2.81, 7.1.1.6, 7.1.1.7, 7.1.1.8, 7.1.2.5, 7.3.1

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

Other comments: ⌘	

4.2.80 EF_{MSK} (MBMS Service Keys List)

~~This~~ A record of this EF contains the list of MBMS Service Keys (MSK) and associated parameters, which are related to an MBMS Key Domain~~Group~~. There are up to two MSKs per ~~Network Id~~Key Domain ID/Key Group ID pair, where the Key Group ID is the Key Group part of the MSK ID as defined in TS 33.246 [43]. Two 4 byte MSK IDs stored within a record have the same value for the 2 byte Key Group part. This file shall be present if the MBMS security service (service number 69) is allocated in EF_{UST} (USIM Service Table).

Identifier: '6FD7'	Structure: linear fixed	Optional
Record length: 19~~17~~ bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 3	Key Domain ID~~Network ID~~	M	3 bytes
~~4 to 5~~	~~Key Group ID~~	~~M~~	~~2 bytes~~
4 to 7~~6 to 7~~	1st MSK ID	M	4~~2~~ bytes
8 to 11	1st Time Stamp Counter (TS)	M	4 bytes
12 to 15~~3~~	2nd MSK ID	M	4~~2~~ bytes
16~~4~~ to 19~~7~~	2nd Time Stamp Counter (TS)	M	4 bytes

- ~~Network~~Key Domain ID:
  Content: Identifier of the ~~Network~~ Domain of the BM-SC providing MBMS Service
  Coding: As defined in TS 33.246 [43]

~~Key Group ID:~~
~~Content: Identifier of an MBMS Key Group.~~
~~Coding: As defined in TS 33.246 [43]~~

- MSK ID:
  Content: Identifier of MBMS Service Key (MSK) within a particular Key Domain~~Network/Key Group pair~~.
  Coding: As defined in TS 33.246 [43]

- Time Stamp Counter (TS)
  Content: Counter for MIKEY replay protection in MTK delivery. Each counter is associated with a particular MSK.
  Coding: As defined in TS 33.246 [43]

4.2.81 EF_{MUK} (MBMS User Key)

This EF contains the identifier of the MBMS User Key (MUK) that is used to protect the transfer of MBMS Service Keys (MSK). The file also contains the Time Stamp Counter associated with the MUK, which is used for Replay Protection in MSK transport messages. This file shall be present if the MBMS security service (service number 69) is allocated in EF_{UST} (USIM Service Table). This EF shall not contain MUK IDs with the same NAF_ID part.

Identifier: '6FD8'	Structure: ~~transparent~~ linear fixed	Optional
~~File~~ Record length: ~~Q+6~~Z bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to Z	MBMS User Key TLV objects~~Length of MUK ID (Q)~~	M	Z~~1~~ bytes
~~2 to Q+1~~	~~MUK ID~~	~~M~~	~~Q bytes~~
~~Q+2~~	~~Length of Time Stamp Counter (TS) (4)~~	~~M~~	~~1 byte~~
~~Q+3 to Q+6~~	~~Time Stamp Counter (TS)~~	~~M~~	~~4 bytes~~

- ~~Length of MUK ID~~
  ~~Contents: number of bytes, not including this length byte, of MUK ID field~~

  ~~MUK ID:~~
  ~~Content: Identifier of MBMS User Key (MUK) being used for MSK transfer security.~~
  ~~Coding: As defined in TS 33.246 [43]~~

  ~~Length of Time Stamp Counter (TS)~~
  ~~Contents: number of bytes (=4), not including this length byte, of Time Stamp Counter (TS)field~~

  - ~~Time Stamp Counter (TS)~~
    ~~Content: Counter for MIKEY replay protection in MSK delivery. The counter is associated with the particular MUK.~~
    ~~Coding: As defined in TS 33.246 [43]~~

- MBMS User Key tags

Description	**Tag Value**
MUK ID Tag	'80'
Time Stamp Counter Tag	'81'

MBMS User Key information

Description	**Value**	**M/O**	**Length (bytes)**
MUK ID Tag	'80'	M	1
Length	X	M	Note
MUK ID value	--	M	X
Time Stamp Counter Tag	'81'	M	1
Length	Y	M	Note
Time Stamp Counter value	--	M	Y
Note: The length is coded according to ISO/IEC 8825 [35]			

- MUK ID Tag '80'
  Content:
  Identifier of MBMS User Key (MUK) being used for MSK transfer security.
  Coding:
  As defined in TS 33.246 [43]

- Time Stamp Counter Tag '81'

Content:
Counter for MIKEY replay protection in MSK delivery. The counter is associated with the particular MUK. The length value is defined in TS 33.246 [43].
Coding:
As defined in TS 33.246 [43]

Unused bytes shall be set to 'FF'.

7.1.1.6 MBMS security context (MSK Update Mode)

USIM operations in MBMS security context are supported if service n°69 is "available".

The USIM receives the ~~NAF_ID and~~ MIKEY packet containing an MSK update message. First, the USIM uses the ~~NAF_Id~~ MUK ID to identify the Ks_int_NAF corresponding with a previous bootstrapping procedure.

The USIM shall check if a new NAF derivation procedure involving the received NAF_ID in the MIKEY message has been performed. In such a case, the USIM shall store the last bootstrapped Ks_int_NAF as the current MUK and update EF_{MUK} as follows:

- If a record with the received NAF_ID (included in the MUK ID: see TS 33.246 [43]) value is already present, then the MUK ID is stored in the corresponding field of this record, and the associated Time Stamp Counter (TS) field is reset. Additionally, the USIM internally stores the last used MUK (i.e. MUK that was used during the last successful MSK update procedure), along with its MUK ID for further use (e.g. to detect Key freshness failure).

- If a record with the received NAF_ID does not exist, the USIM uses an empty record to include the MUK ID, and reset the associated TS field.

If the received MUK ID does not correspond to the current MUK (i.e. last bootstrapped MUK) then the USIM proceeds as follows:

- If the received MUK ID corresponds to the last used MUK and if the received MIKEY message corresponds to a push solicited pull procedure then the USIM uses this MUK to verify the integrity of the message. If the verification is unsuccessful, the USIM abandons the function and returns the status word '9862' (Authentication error, incorrect MAC). If the verification is successful, the USIM abandons the function and returns the status word '9865' (the BM-SC shall be notified to retrieve the latest Ks_int_NAF: see TS 33.246 [43]).

- Otherwise, this is considered as a bootstrapping failure (incorrect MUK) and the USIM abandons the function. The status word '6A88' (Referenced data not found) is returned.

~~If the given NAF_ID does not correspond to any stored Ks_int_NAF, this is considered as a bootstrapping failure (incorrect MUK) and the USIM abandons the function. The status word '6A88' (Referenced data not found) is returned.~~

Otherwise, if the received MUK ID corresponds to the current MUK, the USIM uses ~~Ks_int_NAF as~~ the MUK value for ~~MUK derivation (if needed) and~~ MSK validation and derivation functions as described in TS 33.246 [43]. If the validation is unsuccessful, the status word '9862' (Authentication error, incorrect MAC) is returned and the USIM abandons the function.

After a successful MSK Update procedure the USIM stores the received MSK and updates EF_{MSK} as follows:~~retrieves Network ID, Key Group ID, MSK ID, MSK Validity Data (i.e. MTK ID MAX and SEQs) from the MIKEY message (as described in TS 33.246 [43]) and stores them under EF_{MSK} with the following constraints:~~

~~- If a record with the given Network ID, Key Group ID and MSK_ID values is already present, the new MSK (and associated values) are stored in the corresponding MSK fields of this record.~~

~~- If a record with the given Network Id, Key Group ID already exists and no keys are yet present (MSK associated fields set to 'FF') the new MSK (and associated values) are stored as the 1st MSK of this record~~

~~- If a record with the given Network Id, Key Group ID already exists and only the 1st key is present (2nd MSK associated fields set to 'FF') the new MSK (and associated values) are stored as the 2nd MSK of this record.~~

-If a record with the ~~given Network Id,~~ received Key Domain ID and Key Group ~~ID~~ part (i.e. Key Group part of the MSK ID) already exists, ~~(without the same MSK_ID) and both MSK keys are present,~~ the 2nd ~~1~~st MSK ID ~~(~~and the associated ~~parameters)~~TS shall be replaced by the 1st~~2~~nd MSK ID and the associated TS. Then the new MSK ID is stored as the 1st MSK ID and the associated TS is reset.~~, which is itself replaced by the new one.~~

-If a record with the ~~given Network ID,~~ received Key Domain ID and Key Group ~~ID~~ part does not exist, the USIM uses an empty record to include those values. The received MSK ID is stored as the 1st MSK ID and the associated TS is reset.~~Network Id and Key Group ID values and then proceeds as in the second of the three previous cases.~~ The 2nd MSK ID and the associated TS are set to 'FF FF'.

NOTE: The policy of replacing Key Domain~~Groups~~ records when no more empty records are available in EF_{MSK} is HE specific. (e.g. delete Groups from visited ~~Network Id~~Key Domains first)

Then, the USIM stores the ~~MUK ID and~~ Time Stamp field (retrieved from the MIKEY message) ~~as the MUK ID and Time Stamp Counter (TS) values in the respective~~in its corresponding field~~s~~ under EF_{MUK}.

The USIM stores internally the last used MUK along with its MUK ID for further use. This MUK may be used beyond its GBA validity (i.e. after the derivation of a new Ks_int_NAF resulting from a new bootstrap procedure) to verify the integrity of the first MIKEY message in order to detect a synchronization failure of a push solicited pull procedure. This may occur if the last derived Ks_int_NAF did not reach the BM-SC.

NOTE: The MSK is not necessarily updated in the message, since a MSK transport message can be sent e.g. to update the Key Validity data.

~~Finally, the USIM stores the corresponding MSK (i.e. MSK_I and MSK_C). The Time Stamp value under EF_{MSK} is reset (set to '00000000') when the corresponding MSK is updated.~~

Input:

- ~~NAF_ID,~~ MIKEY message

Output:

- None

7.1.1.7 MBMS security context (MSK Verification Mode)

USIM operations in MBMS security context are supported if service n°69 is "available".

The USIM receives the NAF_ID and MIKEY packet containing an MIKEY verification message, with an empty MAC field.

First, the USIM tests if the given ~~NAF_ID~~ MUK ID corresponds to ~~the~~ a stored MUK ID in EF_{MUK} and if the Time Stamp field in the given MKEY message corresponds with the stored Time Stamp Counter (TS) in EF_{MUK}.

If any of these verifications fails, this is considered as a Verification failure and the USIM abandons the function. The status word ~~'~~'6985'~~'~~ (Conditions of use not satisfied) is returned.

Otherwise, the USIM computes the MAC value as defined in TS 33.246 [43] and sends back the complete MIKEY verification message.

Input:

- NAF_ID, MIKEY message

Output:

- MIKEY message

7.1.1.8 MBMS security context (MTK Generation Mode)

USIM operations in MBMS security context are supported if service n°69 is "available".

The USIM receives the MIKEY message containing an MBMS MTK and a Salt key (if Salt key is available). First, the USIM retrieves the MSK with the Key Domain ID and the MSK ID given by the Extension payload~~identified by the Network ID, Key Group ID and MSK ID enclosed in~~ of the MIKEY message (as described in TS 33.246 [43]).

If the needed MSK does not exist, this is considered as a MSK failure and the USIM abandons the function. The status word ~~'~~'6A88'~~'~~ (Referenced data not found) is returned.

Otherwise, the USIM performs the MBMS Generation and Validation Function (MGV-F) as described in TS 33.246 [43] using MSK~~_I and MSK_C values as integrity and confidentiality keys~~.

If the USIM detects that the given MTK ID is invalid, this is considered as a SEQp freshness failure and the USIM abandons the function. The status word ~~'~~'9865'~~xx'~~ (~~Authentication error, k~~Key freshness failure) is returned.

If the integrity validation of the MIKEY message is unsuccessful, the USIM abandons the function and returns the status word '9862' (Authentication error, incorrect MAC).

After successful MGV_F procedure the USIM stores the Time Stamp field (retrieved from the MIKEY message) as the Time Stamp Counter (TS) associated with the involved MSK under EF_{MSK}

The USIM also stores MTK ID (retrieved from the MIKEY message) as the SEQs associated with MSK.

Then, the USIM returns MTK and Salt key (if Salt key is available).

Input:

- MIKEY message

Output:

- MTK and Salt (if available)

7.1.2.5 MBMS security context (All Modes)

Byte(s)	Description	Length
1	MBMS Security Context Mode	1
2	Length of MIKEY message (L1)	1
3 to (L1+2)	MIKEY message	L1
(L1+3)	Length of NAF_ID (L2) (see note1)	1
(L1+4) to (L1+L2+3)	NAF_ID (see note1)	L2
Note1: Parameter present if and only if ~~in MSK Update Mode or~~ in MSK Verification Mode.		

Parameter MBMS Security Context Mode specifies the MBMS mode in which MBMS security procedure is performed as follows:

Coding of MBMS Security Context Mode

Coding	Meaning
'01'	MSK Update Mode
'02	MSK Verification Mode
'03"	MTK Generation Mode

Response parameters/data, MBMS security context (MSK Verification Mode), command successful:

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

Response parameters/data, MBMS security context (MTK Generation Mode), command successful:

Byte(s)	Description	Length
1	"Successful MBMS operation" tag = 'DB'	1
2	Length of MTK and Salt (if Salt key is available) (L)	1
3 to (L+2)	MTK || Salt (if available)	L

The coding of parameters is described in TS 33.246 [43].

7.3.1 Security management

SW1	SW2	Error description
'98'	'62'	- Authentication error, incorrect MAC
'98'	'64'	- Authentication error, security context not supported
'98'	'65'	- ~~Authentication error, k~~Key freshness failure

3GPP TSG T WG3 Meeting #34 ***T3-050169***
Barcelona, Spain, 8th – 11th February 2005

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.102** **CR** **269** ⌘ **rev** **-** ⌘ Current version: **6.8.0** ⌘

*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:	⌘	Clarification on ADM access condition
Source:	⌘	T3
Work item code:	⌘	TEI-7
Date:	⌘	10/02/2005
Category:	⌘	**F**
Release:	⌘	Rel-7

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:
Ph2 (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)
Rel-7 (Release 7)

Reason for change:	⌘	Whereas in 51.011, the value for ADM is clearly specified : **The definition of access condition ADM does not preclude the administrative authority from using ALW, CHV1, CHV2 and NEV if required.** the definition in 31.102 is not so clear and may lead to misinterpretation.
Summary of change:	⌘	Align the definition of ADM with the one in 51.011 Add definition for PIN/ADM
Consequences if not approved:	⌘	

Clauses affected:	⌘	3.1			
		Y	**N**		
Other specs Affected:	⌘		**X**	Other core specifications	⌘
			X	Test specifications	
			X	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.

3.1 Definitions

For the purposes of the present document, the following definition applies.

ADM: access condition to an EF which is under the control of the authority which creates this file. The definition of access condition ADM does not preclude the administrative authority from using ALW, PIN1, PIN2 and NEV if required. A terminal need not to evaluate access conditions indicated as ADM in the present document.

PIN/ADM: A terminal is required to evaluate the access condition and verify it in order to access the EF if the access condition is set to PIN1 or PIN2.

EHPLMN: represents the Equivalent HPLMNs for network selection purposes. The usage of EHPLMNs is defined in TS 23.122 [31].

[…]

3GPP TSG-T3 #34
Barcelona, Spain, 8-11 February 2005

Tdoc T3-050170

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.102** **CR** 270 ⌘ **rev** **-** ⌘ Current version: **6.8.0** ⌘

*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:	⌘	Collection of essential corrections
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	10/02/2005
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:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change:	⌘	1) Missing reference in the description of the LSA descriptor files when explaining how to allocate the values of the file-Ids. 2) In subclause 5.3.21 $EF_{HPLMNACT}$ is referenced though this EF does not exist in 3GPP TS 31.102
Summary of change:	⌘	Editorial correction in the description of the EF(Hiddenkey) Put the right reference (31.101 aka TS 102221 section 8.6) Correction of referenced $EF_{HPLMNACT}$'s name
Consequences if not approved:	⌘	Risks of wrong implementations

Clauses affected:	⌘	4.2.42, 4.4.1.3, 5.3.21

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

⌘

Other comments:	⌘	Includes changes proposed in Tdocs T3-050012, T3-050082 and T3-050083

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.

4.2.42 $EF_{Hiddenkey}$ (Key for hidden phone book entries)

This EF contains the hidden key that has to be verified by the ME in order to display the phone book entries that are marked as hidden. The hidden key can consist of 4 to 8 digits.

Identifier: '6FC3'	Structure: transparent	Optional
File size: 4 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 4	Hidden Key	M	4 bytes

- Hidden Key.
  Coding:
  - the hidden key is coded on 4 bytes using BCD coding. The minimum number of digits is 4. Unused digits are padded with 'F'.

NOTE: The phone book entries marked as hidden are not scrambled by means of the hidden key. They are stored in plain text in the phone book.

4.4.1.3 LSA Descriptor files

Residing under DF_{SoLSA}, there may be several LSA Descriptor files. These EFs contains one or more records again containing LSA Descriptors forming the LSAs. LSAs can be described in four different ways. As a list of LSA IDs, as a list of LAC + CIs, as a list of CIs or as a list of LACs. As the basic elements (LSA ID, LAC + CI, CI and LAC) of the four types of lists are of different length, they can not be mixed within one record. Different records may contain different kinds of lists within the EFs. Examples of codings of LSA Descriptor files can be found in annex F.

Identifier: '4FXX'	Structure: linear fixed	Optional
Record length: n*X+2 bytes	Update activity: low	

Access Conditions:

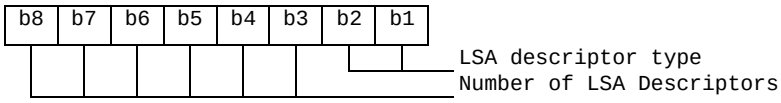
READ	PIN
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	LSA descriptor type and number	M	1 byte
2 to X+1	1st LSA Descriptor	M	X bytes
X+2 to 2X+1	2nd LSA Descriptor	M	X bytes
(n-1)*X+2 to n*X+1	nth LSA Descriptor	M	X bytes
n*X+2	Record Identifier	M	1 byte

- LSA descriptor type and number:

  Contents: The LSA descriptor type gives the format of the LSA descriptor and the number of valid LSA Descriptors within the record.

  Coding:



  LSA descriptor type:

  Contents: Gives the format of the LSA Descriptors.

  b2, b1: 00: LSA ID.
  01: LAC + CI
  10: CI
  11: LAC

  Number of LSA Descriptors:

  Contents: Gives the number of valid LSA Descriptors in the record.

  Coding: binary, with b8 as MSB and b3 as LSB leaving room for 64 LSA Descriptors per record.

- LSA Descriptor

  Contents: Dependant of the coding indicated in the LSA descriptor type:

  - in case of LSA ID the field length 'X' is 3 bytes;
  - in case of LAC + CI the field length 'X' is 4 bytes;
  - in case of CI the field length 'X' is 2 bytes;
  - in case of LAC the field length 'X' is 2 bytes.

Coding: according to TS 24.008 [9].

- Record Identifier:

  Contents: This byte identifies the number of the next record containing the LSA Descriptors forming the LSA.

  Coding: record number of next record. 'FF' identifies the end of the chain.

This file utilises the concept of chaining as for EF_{EXT1}.

The identifier '4FXX' shall be different from one LSA Descriptor file to the other and different from the identifiers of EF_{SAI} and EF_{SLL}. For the range of 'XX', see TS 31.101 [11], ~~subclause x.x.~~.

5.3.21 HPLMN selector with Access Technology

Requirement: Service n°43 "available".

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

3GPP TSG-T3 #34
Barcelona, Spain, 8-11 February 2005

Tdoc ⌘T3-050171

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.102** **CR** 265 ⌘**rev** **-** ⌘ Current version: **6.8.0** ⌘

*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:	⌘	Completion of GBA_U-related procedures
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	09/02/05
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:
Ph2 *(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)*
Rel-7 *(Release 7)*

Reason for change: ⌘ The GBA_U related procedures in TS 31.102, are not in line with those described in TS 33.220. The following points should be clarified in TS 31.102:

- It is stated in the annex G of TS 33.220 that after a successful bootstrap operation, the ME stores in the UICC the Transaction Identifier (B-TID) and the Key Life Time associated with the previous bootstrapped keys. While in section 5.2.20 of TS 31.102 it is only stated that the B-TID shall be updated in EF_{GBABP}
- TS 33.220 clarifies that in the UE there is at most one Ks_int_NAF/Ks_ext_NAF key pair stored per NAF_Id. This clarification should exist in the GBA_U-related procedures in TS 31.102.
- TS 33.220 indicates that if NAF key, derived from one NAF_ID, is updated, the other NAF keys, derived from different NAF_ID values, stored on the UE shall not be affected.
- Finally, in some cases, the NAF_ID is not enough to identify the Ks_int_NAF/Ks_est_NAF unambiguously. For example, a new NAF key generation, from which the http session was not able to complete towards the corresponding NAF, results in different Ks_ext_NAF/Ks_int_NAF key pairs (one in the UE and another in the NAF) identified with the same NAF_ID. Therefore, text should also be added in TS 31.102 to indicate that the USIM shall store B-TID together with Ks_int_NAF and NAF_ID in order to identify unambiguously the Ks_int_NAF key.

Summary of change:	⌘	Complete the description of GBA_U procedures
Consequences if not approved:	⌘	Incomplete description of GBA_U procedures in TS 31.102 that could result in the misinterpretation of the original requirements and procedures, which are described in TS 33.220.

Clauses affected:	⌘	5.2.20, 7.1.1.4, 7.1.1.5			
Other specs affected:	⌘	**Y**	**N**	Other core specifications	⌘
			X	Test specifications	
			X	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.

5.2.20 Generic Bootstrapping architecture (Bootstrap)

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

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

7.1.1.4 GBA security context (Bootstrapping Mode)

USIM operations in GBA security context are supported if service n°68 is "available".

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

The USIM calculates IK = $f4_K$ (RAND) and MAC (by performing the MAC modification function described in TS 33.220 [42]). Then the USIM computes XMAC = $f1_K$ (SQN || RAND || AMF) and compares this with the MAC previously produced. If they are different, the USIM abandons the function.

Then the USIM proceeds by checking AUTN as in UMTS security context. If the USIM detects the sequence numbers to be invalid, this is considered as a synchronisation failure and the USIM abandons the function. In this case the command response is AUTS, which is computed as in UMTS security context.

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

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

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

NOTE: According to TS 33.220 [42], NAF-specific keys that may be stored on the USIM are not affected by this bootstrapping operation.

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

Input:

- RAND, AUTN

Output:

- RES

or

- AUTS

7.1.1.5 GBA security context (NAF Derivation Mode)

USIM operations in GBA security context are supported if service n°68 is "available".

The USIM receives the NAF_ID and IMPI.

The USIM performs Ks_ext_NAF and Ks_int_NAF derivation as defined in TS 33.220 [42] using the key material from the previous GBA_U bootstrapping procedure.

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

Otherwise, the USIM stores Ks_int_NAF and associated B-TID together with NAF_ID. ~~-~~The Ks_int_NAF keys related to other NAF_IDs, which are already stored in the USIM, shall not be affected.

NOTE: According to TS 33.220 [42], ~~T~~the USIM can contain several Ks_int_NAF together with the associated B-TID and NAF_ID, but there is at most one pair of Ks_int_NAF and associated B-TID stored per NAF_ID.

Then, the USIM returns Ks_ext_NAF.

Input:

- NAF_ID, IMPI

Output:

- Ks_ext_NAF

3GPP TSG-T3 #34
Barcelona, Spain, 8-11 February 2005

Tdoc ⌘T3-050184

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.102** **CR** 266 ⌘**rev** **-** ⌘ Current version: **6.8.0** ⌘

*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:	⌘	Storage of NAF-keys identifiers in GBA_U
Source:	⌘	Axalto, Gemplus
Work item code:	⌘	TEI
Date:	⌘	09/02/05
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:
Ph2 (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)
Rel-7 (Release 7)

Reason for change:	⌘	The USIM can contain several Ks_int_NAF keys together with associated B-TID and NAF-ID. At the moment the ME cannot detect in the UICC the existence of a Ks_int_NAF key already shared between the UICC and a NAF after a GBA NAF Derivation procedure. This issue is solved by the creation of an EF (EF_{GBANL}) containing the list of NAF_IDs and B-TIDs, which are associated to the last GBA NAF derivation procedure successfully executed for a given NAF. The existence of this EF is very useful for some GBA-based service. E.g. in MBMS the ME needs to detect for a given NAF the presence in the USIM of the key derived from the last successful GBA NAF Derivation procedure.
Summary of change:	⌘	Creation of an EF listing the NAF_IDs and B-TIDs which are associated to the last GBA NAF derivation procedure successfully executed for a given NAF.
Consequences if not approved:	⌘	For some GBA-based services the ME can lack of information on the previous GBA NAF Derivation procedure successfully executed on the UICC for a given NAF.

Clauses affected:	⌘	4.2.x (new), 4.7, 7.1.1.5, Annex A, Annex E

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

Other comments:	⌘	This CR is related to S3-041126, which was approved by SP#26 in SP-040859

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.x EF_{GBANL} (GBA NAF List)

If service n°68 is "available", this file shall be present.

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

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

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

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

- NAF Key Identifier tags

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

NAF Key Identifier information

Description	Value	M/O	Length (bytes)
NAF_ID Tag	'80'	M	1
Length	X	M	Note
NAF_ID value	--	M	X
B-TID Tag	'81'	M	1
Length	Y	M	Note
B-TID value	--	M	Y
Note: The length is coded according to ISO/IEC 8825 [35]			

- NAF_ID Tag '80'

  Contents:

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

  Coding:

  As defined in 33.220 [42]

- B-TID Tag '81'

  Content:

  Bootstrapping Transaction Identifier of the GBA_U bootstrapped key

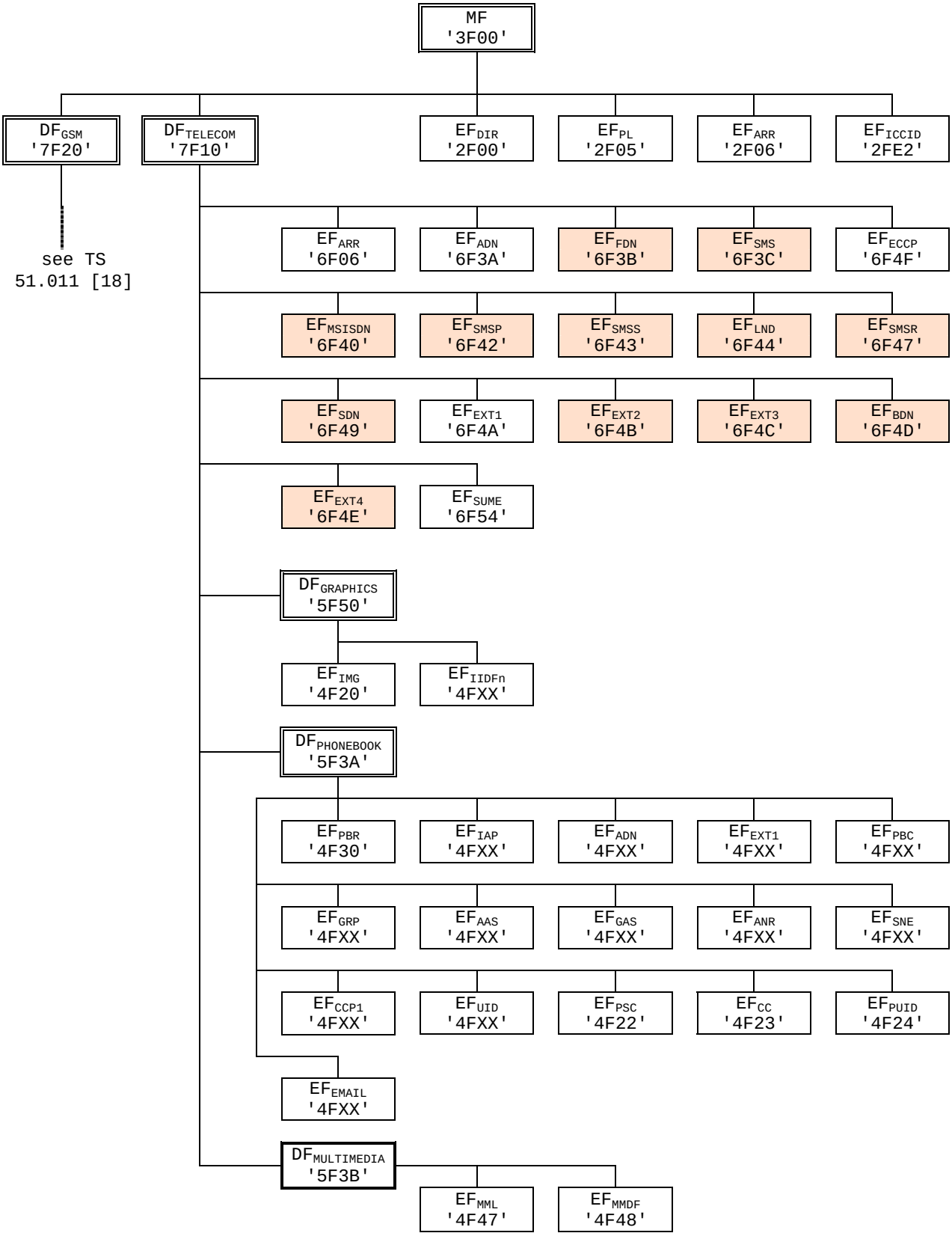
  Coding:

  As defined in TS 33.220 [42]

Unused bytes shall be set to 'FF'

4.7 Files of USIM

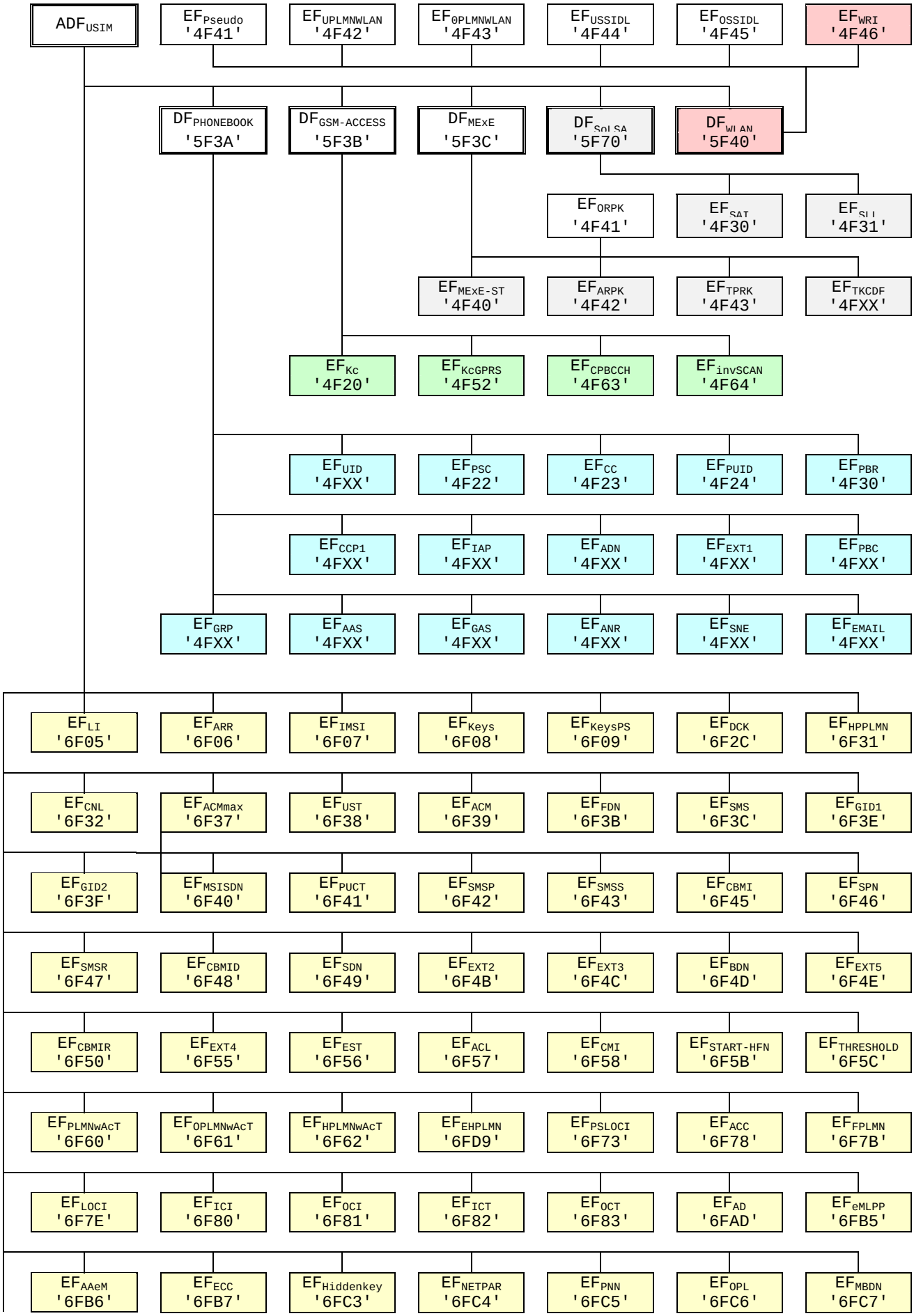
This clause contains two figures depicting the file structure of the UICC and the ADF_{USIM}. ADF_{USIM} shall be selected using the AID and information in EF_{DIR}.

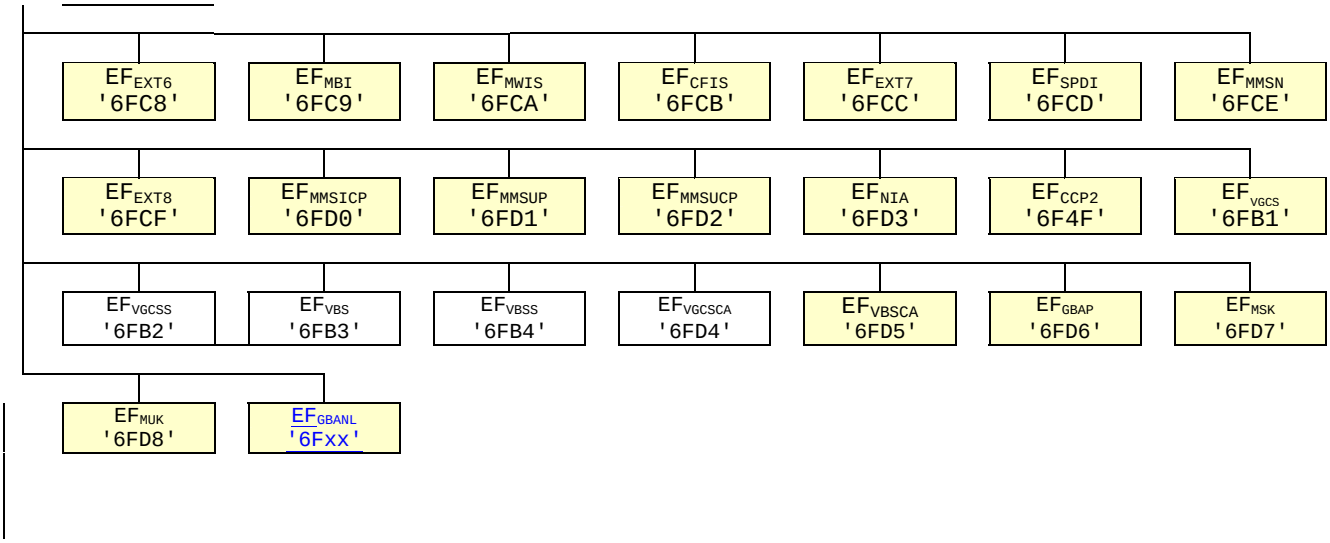


NOTE 1: Files under $DF_{TELECOM}$ with shaded background are defined in TS 51.011 [18].

NOTE 2: The value '6F65' under ADFUSIM was used in earlier versions of this specification, and should not be re-assigned in future versions.

Figure 4.1: File identifiers and directory structures of UICC


ADF USIM
EF Pseudo '4F41'
EF UPLMNWLAN '4F42'
EF 0PLMNWLAN '4F43'
EF USSIDL '4F44'
EF OSSIDL '4F45'
EF WRI '4F46'
DF PHONEBOOK '5F3A'
DF GSM-ACCESS '5F3B'
DF MExE '5F3C'
DF SoLSA '5F70'
DF WLAN '5F40'
EF ORPK '4F41'
EF SAT '4F30'
EF SLL '4F31'
EF MExE-ST '4F40'
EF ARPK '4F42'
EF TPRK '4F43'
EF TKCDF '4FXX'
EF Kc '4F20'
EF KcGPRS '4F52'
EF CPBCCH '4F63'
EF invSCAN '4F64'
EF UID '4FXX'
EF PSC '4F22'
EF CC '4F23'
EF PUID '4F24'
EF PBR '4F30'
EF CCP1 '4FXX'
EF IAP '4FXX'
EF ADN '4FXX'
EF EXT1 '4FXX'
EF PBC '4FXX'
EF GRP '4FXX'
EF AAS '4FXX'
EF GAS '4FXX'
EF ANR '4FXX'
EF SNE '4FXX'
EF EMAIL '4FXX'
EF LI '6F05'
EF ARR '6F06'
EF IMSI '6F07'
EF Keys '6F08'
EF KeysPS '6F09'
EF DCK '6F2C'
EF HPPLMN '6F31'
EF CNL '6F32'
EF ACMmax '6F37'
EF UST '6F38'
EF ACM '6F39'
EF FDN '6F3B'
EF SMS '6F3C'
EF GID1 '6F3E'
EF GID2 '6F3F'
EF MSISDN '6F40'
EF PUCT '6F41'
EF SMSP '6F42'
EF SMSS '6F43'
EF CBMI '6F45'
EF SPN '6F46'
EF SMSR '6F47'
EF CBMID '6F48'
EF SDN '6F49'
EF EXT2 '6F4B'
EF EXT3 '6F4C'
EF BDN '6F4D'
EF EXT5 '6F4E'
EF CBMIR '6F50'
EF EXT4 '6F55'
EF EST '6F56'
EF ACL '6F57'
EF CMI '6F58'
EF START-HFN '6F5B'
EF THRESHOLD '6F5C'
EF PLMNwAcT '6F60'
EF OPLMNwAcT '6F61'
EF HPLMNwAcT '6F62'
EF EHPLMN '6FD9'
EF PSLOCI '6F73'
EF ACC '6F78'
EF FPLMN '6F7B'
EF LOCI '6F7E'
EF ICI '6F80'
EF OCI '6F81'
EF ICT '6F82'
EF OCT '6F83'
EF AD '6FAD'
EF eMLPP '6FB5'
EF AAeM '6FB6'
EF ECC '6FB7'
EF Hiddenkey '6FC3'
EF NETPAR '6FC4'
EF PNN '6FC5'
EF OPL '6FC6'
EF MBDN '6FC7'


EF EXT6 '6FC8'
EF MBI '6FC9'
EF MWIS '6FCA'
EF CFIS '6FCB'
EF EXT7 '6FCC'
EF SPDI '6FCD'
EF MMSN '6FCE'
EF EXT8 '6FCF'
EF MMSICP '6FD0'
EF MMSUP '6FD1'
EF MMSUCP '6FD2'
EF NIA '6FD3'
EF CCP2 '6F4F'
EF VGCS '6FB1'
EF VGCSS '6FB2'
EF VBS '6FB3'
EF VBSS '6FB4'
EF VGCSCA '6FD4'
EF VBSCA '6FD5'
EF GBAP '6FD6'
EF MSK '6FD7'
EF MUK '6FD8'
EF GBANL '6Fxx'

7.1.1.5 GBA security context (NAF Derivation Mode)

USIM operations in GBA security context are supported if service n°68 is "available".

The USIM receives the NAF_ID and IMPI.

The USIM performs Ks_ext_NAF and Ks_int_NAF derivation as defined in TS 33.220 [42] using the key material from the previous GBA_U bootstrapping procedure.

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

Otherwise, the USIM stores Ks_int_NAF together with NAF_ID ~~.~~ and updates EF_{GBANL} as follows:

-If a record with the given NAF_ID already exists, the USIM updates the B-TID field of this record with the B-TID value associated to the GBA_U bootstrapped key involved in this GBA_U NAF derivation procedure.

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

NOTE: The USIM can contain several Ks_int_NAF together with NAF_ID

Then, the USIM returns Ks_ext_NAF.

Input:

- NAF_ID, IMPI

Output:

- Ks_ext_NAF

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

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

File identification	Description	Change advised
'2F00'	Application directory	Caution
'2F05'	Preferred languages	Yes
'2F06'	Access rule reference	Caution
'2FE2'	ICC identification	No
'4F20'	Image data	Yes
'4F20'	GSM Ciphering key Kc	No
'4FXX'	Image Instance data Files	Yes
'4FXX'	Unique identifier	Yes
'4F22'	Phone book synchronisation counter	Yes
'4F23'	Change counter	Yes
'4F24'	Previous unique identifier	Yes
'4F30'	Phone book reference file	Yes
'4FXX'	Capability configuration parameters 1	Yes
'4F30'	SoLSA Access Indicator	Caution
'4F31'	SoLSA LSA List	Caution
'4FXX'	LSA Descriptor files	Caution
'4F52'	GPRS Ciphring key KcGPRS	No
'4F63'	CPBCCH Information	No
'4F64'	Investigation Scan	Caution
'4FXX'	Additional number alpha string	Yes
'4FXX'	Additional number	Yes
'4FXX'	Second name entry	Yes
'4FXX'	Grouping information alpha string	Yes
'4FXX'	Phone book control	Yes
'4FXX'	E-mail addresses	Yes
'4FXX'	Index administration phone book	Yes
'4FXX'	Extension 1	Yes
'4FXX'	Abbreviated dialling numbers	Yes
'4FXX'	Grouping file	Yes
'4F41'	Pseudonym	Caution
'4F42'	User controlled PLMN selector for WLAN	No
'4F43'	Operator controlled PLMN selector for WLAN	Caution
'4F44'	User controlled WSID List	No
'4F45'	Operator controlled WSID List	Caution
'4F46'	WLAN Reauthentication Identity	No
'4F47'	Multimedia Messages List	Yes
'4F48'	Multimedia Messages Data File	Yes
'6F05'	Language indication	Yes
'6F06'	Access rule reference (under ADF_{USIM} and $DF_{TELECOM}$)	Caution
'6F07'	IMSI	Caution (Note 1)
'6F08'	Ciphering and integrity keys	No
'6F09'	Ciphering and integrity keys for packet switched domain	No
'6F2C'	De-personalization Control Keys	Caution
'6F31'	Higher Priority PLMN search period	Caution
'6F32'	Co-operative network list	Caution
'6F37'	ACM maximum value	Yes
'6F38'	USIM service table	Caution
'6F39'	Accumulated call meter	Yes
'6F3B'	Fixed dialling numbers	Yes
'6F3C'	Short messages	Yes
'6F3E'	Group identifier level 1	Yes
'6F3F'	Group identifier level 2	Yes

File identification	Description	Change advised
	Continued….	

File identification	Description	Change advised
'6F40'	MSISDN storage	Yes
'6F41'	PUCT	Yes
'6F42'	SMS parameters	Yes
'6F43'	SMS status	Yes
'6F45'	CBMI	Caution
'6F46'	Service provider name	Yes
'6F47'	Short message status reports	Yes
'6F48'	CBMID	Yes
'6F49'	Service Dialling Numbers	Yes
'6F4B'	Extension 2	Yes
'6F4C'	Extension 3	Yes
'6F4D'	Barred dialling numbers	Yes
'6F4E'	Extension 5	Yes
'6F4F'	Capability configuration parameters 2	Yes
'6F50'	CBMIR	Yes
'6F54'	SetUp Menu Elements	Yes
'6F55'	Extension 4	Yes
'6F56'	Enabled services table	Caution
'6F57'	Access point name control list	Yes
'6F58'	Comparison method information	Yes
'6F5B'	Initialisation value for Hyperframe number	Caution
'6F5C'	Maximum value of START	Yes
'6F60'	User controlled PLMN selector with Access Technology	No
'6F61'	Operator controlled PLMN selector with Access Technology	Caution
'6F62'	HPLMN selector with Access Technology	Caution
'6F73'	Packet switched location information	Caution
'6F78'	Access control class	Caution
'6F7B'	Forbidden PLMNs	Caution
'6F7E'	Location information	No (Note 1)
'6F80'	Incoming call information	Yes
'6F81'	Outgoing call information	Yes
'6F82'	Incoming call timer	Yes
'6F83'	Outgoing call timer	Yes
'6FAD'	Administrative data	Caution
'6FB1'	Voice Group Call Service	Yes
'6FB2'	Voice Group Call Service Status	Yes
'6FB3'	Voice Broadcast Service	Yes
'6FB4'	Voice Broadcast Service Status	Yes
'6FB5'	Enhanced Multi Level Pre-emption and Priority	Yes
'6FB6'	Automatic Answer for eMLPP Service	Yes
'6FB7'	Emergency Call Codes	Caution
'6FC3'	Key for hidden phone book entries	No
'6FC4'	Network Parameters	No
'6FC5'	PLMN Network Name	Yes
'6FC6'	Operator Network List	Yes
'6FC7'	Mailbox Dialling Numbers	Yes
'6FC8'	Extension 6	Yes
'6FC9'	Mailbox Identifier	Caution
'6FCA'	Message Waiting Indication Status	Caution
'6FCB'	Call Forwarding Indication Status	Caution
'6FCC'	Extension 7	Yes
'6FCD'	Service Provider Display Information	Yes
'6FCE'	MMS Notification	Yes
'6FCF'	Extension 8	Yes
'6FD0'	MMS Issuer Connectivity Parameters	Yes
'6FD1'	MMS User Preferences	Yes
'6FD2'	MMS User Connectivity Parameters	Yes
'6FD3'	Network's indication of alerting (NIA)	Caution
'6FD4'	Voice Group Call Service Ciphering Algorithm	Yes
'6FD5'	Voice Broadcast Service Ciphering Algorithm	Yes
'6FD6'	GBA Bootstrapping parameters	Caution
'6FD7'	MBMS Service Keys List	Caution

File identification	Description	Change advised
'6FD8'	MBMS User Key	Caution
'6FD9'	EHPLMN	Caution
'6Fxx'	GBA NAF List	Caution
NOTE1: If EF_{IMSI} is changed, the UICC should issue REFRESH as defined in TS 31.111 and update EF_{LOCI} accordingly.		

Annex E (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
'2F00'	Application directory	Card issuer/operator dependant
'2F05'	Preferred languages	'FF…FF'
'2F06'	Access rule reference	Card issuer/operator dependant
'2FE2'	ICC identification	operator dependant
'4F20'	Image data	'00FF...FF'
'4F20'	GSM Ciphering key Kc	'FF...FF07'
'4FXX'	Image instance data files	'FF…FF'
'4FXX'	Unique identifier	'0000'
'4F22'	Phone book synchronisation counter	'00000000'
'4F23'	Change counter	'0000'
'4F24'	Previous unique identifier	'0000'
'4F30'	Phone book reference file	Operator dependant
'4F30'	SoLSA Access Indicator	'00FF...FF'
'4F31'	SoLSA LSA List	'FF...FF'
'4FXX'	LSA Descriptor files	'FF…FF'
'4FXX'	Capability configuration parameters 1	'FF…FF'
'4F52'	GPRS Ciphring key KcGPRS	'FF...FF07'
'4F63'	CPBCCH Information	'FF..FF'
'4F64'	Investigation PLMN scan	'00'
'4FXX'	E-mail addresses	'FF…FF'
'4FXX'	Additional number alpha string	'FF…FF'
'4FXX'	Second name entry	'FF…FF'
'4FXX'	Abbreviated dialling numbers	'FF...FF'
'4FXX'	Grouping file	'00…00'
'4FXX'	Grouping information alpha string	'FF…FF'
'4FXX'	Phone book control	'0000'
'4FXX'	Index administration phone book	'FF…FF'
'4FXX'	Additional number	'FF…FF'
'4FXX'	Extension 1	'00FF...FF'
'4F41'	Pseudonym	'00FF…FF'
'4F42'	User Controlled PLMN selector for WLAN	'FF…FF'
'4F43'	Operator Controlled PLMN selector for WLAN	Operator dependant
'4F44'	User Controlled WSID list	'00FF…FF'
'4F45'	Operator controlled WSID list	Operator dependant
'4F46'	WLAN Reauthentication Identity	'FF…FF'
'4F47'	Multimedia Messages List	'FF…FF'
'4F48'	Multimedia Messages Data File	'FF…FF'
'6F05'	Language indication	'FF…FF'
'6F06'	Access rule reference (under ADF_{USIM} and $DF_{TELECOM}$)	Card issuer/operator dependant
'6F07'	IMSI	Operator dependant
'6F08'	Ciphering and integrity keys	'07FF…FF'
'6F09'	Ciphering and integrity keys for packet switched domain	'07FF…FF'
'6F2C'	De-personalization control keys	'FF…FF'
'6F31'	Higher Priority PLMN search period	'FF'
'6F32'	Co-operative network list	'FF…FF'
'6F37'	ACM maximum value	'000000' (see note 1)
'6F38'	USIM service table	Operator dependant
'6F39'	Accumulated call meter	'000000'
'6F3B'	Fixed dialling numbers	'FF...FF'
'6F3C'	Short messages	'00FF...FF'
'6F3E'	Group identifier level 1	Operator dependant
'6F3F'	Group identifier level 2	Operator dependant
'6F40'	MSISDN storage	'FF...FF'
'6F41'	PUCT	'FFFFFF0000'
'6F42'	SMS parameters	'FF...FF'
'6F43'	SMS status	'FF...FF'
'6F45'	CBMI	'FF...FF'
'6F46'	Service provider name	Operator dependant
'6F47'	Short message status reports	'00FF…FF'
'6F48'	CBMID	'FF...FF'
'6F49'	Service Dialling Numbers	'FF...FF'

'6F4B'	Extension 2	'00FF...FF'
'6F4C'	Extension 3	'00FF...FF'

Continued....

File Identification	Description	Value
'6F4D'	Barred Dialling Numbers	'FF...FF'
'6F4E'	Extension 5	'00FF...FF'
'6F4F'	Capability configuration parameters 2	'FF...FF'
'6F50'	CBMIR	'FF...FF'
'6F54'	SetUp Menu Elements	Operator dependant
'6F55'	Extension 4	'00FF...FF'
'6F56'	Enabled services table	Operator dependant
'6F57'	Access point name control list	'00FF…FF'
'6F58'	Comparison method information	'FF…FF'
'6F5B'	Initialisation value for Hyperframe number	'F0 00 00 F0 00 00'
'6F5C'	Maximum value of START	Operator dependant
'6F60'	User controlled PLMN selector with Access Technology	'FFFFFF0000..FFFFFF0000'
'6F61'	Operator controlled PLMN selector with Access Technology	'FFFFFF0000..FFFFFF0000'
'6F62'	HPLMN selector with Access Technology	'FFFFFF0000..FFFFFF0000'
'6F73'	Packet switched location information	'FFFFFFFF FFFFFF xxxxxx 0000 FF 01' (see note 2)
'6F78'	Access control class	Operator dependant
'6F7B'	Forbidden PLMNs	'FF...FF'
'6F7E	Location information	'FFFFFFFF xxxxxx 0000 FF 01' (see note 2)
'6F80'	Incoming call information	'FF…FF 000000 00 01FFFF'
'6F81'	Outgoing call information	'FF…FF 000000 01FFFF'
'6F82'	Incoming call timer	'000000'
'6F83'	Outgoing call timer	'000000'
'6FAD'	Administrative data	Operator dependant
'6FB1'	Voice Group Call Service	Operator dependant
'6FB2'	Voice Group Call Service Status	Operator dependant
'6FB3'	Voice Broadcast Service	Operator dependant
'6FB4'	Voice Broadcast Service Status	Operator dependant
'6FB5'	EMLPP	Operator dependant
'6FB6'	AaeM	'00'
'6FB7'	Emergency call codes	Operator dependant
'6FC3'	Key for hidden phone book entries	'FF…FF'
'6FC4'	Network Parameters	'FF…FF'
'6FC5'	PLMN Network Name	Operator dependant
'6FC6'	Operator Network List	Operator dependant
'6FC7'	Mailbox Dialling Numbers	Operator dependant
'6FC8'	Extension 6	'00 FF...FF'
'6FC9'	Mailbox Identifier	Operator dependant
'6FCA'	Message Waiting Indication Status	'00 00 00 00 00'
'6FCB'	Call Forwarding Indication Status	'xx 00 FF...FF'
'6FCC'	Extension 7	'00 FF...FF'
'6FCD'	Service Provider Display Information	
'6FCE'	MMS Notification	'00 00 00 FF…FF'
'6FCF'	Extension 8	'00FF...FF'
'6FD0'	MMS Issuer Connectivity Parameters	'FF…FF'
'6FD1'	MMS User Preferences	'FF…FF'
'6FD2'	MMS User Connectivity Parameters	'FF…FF'
'6FD3'	Network's Indication of Alerting (NIA)	'FF...FF'
'6FD4'	Voice Group Call Service Ciphering Algorithm	'00…00'
'6FD5'	Voice Broadcast Service Ciphering Algorithm	'00…00'
'6FD6'	GBA Bootstrapping parameters	'FF…FF'
'6FD7'	MBMS Service Keys List	'FF…FF'
'6FD8'	MBMS User Key	'FF…FF'
'6FD9'	EHPLMN	'FF…FF' or xxxxxx (see Note 2)
'6Fxx'	GBA NAF List	'FF…FF'

NOTE 1: The value '000000' means that ACMmax is not valid, i.e. there is no restriction on the ACM. When assigning a value to ACMmax, care should be taken not to use values too close to the maximum possible value 'FFFFFF', because the INCREASE command does not update EF_{ACM} if the units to be added would exceed 'FFFFFF'. This could affect the call termination procedure of the Advice of Charge function.

NOTE 2: xxxxxx stands for any valid MCC and MNC, coded according to TS 24.008 [9].

3GPP TSG-T3 Meeting #34
Barcelona, Spain, 8th – 11th February 2005

Tdoc ⌘T3-050189

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.102** **CR** **264** ⌘ **rev** **1** ⌘ Current version: **6.8.0** ⌘

*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:	⌘	Correction to overcome IMSI number space limitation – inclusion of EHPLMN
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	10/02/2005
Category:	⌘	**B**
Release:	⌘	Rel-7

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:
Ph2 *(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)*
Rel-7 *(Release 7)*

Reason for change:	⌘	The currently defined IMSI does not provide a large enough range of numbers to cover all (future) customers and TSG SA#24 approved a CR to introduce the concept of the Equivalent HPLMN list to deal with this problem (CR#63 to TS 22.011). CN1 has been agreed that the introduction of a new file, to cater for the EHPLMN requirement, would be the safer option. The feature has been introduced into the Release 7 version of the SA1 and CN1 specifications so also needs to be included in the Rel 7 version of 31.102
Summary of change:	⌘	A new file has been introduced EF_{EHPLMN} and procedures related to the usage of the data field
Consequences if not approved:	⌘	There will be no means for allowing a mobile to consider a network broadcasting a different MCC+MNC than the MCC+MNC part of the IMSI as its HPLMN

Clauses affected:	⌘	3.1, 4.2.8, 4.2.xx, 4.7, 5.1.1.2, 5.2.yy, 5.3.zz, Annex A, Annex E

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

Other comments:	⌘	This CR creates Rel-7 of 31.102.

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.

3 Definitions, symbols, abbreviations and coding conventions

3.1 Definitions

For the purposes of the present document, the following definition applies.

ADM: access condition to an EF which is under the control of the authority which creates this file

EHPLMN: represents the Equivalent HPLMNs for network selection purposes. The behaviour of EHPLMNs is defined in TS 22.011 [2].

========== Next Modification ==========

4.2.8 EF_{UST} (USIM Service Table)

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

Identifier: '6F38'	Structure: transparent	Mandatory
SFI: '04'		
File size: X bytes, X >= 1	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

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

-Services

Contents:	Service n°1:	Local Phone Book
	Service n°2:	Fixed Dialling Numbers (FDN)
	Service n°3:	Extension 2
	Service n°4:	Service Dialling Numbers (SDN)
	Service n°5:	Extension3
	Service n°6:	Barred Dialling Numbers (BDN)
	Service n°7:	Extension4
	Service n°8:	Outgoing Call Information (OCI and OCT)
	Service n°9:	Incoming Call Information (ICI and ICT)
	Service n°10:	Short Message Storage (SMS)
	Service n°11:	Short Message Status Reports (SMSR)
	Service n°12:	Short Message Service Parameters (SMSP)
	Service n°13:	Advice of Charge (AoC)
	Service n°14:	Capability Configuration Parameters (CCP)
	Service n°15:	Cell Broadcast Message Identifier
	Service n°16:	Cell Broadcast Message Identifier Ranges
	Service n°17:	Group Identifier Level 1
	Service n°18:	Group Identifier Level 2
	Service n°19:	Service Provider Name
	Service n°20:	User controlled PLMN selector with Access Technology
	Service n°21:	MSISDN
	Service n°22:	Image (IMG)
	Service n°23:	Support of Localised Service Areas (SoLSA)
	Service n°24:	Enhanced Multi-Level Precedence and Pre-emption Service
	Service n°25:	Automatic Answer for eMLPP
	Service n°26:	RFU
	Service n°27:	GSM Access
	Service n°28:	Data download via SMS-PP
	Service n°29:	Data download via SMS-CB
	Service n°30:	Call Control by USIM
	Service n°31:	MO-SMS Control by USIM
	Service n°32:	RUN AT COMMAND command
	Service n°33:	shall be set to '1'
	Service n°34:	Enabled Services Table
	Service n°35:	APN Control List (ACL)
	Service n°36:	Depersonalisation Control Keys
	Service n°37:	Co-operative Network List
	Service n°38:	GSM security context
	Service n°39:	CPBCCH Information
	Service n°40:	Investigation Scan
	Service n°41:	MExE
	Service n°42:	Operator controlled PLMN selector with Access Technology
	Service n°43:	HPLMN selector with Access Technology
	Service n°44:	Extension 5
	Service n°45:	PLMN Network Name
	Service n°46:	Operator PLMN List
	Service n°47:	Mailbox Dialling Numbers
	Service n°48:	Message Waiting Indication Status
	Service n°49:	Call Forwarding Indication Status
	Service n°50:	Reserved and shall be ignored
	Service n°51:	Service Provider Display Information
	Service n°52	Multimedia Messaging Service (MMS)
	Service n°53	Extension 8
	Service n°54	Call control on GPRS by USIM
	Service n°55	MMS User Connectivity Parameters
	Service n°56	Network's indication of alerting in the MS (NIA)
	Service n°57	VGCS Group Identifier List (EF_{VGCS} and EF_{VGCSS})
	Service n°58	VBS Group Identifier List (EF_{VBS} and EF_{VBSS})
	Service n°59	Pseudonym
	Service n°60	User Controlled PLMN selector for WLAN access
	Service n°61	Operator Controlled PLMN selector for WLAN access
	Service n°62	User controlled WSID list
	Service n°63	Operator controlled WSID list
	Service n°64	VGCS security
	Service n°65	VBS security
	Service n°66	WLAN Reauthentication Identity
	Service n°67	Multimedia Messages Storage
	Service n°68	Generic Bootstrapping Architecture (GBA)

Service n°69	MBMS security
Service n°70	Data download via USSD and USSD application mode
Service n°71	Equivalent HPLMN

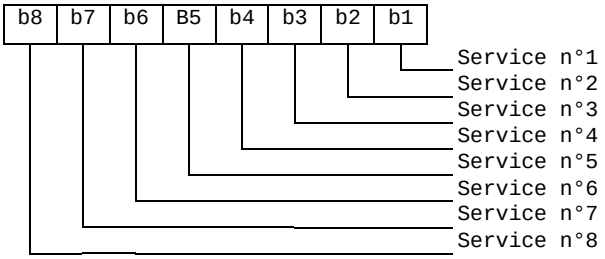
The EF shall contain at least one byte. Further bytes may be included, but if the EF includes an optional byte, then it is mandatory for the EF to also contain all bytes before that byte. Other services are possible in the future and will be coded on further bytes in the EF. The coding falls under the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

Coding:

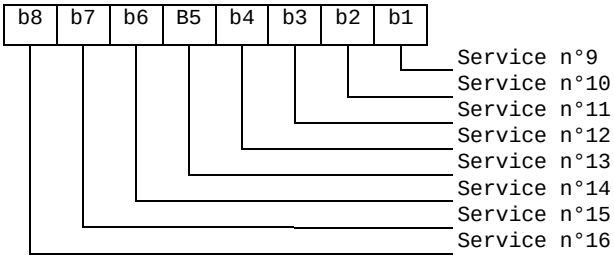
1 bit is used to code each service:
bit = 1: service available;
bit = 0: service not available.

- Service available means that the USIM has the capability to support the service and that the service is available for the user of the USIM unless the service is identified as "disabled" in EF_{EST}.
  Service not available means that the service shall not be used by the USIM user, even if the USIM has the capability to support the service.

First byte:



Second byte:



etc.

4.2.xx EF_{EHPLMN} (Equivalent HPLMN)

If service n°71 is "available", this file shall be present.

This EF contains the coding for n EHPLMNs. The usage of EHPLMN is defined in 23.122 [31]. This data field shall not contain the HPLMN code derived from the IMSI as an EHPLMN entry.

Identifier: '6FD9'	Structure: transparent	Optional
SFI: 'xx'		
File size: 3*n (where n ≥1)	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 3	1st EHPLMN (highest priority)	M	3 bytes
4 to 6	2nd EHPLMN	O	3 bytes
:	:		
(3n-2) to (3n)	nth EHPLMN (lowest priority)	O	3 bytes

- EHPLMN

  Contents:

  - Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).

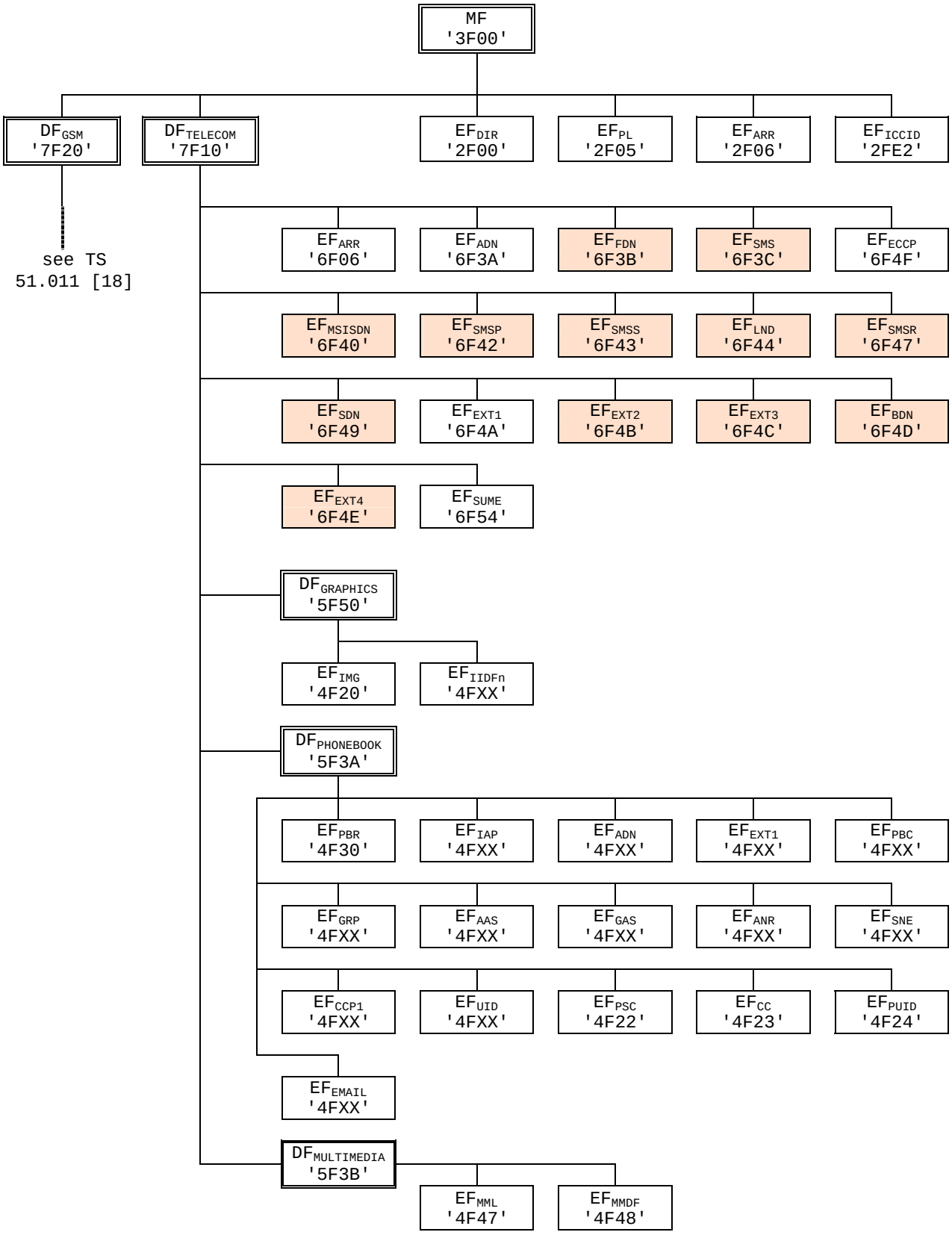
  Coding:

  - - according to TS 24.008 [9].

  - Unused entries shall be set to 'FF FF FF'

4.7 Files of USIM

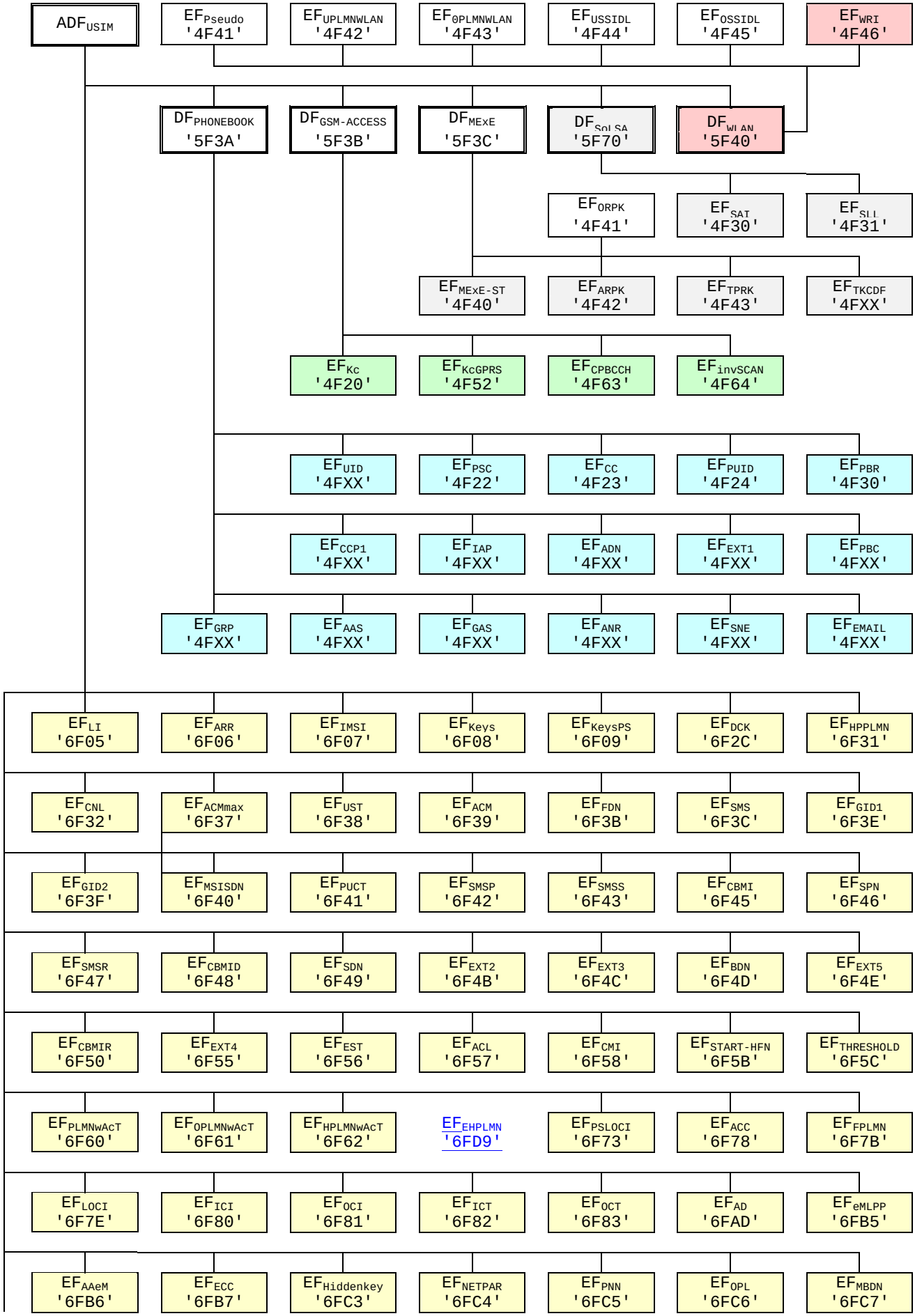
This clause contains two figures depicting the file structure of the UICC and the ADF_{USIM}. ADF_{USIM} shall be selected using the AID and information in EF_{DIR}.



NOTE 1: Files under $DF_{TELECOM}$ with shaded background are defined in TS 51.011 [18].

NOTE 2: The value '6F65' under ADFUSIM was used in earlier versions of this specification, and should not be re-assigned in future versions.

Figure 4.1: File identifiers and directory structures of UICC


ADF USIM
EF Pseudo '4F41'
EF UPLMNWLAN '4F42'
EF 0PLMNWLAN '4F43'
EF USSIDL '4F44'
EF OSSIDL '4F45'
EF WRI '4F46'
DF PHONEBOOK '5F3A'
DF GSM-ACCESS '5F3B'
DF MExE '5F3C'
DF SoLSA '5F70'
DF WLAN '5F40'
EF ORPK '4F41'
EF SAI '4F30'
EF SLL '4F31'
EF MExE-ST '4F40'
EF ARPK '4F42'
EF TPRK '4F43'
EF TKCDF '4FXX'
EF Kc '4F20'
EF KcGPRS '4F52'
EF CPBCCH '4F63'
EF invSCAN '4F64'
EF UID '4FXX'
EF PSC '4F22'
EF CC '4F23'
EF PUID '4F24'
EF PBR '4F30'
EF CCP1 '4FXX'
EF IAP '4FXX'
EF ADN '4FXX'
EF EXT1 '4FXX'
EF PBC '4FXX'
EF GRP '4FXX'
EF AAS '4FXX'
EF GAS '4FXX'
EF ANR '4FXX'
EF SNE '4FXX'
EF EMAIL '4FXX'
EF LI '6F05'
EF ARR '6F06'
EF IMSI '6F07'
EF Keys '6F08'
EF KeysPS '6F09'
EF DCK '6F2C'
EF HPPLMN '6F31'
EF CNL '6F32'
EF ACMmax '6F37'
EF UST '6F38'
EF ACM '6F39'
EF FDN '6F3B'
EF SMS '6F3C'
EF GID1 '6F3E'
EF GID2 '6F3F'
EF MSISDN '6F40'
EF PUCT '6F41'
EF SMSP '6F42'
EF SMSS '6F43'
EF CBMI '6F45'
EF SPN '6F46'
EF SMSR '6F47'
EF CBMID '6F48'
EF SDN '6F49'
EF EXT2 '6F4B'
EF EXT3 '6F4C'
EF BDN '6F4D'
EF EXT5 '6F4E'
EF CBMIR '6F50'
EF EXT4 '6F55'
EF EST '6F56'
EF ACL '6F57'
EF CMI '6F58'
EF START-HFN '6F5B'
EF THRESHOLD '6F5C'
EF PLMNwAcT '6F60'
EF OPLMNwAcT '6F61'
EF HPLMNwAcT '6F62'
EF EHPLMN '6FD9'
EF PSLOCI '6F73'
EF ACC '6F78'
EF FPLMN '6F7B'
EF LOCI '6F7E'
EF ICI '6F80'
EF OCI '6F81'
EF ICT '6F82'
EF OCT '6F83'
EF AD '6FAD'
EF eMLPP '6FB5'
EF AAeM '6FB6'
EF ECC '6FB7'
EF Hiddenkey '6FC3'
EF NETPAR '6FC4'
EF PNN '6FC5'
EF OPL '6FC6'
EF MBDN '6FC7'

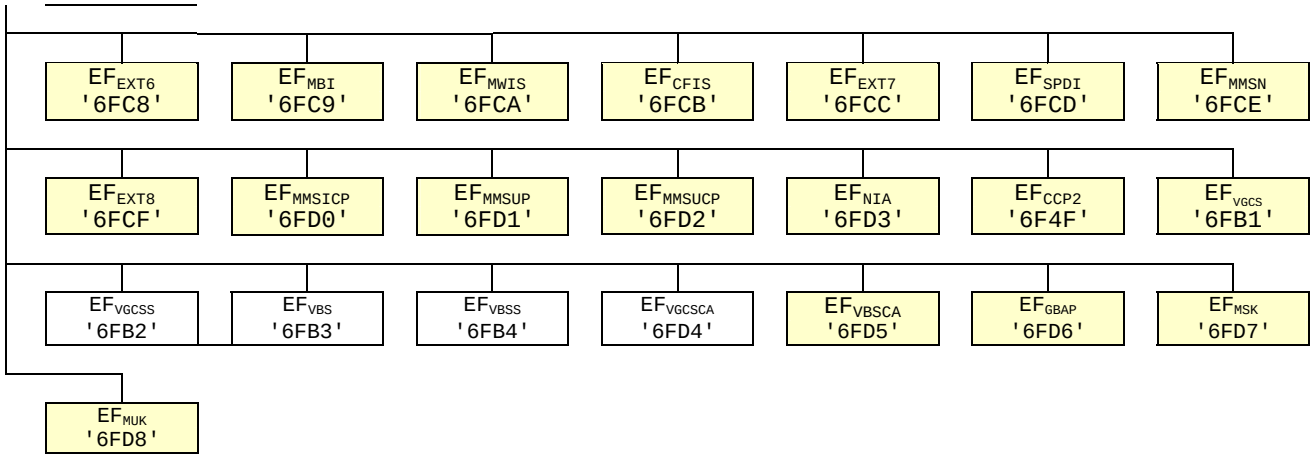


Figure 4.2: File identifiers and directory structures of USIM

5.1.1.2 USIM initialisation

The ME requests the emergency call codes. For service requirements, see TS 22.101 [24].

The ME requests the Language Indication. The preferred language selection shall always use the EF_{LI} in preference to the EF_{PL} at the MF unless any of the following conditions applies:

- if the EF_{LI} has the value 'FFFF' in its highest priority position, then the preferred language selection shall be the language preference in the EF_{PL} at the MF level according the procedure defined in TS 31.101[11];
- if the ME does not support any of the language codes indicated in EF_{LI}, or if EF_{LI} is not present, then the language selection shall be as defined in EF_{PL} at the MF level according the procedure defined in TS 31.101[11];
- if neither the languages of EF_{LI} nor EF_{PL} are supported by the terminal, then the terminal shall use its own internal default selection.

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

The ME performs the administrative information request.

The ME performs the USIM Service Table request.

The ME performs the Enabled Services Table Request.

In case FDN is enabled, an ME which does not support FDN shall allow emergency calls but shall not allow MO-CS calls and MO-SMS.

If BDN is enabled, an ME which does not support Call Control shall allow emergency calls but shall not allow MO-CS calls.

If ACL is enabled, an ME which does not support ACL shall not send any APN to the network.

If all these procedures have been performed successfully then 3G session shall start. In all other cases 3G session shall not start.

Afterwards, the ME runs the following procedures if the ME and the USIM support the related services:

- IMSI request.
- Access control information request.
- Higher Priority PLMN search period request.

- EHPLMN request
- HPLMN selector with Access Technology request;
- User controlled PLMN selector with Access Technology request;
- Operator controlled PLMN selector with Access Technology request;
- GSM initialisation requests.
- Location Information request for CS-and/or PS-mode.
- Cipher key and integrity key request for CS- and/or PS-mode.
- Forbidden PLMN request.
- Initialisation value for hyperframe number request.
- Maximum value of START request.
- CBMID request.
- Depending on the further services that are supported by both the ME and the USIM the corresponding EFs have to be read.

After the USIM initialisation has been completed successfully, the ME is ready for a 3G session and shall indicate this to the USIM by sending a particular STATUS command.

5.2.zz EHPLMN request

- Requirement: Service n°71 "available".
- Request: The ME performs the reading procedure with EF_{EHPLMN}.

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

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

File identification	Description	Change advised
'2F00'	Application directory	Caution
'2F05'	Preferred languages	Yes
'2F06'	Access rule reference	Caution
'2FE2'	ICC identification	No
'4F20'	Image data	Yes
'4F20'	GSM Ciphering key Kc	No
'4FXX'	Image Instance data Files	Yes
'4FXX'	Unique identifier	Yes
'4F22'	Phone book synchronisation counter	Yes
'4F23'	Change counter	Yes
'4F24'	Previous unique identifier	Yes
'4F30'	Phone book reference file	Yes
'4FXX'	Capability configuration parameters 1	Yes
'4F30'	SoLSA Access Indicator	Caution
'4F31'	SoLSA LSA List	Caution
'4FXX'	LSA Descriptor files	Caution
'4F52'	GPRS Ciphring key KcGPRS	No
'4F63'	CPBCCH Information	No
'4F64'	Investigation Scan	Caution
'4FXX'	Additional number alpha string	Yes
'4FXX'	Additional number	Yes
'4FXX'	Second name entry	Yes
'4FXX'	Grouping information alpha string	Yes
'4FXX'	Phone book control	Yes
'4FXX'	E-mail addresses	Yes
'4FXX'	Index administration phone book	Yes
'4FXX'	Extension 1	Yes
'4FXX'	Abbreviated dialling numbers	Yes
'4FXX'	Grouping file	Yes
'4F41'	Pseudonym	Caution
'4F42'	User controlled PLMN selector for WLAN	No
'4F43'	Operator controlled PLMN selector for WLAN	Caution
'4F44'	User controlled WSID List	No
'4F45'	Operator controlled WSID List	Caution
'4F46'	WLAN Reauthentication Identity	No
'4F47'	Multimedia Messages List	Yes
'4F48'	Multimedia Messages Data File	Yes
'6F05'	Language indication	Yes
'6F06'	Access rule reference (under ADF_{USIM} and $DF_{TELECOM}$)	Caution
'6F07'	IMSI	Caution (Note 1)
'6F08'	Ciphering and integrity keys	No
'6F09'	Ciphering and integrity keys for packet switched domain	No
'6F2C'	De-personalization Control Keys	Caution
'6F31'	Higher Priority PLMN search period	Caution
'6F32'	Co-operative network list	Caution
'6F37'	ACM maximum value	Yes
'6F38'	USIM service table	Caution
'6F39'	Accumulated call meter	Yes
'6F3B'	Fixed dialling numbers	Yes
'6F3C'	Short messages	Yes
'6F3E'	Group identifier level 1	Yes

File identification	Description	Change advised
'6F3F'	Group identifier level 2	Yes

Continued….

File identification	Description	Change advised
'6F40'	MSISDN storage	Yes
'6F41'	PUCT	Yes
'6F42'	SMS parameters	Yes
'6F43'	SMS status	Yes
'6F45'	CBMI	Caution
'6F46'	Service provider name	Yes
'6F47'	Short message status reports	Yes
'6F48'	CBMID	Yes
'6F49'	Service Dialling Numbers	Yes
'6F4B'	Extension 2	Yes
'6F4C'	Extension 3	Yes
'6F4D'	Barred dialling numbers	Yes
'6F4E'	Extension 5	Yes
'6F4F'	Capability configuration parameters 2	Yes
'6F50'	CBMIR	Yes
'6F54'	SetUp Menu Elements	Yes
'6F55'	Extension 4	Yes
'6F56'	Enabled services table	Caution
'6F57'	Access point name control list	Yes
'6F58'	Comparison method information	Yes
'6F5B'	Initialisation value for Hyperframe number	Caution
'6F5C'	Maximum value of START	Yes
'6F60'	User controlled PLMN selector with Access Technology	No
'6F61'	Operator controlled PLMN selector with Access Technology	Caution
'6F62'	HPLMN selector with Access Technology	Caution
'6F73'	Packet switched location information	Caution
'6F78'	Access control class	Caution
'6F7B'	Forbidden PLMNs	Caution
'6F7E'	Location information	No (Note 1)
'6F80'	Incoming call information	Yes
'6F81'	Outgoing call information	Yes
'6F82'	Incoming call timer	Yes
'6F83'	Outgoing call timer	Yes
'6FAD'	Administrative data	Caution
'6FB1'	Voice Group Call Service	Yes
'6FB2'	Voice Group Call Service Status	Yes
'6FB3'	Voice Broadcast Service	Yes
'6FB4'	Voice Broadcast Service Status	Yes
'6FB5'	Enhanced Multi Level Pre-emption and Priority	Yes
'6FB6'	Automatic Answer for eMLPP Service	Yes
'6FB7'	Emergency Call Codes	Caution
'6FC3'	Key for hidden phone book entries	No
'6FC4'	Network Parameters	No
'6FC5'	PLMN Network Name	Yes
'6FC6'	Operator Network List	Yes
'6FC7'	Mailbox Dialling Numbers	Yes
'6FC8'	Extension 6	Yes
'6FC9'	Mailbox Identifier	Caution
'6FCA'	Message Waiting Indication Status	Caution
'6FCB'	Call Forwarding Indication Status	Caution
'6FCC'	Extension 7	Yes
'6FCD'	Service Provider Display Information	Yes
'6FCE'	MMS Notification	Yes
'6FCF'	Extension 8	Yes
'6FD0'	MMS Issuer Connectivity Parameters	Yes
'6FD1'	MMS User Preferences	Yes
'6FD2'	MMS User Connectivity Parameters	Yes
'6FD3'	Network's indication of alerting (NIA)	Caution
'6FD4'	Voice Group Call Service Ciphering Algorithm	Yes
'6FD5'	Voice Broadcast Service Ciphering Algorithm	Yes
'6FD6'	GBA Bootstrapping parameters	Caution
'6FD7'	MBMS Service Keys List	Caution

File identification	Description	Change advised
'6FD8'	MBMS User Key	Caution
'6FD9'	EHPLMN	Caution
NOTE1: If EF_{IMSI} is changed, the UICC should issue REFRESH as defined in TS 31.111 and update EF_{LOCI} accordingly.		

Annex E (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
'2F00'	Application directory	Card issuer/operator dependant
'2F05'	Preferred languages	'FF…FF'
'2F06'	Access rule reference	Card issuer/operator dependant
'2FE2'	ICC identification	operator dependant
'4F20'	Image data	'00FF...FF'
'4F20'	GSM Ciphering key Kc	'FF...FF07'
'4FXX'	Image instance data files	'FF…FF'
'4FXX'	Unique identifier	'0000'
'4F22'	Phone book synchronisation counter	'00000000'
'4F23'	Change counter	'0000'
'4F24'	Previous unique identifier	'0000'
'4F30'	Phone book reference file	Operator dependant
'4F30'	SoLSA Access Indicator	'00FF...FF'
'4F31'	SoLSA LSA List	'FF...FF'
'4FXX'	LSA Descriptor files	'FF…FF'
'4FXX'	Capability configuration parameters 1	'FF…FF'
'4F52'	GPRS Ciphring key KcGPRS	'FF...FF07'
'4F63'	CPBCCH Information	'FF..FF'
'4F64'	Investigation PLMN scan	'00'
'4FXX'	E-mail addresses	'FF…FF'
'4FXX'	Additional number alpha string	'FF…FF'
'4FXX'	Second name entry	'FF…FF'
'4FXX'	Abbreviated dialling numbers	'FF...FF'
'4FXX'	Grouping file	'00…00'
'4FXX'	Grouping information alpha string	'FF…FF'
'4FXX'	Phone book control	'0000'
'4FXX'	Index administration phone book	'FF…FF'
'4FXX'	Additional number	'FF…FF'
'4FXX'	Extension 1	'00FF...FF'
'4F41'	Pseudonym	'00FF…FF'
'4F42'	User Controlled PLMN selector for WLAN	'FF…FF'
'4F43'	Operator Controlled PLMN selector for WLAN	Operator dependant
'4F44'	User Controlled WSID list	'00FF…FF'
'4F45'	Operator controlled WSID list	Operator dependant
'4F46'	WLAN Reauthentication Identity	'FF…FF'
'4F47'	Multimedia Messages List	'FF…FF'
'4F48'	Multimedia Messages Data File	'FF…FF'
'6F05'	Language indication	'FF…FF'
'6F06'	Access rule reference (under ADF_{USIM} and $DF_{TELECOM}$)	Card issuer/operator dependant
'6F07'	IMSI	Operator dependant
'6F08'	Ciphering and integrity keys	'07FF…FF'
'6F09'	Ciphering and integrity keys for packet switched domain	'07FF…FF'
'6F2C'	De-personalization control keys	'FF…FF'
'6F31'	Higher Priority PLMN search period	'FF'
'6F32'	Co-operative network list	'FF…FF'
'6F37'	ACM maximum value	'000000' (see note 1)
'6F38'	USIM service table	Operator dependant
'6F39'	Accumulated call meter	'000000'
'6F3B'	Fixed dialling numbers	'FF...FF'
'6F3C'	Short messages	'00FF...FF'
'6F3E'	Group identifier level 1	Operator dependant
'6F3F'	Group identifier level 2	Operator dependant
'6F40'	MSISDN storage	'FF...FF'
'6F41'	PUCT	'FFFFFF0000'
'6F42'	SMS parameters	'FF...FF'
'6F43'	SMS status	'FF...FF'
'6F45'	CBMI	'FF...FF'
'6F46'	Service provider name	Operator dependant
'6F47'	Short message status reports	'00FF…FF'
'6F48'	CBMID	'FF...FF'
'6F49'	Service Dialling Numbers	'FF...FF'

'6F4B'	Extension 2	'00FF...FF'
'6F4C'	Extension 3	'00FF...FF'

Continued....

File Identification	Description	Value
'6F4D'	Barred Dialling Numbers	'FF...FF'
'6F4E'	Extension 5	'00FF...FF'
'6F4F'	Capability configuration parameters 2	'FF...FF'
'6F50'	CBMIR	'FF...FF'
'6F54'	SetUp Menu Elements	Operator dependant
'6F55'	Extension 4	'00FF...FF'
'6F56'	Enabled services table	Operator dependant
'6F57'	Access point name control list	'00FF…FF'
'6F58'	Comparison method information	'FF…FF'
'6F5B'	Initialisation value for Hyperframe number	'F0 00 00 F0 00 00'
'6F5C'	Maximum value of START	Operator dependant
'6F60'	User controlled PLMN selector with Access Technology	'FFFFFF0000..FFFFFF0000'
'6F61'	Operator controlled PLMN selector with Access Technology	'FFFFFF0000..FFFFFF0000'
'6F62'	HPLMN selector with Access Technology	'FFFFFF0000..FFFFFF0000'
'6F73'	Packet switched location information	'FFFFFFFF FFFFFF xxxxxx 0000 FF 01' (see note 2)
'6F78'	Access control class	Operator dependant
'6F7B'	Forbidden PLMNs	'FF...FF'
'6F7E	Location information	'FFFFFFFF xxxxxx 0000 FF 01' (see note 2)
'6F80'	Incoming call information	'FF…FF 000000 00 01FFFF'
'6F81'	Outgoing call information	'FF…FF 000000 01FFFF'
'6F82'	Incoming call timer	'000000'
'6F83'	Outgoing call timer	'000000'
'6FAD'	Administrative data	Operator dependant
'6FB1'	Voice Group Call Service	Operator dependant
'6FB2'	Voice Group Call Service Status	Operator dependant
'6FB3'	Voice Broadcast Service	Operator dependant
'6FB4'	Voice Broadcast Service Status	Operator dependant
'6FB5'	EMLPP	Operator dependant
'6FB6'	AaeM	'00'
'6FB7'	Emergency call codes	Operator dependant
'6FC3'	Key for hidden phone book entries	'FF…FF'
'6FC4'	Network Parameters	'FF…FF'
'6FC5'	PLMN Network Name	Operator dependant
'6FC6'	Operator Network List	Operator dependant
'6FC7'	Mailbox Dialling Numbers	Operator dependant
'6FC8'	Extension 6	'00 FF...FF'
'6FC9'	Mailbox Identifier	Operator dependant
'6FCA'	Message Waiting Indication Status	'00 00 00 00 00'
'6FCB'	Call Forwarding Indication Status	'xx 00 FF...FF'
'6FCC'	Extension 7	'00 FF...FF'
'6FCD'	Service Provider Display Information	
'6FCE'	MMS Notification	'00 00 00 FF…FF'
'6FCF'	Extension 8	'00FF...FF'
'6FD0'	MMS Issuer Connectivity Parameters	'FF…FF'
'6FD1'	MMS User Preferences	'FF…FF'
'6FD2'	MMS User Connectivity Parameters	'FF…FF'
'6FD3'	Network's Indication of Alerting (NIA)	'FF...FF'
'6FD4'	Voice Group Call Service Ciphering Algorithm	'00…00'
'6FD5'	Voice Broadcast Service Ciphering Algorithm	'00…00'
'6FD6'	GBA Bootstrapping parameters	'FF…FF'
'6FD7'	MBMS Service Keys List	'FF…FF'
'6FD8'	MBMS User Key	'FF…FF'
'6FD9'	EHPLMN	'FF…FF' or xxxxxx (see Note 2)

NOTE 1: The value '000000' means that ACMmax is not valid, i.e. there is no restriction on the ACM. When assigning a value to ACMmax, care should be taken not to use values too close to the maximum possible value 'FFFFFF', because the INCREASE command does not update EF_{ACM} if the units to be added would exceed 'FFFFFF'. This could affect the call termination procedure of the Advice of Charge function.

NOTE 2: xxxxxx stands for any valid MCC and MNC, coded according to TS 24.008 [9].

3GPP TSG-T3 #34
Barcelona, Spain
08-11 February 2005

T3-050201
previous document: T3-040825

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.102** **CR** **250** ⌘ **rev** **2** ⌘ Current version: **6.8.0** ⌘

*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:	⌘	Enable multiple Terminal Profile downloads in UST
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	11/02/2005
Category:	⌘	**B**
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:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change:	⌘	Applets and applications that were designed for earlier releases may expect a Terminal Profile only during the initialisation procedure. Due to the lack of other mechanisms, the Terminal Profile could have been used for startup processing, etc. Allowing additional Terminal Profiles, as introduced in TS 102 223 v6.4.0, could cause problems if cards with these applications were used in new phones.
Summary of change:	⌘	Additional Terminal Profiles are only allowed, if the corresponding service is activated in the UST.
Consequences if not approved:	⌘	Backwards compatibility problems with applications on existing cards used in new phones.

Clauses affected:	⌘	4.2.8			
Other specs affected:	⌘	**Y** / **N**	Other core specifications	⌘	TS 31.111 – see T3-050032
		X /	Test specifications		
		/	O&M Specifications		
Other comments:	⌘				

4.2.8 EF_{UST} (USIM Service Table)

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

Identifier: '6F38'	Structure: transparent	Mandatory
SFI: '04'		
File size: X bytes, X >= 1	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

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

-Services

Contents:

Service n°1:	Local Phone Book
Service n°2:	Fixed Dialling Numbers (FDN)
Service n°3:	Extension 2
Service n°4:	Service Dialling Numbers (SDN)
Service n°5:	Extension3
Service n°6:	Barred Dialling Numbers (BDN)
Service n°7:	Extension4
Service n°8:	Outgoing Call Information (OCI and OCT)
...	...
Service n°60	User Controlled PLMN selector for WLAN access
Service n°61	Operator Controlled PLMN selector for WLAN access
Service n°62	User controlled WSID list
Service n°63	Operator controlled WSID list
Service n°64	VGCS security
Service n°65	VBS security
Service n°66	WLAN Reauthentication Identity
Service n°67	Multimedia Messages Storage
Service n°68	Generic Bootstrapping Architecture (GBA)
Service n°69	MBMS security
Service n°70	Data download via USSD and USSD application mode
Service n°71	Equivalent HPLMN
Service n°xx	Additional TERMINAL PROFILE after UICC activation