3GPP TSG-T (Terminals) Meeting #25
Palm Springs, CA, USA
8 - 10 September 2004

TP-040181

Agenda Item: 5.3.3
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#25 for approval:

Doc-2nd-Level	Spec	CR	Rev	Phase	Subject	Cat	Version-Current	Version-New	Workitem
T3-040539	31.102	234	-	Rel-6	MMs storage on the card	B	6.6.0	6.7.0	TEI
T3-040540	31.102	235	-	Rel-6	GBAU ME-USIM interface	B	6.6.0	6.7.0	SEC1-SC
T3-040545	31.102	238	-	Rel-6	Storage of WLAN fast re-authentication information	B	6.6.0	6.7.0	TEI
T3-040572	31.102	239	-	Rel-6	MBMS security	B	6.6.0	6.7.0	MBMS
T3-040584	31.102	240	-	Rel-5	Correction of a wrong reference to TS 102 221	F	5.9.0	5.10.0	TEI
T3-040585	31.102	241	-	Rel-6	Removal of a wrong reference to 102 221	F	6.6.0	6.7.0	TEI
T3-040591	31.102	233	1	Rel-6	VGCS/VBS security	B	6.6.0	6.7.0	TEI
T3-040593	31.102	236	-	Rel-6	Introduction of M-IMAP and SIP as MMS implementations in MMS provisioning	B	6.6.0	6.7.0	TEI
T3-040597	31.102	237	1	Rel-6	Editorial changes in WLAN identities lists	D	6.6.0	6.7.0	I-WLAN
T3-040603	31.102	242	-	Rel-6	Alignement with requirements regarding USSD usage	B	6.6.0	6.7.0	TEI
T3-040606	31.102	243	-	Rel-5	Correction of PPS procedure	F	5.9.0	5.10.0	TEI

3GPP TSG-T3 Meeting #32
Ney York, USA, 10-13 August 2004,

Tdoc ⌘ T3-040539

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.102** **CR** **234** ⌘ **rev** **-** ⌘ Current version: **6.6.0** ⌘

*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:	⌘	MMs storage on the card
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	11/08/2004
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:	⌘	As required by TS 22.140, a USIM must be able to support the MMs storage functionality. This CR proposes a way to store MMs in the current release of the specification.
Summary of change:	⌘	The following changes are included: - Adding $DF_{MULTIMEDIA}$ under $DF_{TELECOM}$ to group all files related to MM storage - Adding EF_{MML} to store the list of Multimedia Messages - Adding EF_{MMDF} to store MMs content
Consequences if not approved:	⌘	No support of MM storage on the USIM
Clauses affected:	⌘	3.3, 4.2.8, 4.6, 4.7, Annex A, Annex E New sections 4.6.x, 4.6.x.1, 4.6.x.2, 5.3.x

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

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	3rd Generation Partnership Project
AC	Access Condition
ACL	APN Control List
ADF	Application Dedicated File
AID	Application IDentifier
AK	Anonymity key
ALW	ALWays
AMF	Authentication Management Field
AoC	Advice of Charge
APN	Access Point Name
ASN.1	Abstract Syntax Notation One
AuC	Authentication Centre
AUTN	Authentication token
BDN	Barred Dialling Number
BER-TLV	Basic Encoding Rule - TLV
CCP	Capability Configuration Parameter
CK	Cipher key
CLI	Calling Line Identifier
CNL	Co-operative Network List
CPBCCH	COMPACT Packet BCCH
CS	Circuit switched
DCK	Depersonalisation Control Keys
DF	Dedicated File
DO	Data Object
EF	Elementary File
FCP	File Control Parameters
FFS	For Further Study
GSM	Global System for Mobile communications
HE	Home Environment
ICC	Integrated Circuit Card
ICI	Incoming Call Information
ICT	Incoming Call Timer
ID	IDentifier
IEI	Information Element Identifier
IK	Integrity key
IMSI	International Mobile Subscriber Identity
K	USIM Individual key
K_C	Cryptographic key used by the cipher A5
KSI	Key Set Identifier
LI	Language Indication
LSB	Least Significant Bit
MAC	Message authentication code
MAC-A	MAC used for authentication and key agreement
MAC-I	MAC used for data integrity of signalling messages
MCC	Mobile Country Code
MExE	Mobile Execution Environment
MF	Master File
MM	Multimedia Message
MMI	Man Machine Interface
MMS	Multimedia Messaging Service
MNC	Mobile Network Code
MODE	Indication packet switched/circuit switched mode
MSB	Most Significant Bit
NEV	NEVer
NPI	Numbering Plan Identifier

OCI	Outgoing Call Information
OCT	Outgoing Call Timer
PBID	Phonebook Identifier
PIN	Personal Identification Number
PL	Preferred Languages
PS	Packet switched
PS_DO	PIN Status Data Object
RAND	Random challenge
$RAND_{MS}$	Random challenge stored in the USIM
RES	User response
RFU	Reserved for Future Use
RST	Reset
SDN	Service dialling number
SE	Security Environment
SFI	Short EF Identifier
SGSN	Serving GPRS Support Node
SN	Serving Network
SQN	Sequence number
SRES	Signed RESponse calculated by a USIM
SW	Status Word
TLV	Tag Length Value
USAT	USIM Application Toolkit
USIM	Universal Subscriber Identity Module
VLR	Visitor Location Register
XRES	Expected user RESponse

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 SSID list
	Service n°63	Operator controlled SSID list
	Service n°64	VGCS security
	Service n°xx	Multimedia Messages Storage

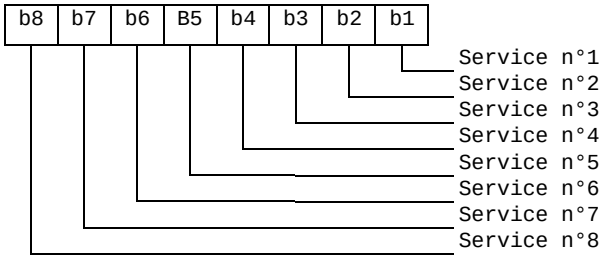
The EF shall contain at least one byte. Further bytes may be included, but if the EF includes an optional byte, then it is mandatory for the EF to also contain all bytes before that byte. Other services are possible in the future and will be coded on further bytes in the EF. The coding falls under the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

Coding:

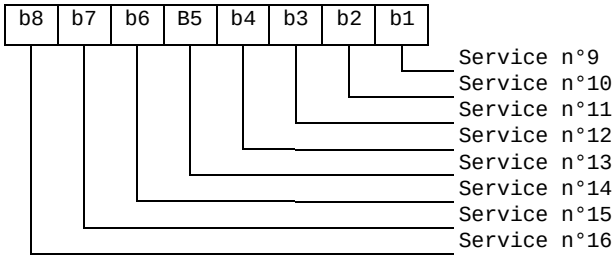
1 bit is used to code each service:
bit = 1: service available;
bit = 0: service not available.

- 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.

4.6 Contents of DFs at the TELECOM level

DFs may be present as child directories of $DF_{TELECOM}$. The following DFs have been defined:

- $DF_{GRAPHICS}$ '5F50'.
- $DF_{PHONEBOOK}$ '5F3A'.

(DF for public phone book. This DF has the same structure as $DF_{PHONEBOOK}$ under ADF USIM).

- $DF_{MULTIMEDIA}$ '5Fxx'.

4.6.x Contents of files at the $DF_{MULTIMEDIA}$ level

The EFs in the Dedicated File $DF_{MULTIMEDIA}$ contain multimedia information. This DF shall be present if service n°xx is available, i.e. if the card supports MMS storage.

4.6.x.1 EF_{MML} (Multimedia Messages List)

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

This file contains information about the MM data stored in EF_{MMDF}. MM information are encapsulated in a BER-TLV data object. Each data object in EF_{MML} points to a corresponding MM in EF_{MMDF}.

Identifier: '4Fxx'	Structure: BER-TLV	Optional
	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to X	MM Descriptor Data Object(s)	M	X bytes

- MM Descriptor Data Object

The content and coding are defined below:

Coding of the MM Descriptor Data Objects

Length	Description	Coding	Status
1 to A bytes (A ≤ 3)	MM Descriptor Data Object tag	As defined in TS 31.101 [11] for BER-TLV structured files	M
1 to B bytes (B ≤ 4)	MM Descriptor Data Object length	As defined in TS 31.101 [11] for BER-TLV structured files	M
1 byte	MMS Implementation tag '80'		M
1 byte	MMS Implementation length		M
1 byte	MMS Implementation	See below	M
1 byte	MM File Identifier / SFI tag '81'		M
1 byte	MM File Identifier / SFI length		M
1 or 2 bytes	MM File Identifier / SFI	See below	M
1 byte	MM Content Data Object Tag tag '82'		M
1 byte	MM Content Data Object Tag length		M
1 to C bytes (C ≤ 3)	MM Content Data Object Tag	See below	M
1 byte	MM Size tag '83'		M
1 byte	MM Size length		M
1 to D bytes (D ≤ 4)	MM Size in bytes	See below	M
1 byte	MM Status tag '84'		M
1 byte	MM Status length		M
2 bytes	MM Status	See below	M
1 byte	MM Alpha Identifier tag '85'		M
1 byte	MM Alpha Identifier length		M
1 to E bytes	MM Alpha Identifier	See below	M

- MMS Implementation

Contents:

The MMS Implementation indicates the used implementation type, e.g. WAP.

Coding:

Allocation of bits:

Bit number	Parameter indicated
1	WAP implementation of MMS
2-8	Reserved for future use

Bit value	Meaning
0	Implementation not supported.
1	Implementation supported.

- MM File Identifier / SFI

Contents:

file identifier or SFI of EF_{MMDF} which contains the actual MM message. If the length of this TLV object is equal to 1 then the content indicates the SFI of the EF_{MMDF}, the SFI is coded on b1 to b5. Otherwise the TLV contains the file identifier.

Coding:

according to TS 31.101 [11].

- MM Content Data Object Tag

Contents:

tag indentifying a MM (i.e. identifying a data object) within EF_{MMDF}.

Coding:

according to TS 31.101 [11].

- MM Size

Contents:

size of the corresponding MM stored in EF_{MMDF}.

Coding:

according to TS 31.101 [11].

- MM Status

Contents:

The status bytes contain the status information of the stored Multimedia Message.

Coding:

First byte:

bit b1 indicates whether the MM has been read or not. Bit b2 indicates the MM forwarding status. Bit b3 indicates whether it is a received MM or an originated MM. Bits b4-b8 are reserved for future use.

Second byte:

Coding of the second byte depends on whether the MM has been identified as a received MM or originated MM in the first byte:

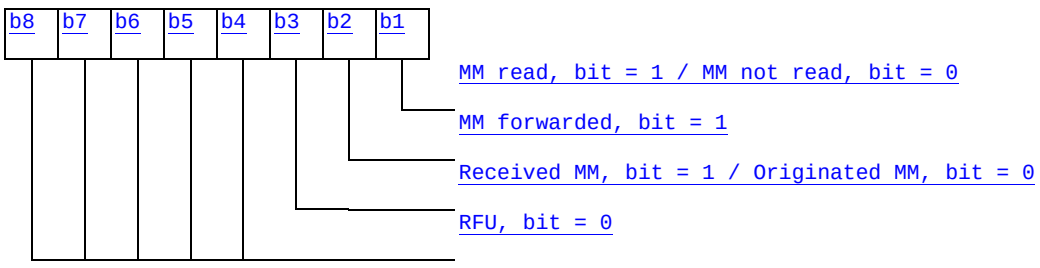
- Received MM coding:

  bits b1 and b2 are used to provide information on Read-reply reports. Bits b3 to b8 are reserved for future use.

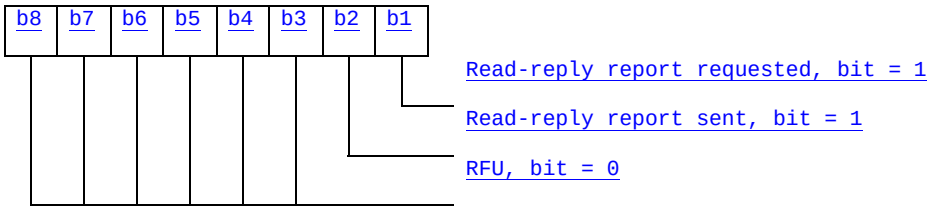
- Originated MM coding:

  bit b1 is used to provide information on Delivery-report. Bits b2 to b8 are reserved for future use.

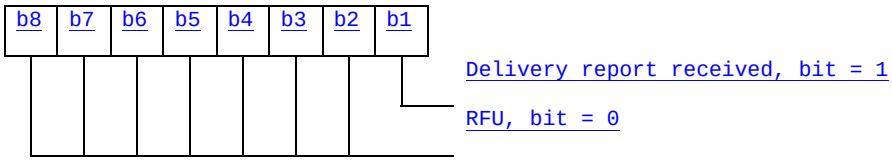
First byte:



Second byte coding for Received MM:



Second byte coding for Originated MM:



- MM Alpha Identifier

  Contents:

  information about the MM to be displayed to the user (e.g. sender, subject, date etc).

  Coding:

  this alpha identifier shall use either:

  - the SMS default 7-bit coded alphabet as defined in TS 23.038 [5] with bit 8 set to 0. The alpha identifier shall be left justified. Unused bytes shall be set to 'FF';
  - or one of the UCS2 coded options as defined in the annex of TS 31.101 [11].

4.6.x.2 EF_{MMDF} (Multimedia Messages Data File)

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

Residing under $DF_{MULTIMEDIA}$, this EF contains Multimedia Messages data. The structure of this EF is BER-TLV (see TS 31.101 [11]). Each MM in this file is identified by a tag. The tag value for a particular MM in this file is stored in EF_{MML}.

Identifier: '4Fxx'	Structure: BER-TLV		Optional
		Update activity: low	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM			
Bytes	Description	M/O	Length
1 to X	MM Content Data Object(s)	M	X bytes

- MM Content Data Object

  The content and coding are defined below:

Coding of the MM Content Data Objects

Length	Description	Coding	Status
1 to T bytes (T ≤ 3)	MM Content Data Object tag	As defined in TS 31.101 [11] for BER-TLV structured files	M
1 to L (L ≤ 4)	MM Content Data Object length	As defined in TS 31.101 [11] for BER-TLV structured files	M
X-L-T bytes	MM Content	According to MMS Implementation	M

Contents:

The Multimedia Message content consists of MM headers and a message body. The content of the Multimedia Message data depends on whether the MM has been identified as a received MM or an originated MM:

- For a received message, the stored Multimedia Message data consists of the information elements (i.e. relevant MM control information and MM content) of the MM1_retrieve.RES (see TS 23.140 [38]).

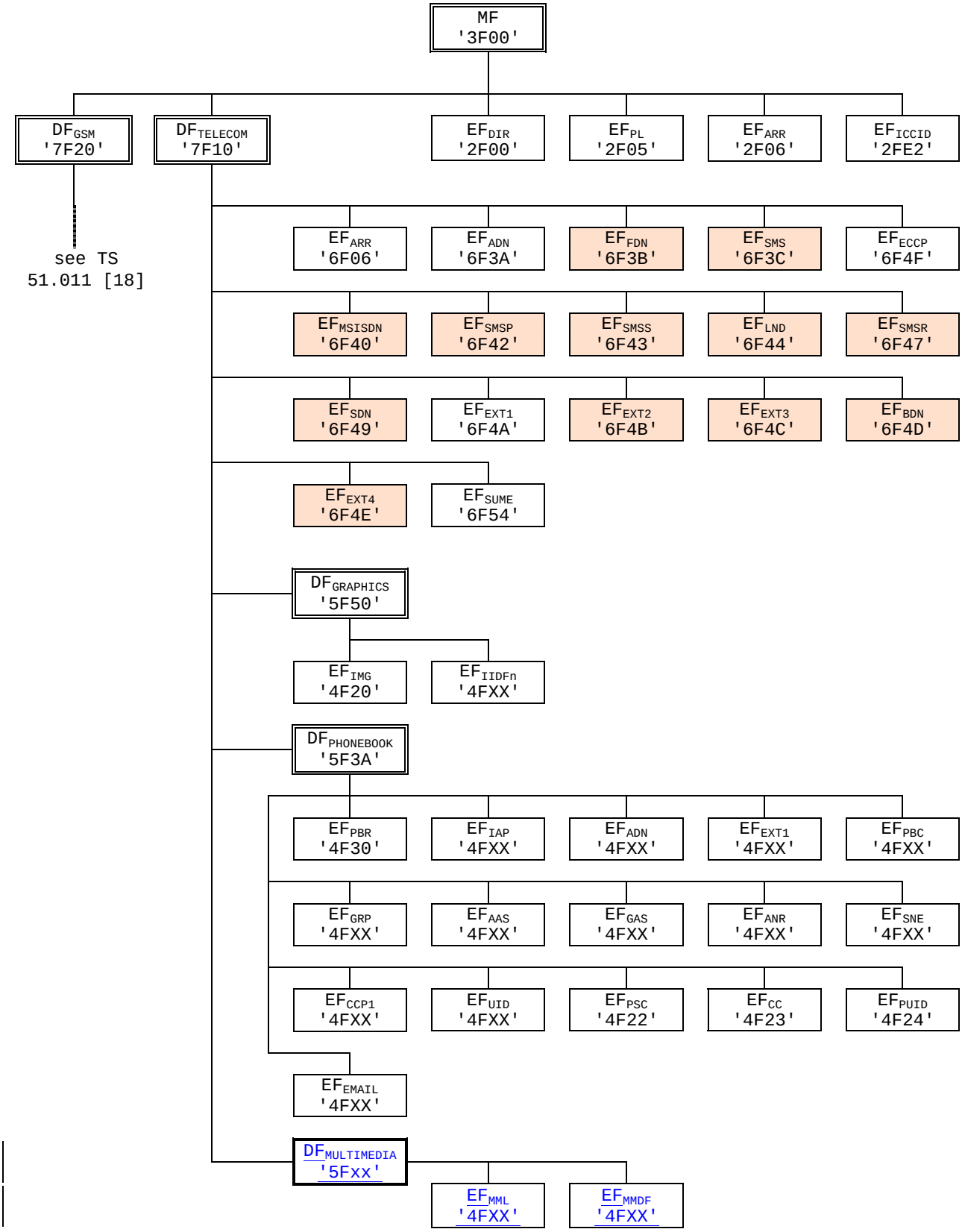
- For an originated message, the stored Multimedia Message data consists of the information elements (i.e. relevant MM control information and MM content) of the MM1_submit.REQ (see TS 23.140 [38]).

Coding:

The MM data encapsulation scheme and encoding rules are defined by the MMS Implementation.

4.7 Files of USIM

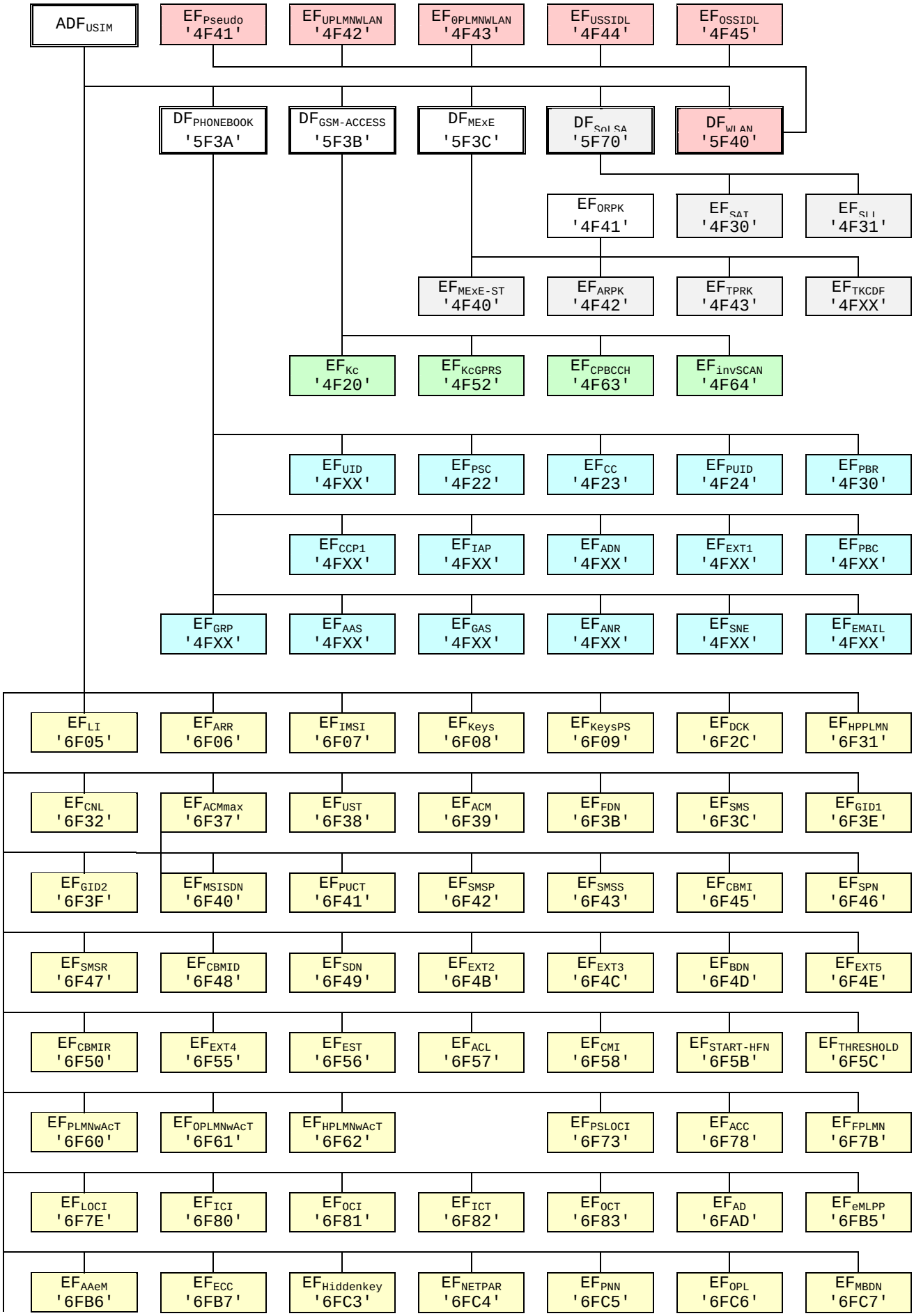
This clause contains two figures depicting the file structure of the UICC and the ADF_{USIM}. ADF_{USIM} shall be selected using the AID and information in EF_{DIR}.



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'
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 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'

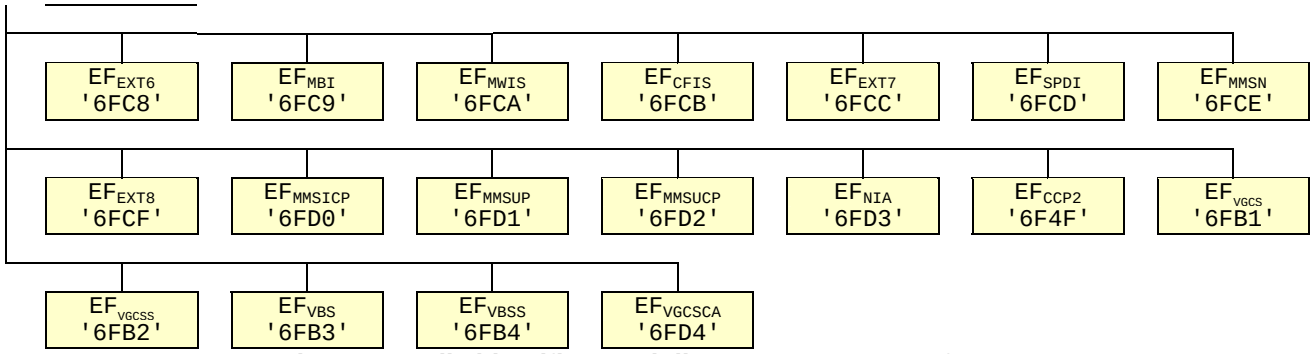


Figure 4.2: File identifiers and directory structures of USIM

5.3.x Multimedia Messages Storage

If the terminal supports Multimedia Message Storage on the USIM, then the following procedures apply.

As defined in TS 23.140 [38] a Multimedia Message consists of content, or multimedia objects, and headers to describe various properties of that content. An MM is stored in EF_{MMDF}, a BER-TLV structured file.

A list of multimedia messages is stored in the BER-TLV file EF_{MML} where each data object identifies one Multimedia Message stored in EF_{MMDF}.

Prerequisite: Service n°xx "available".

Request: The ME performs the reading procedures on EF_{MML} to verify the presence and to get the location information of the targeted MM. Then the ME performs the reading procedure of the EF_{MMDF} file to get the MM.

Update: The ME chooses a free identity (i.e. not listed in EF_{MML}) for the multimedia message and check for available space in the EF_{MMDF} file. This procedure could be done for each update or once at the startup of the UE and after a REFRESH command involving one of the $DF_{MULTIMEDIA}$ files. Then the ME performs the following procedures:

- If there is no available empty space in the EF_{MMDF} file to store the MM, the procedure is aborted and the user is notified.

- Else, the ME stores the MM in EF_{MMDF}, then updates the information in EF_{MML} accordingly.

Erasure: After a successful deletion of an MM in EF_{MMDF} the terminal updates the information in EF_{MML} accordingly.

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 SSID List	No
'4F45'	Operator controlled SSID List	Caution
'4FXX'	Multimedia Messages List	Yes
'4FXX'	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
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 SSID list	'00FF…FF'
'4F45'	Operator controlled SSID list	Operator dependant
'4FXX'	Multimedia Messages List	'FF…FF'
'4FXX'	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'

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#32
New York, USA, 10-13 August 2004

Tdoc ⌘ T3-040540

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.102** **CR** 235 ⌘ **rev** **-** ⌘ Current version: **6.6.0** ⌘

*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:	⌘	GBAU ME-USIM interface
Source:	⌘	T3
Work item code:	⌘	SEC1-SC
Date:	⌘	11/08/2004
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:	⌘	Generic Bootstrapping Architecture in TS 33.220 GBA consists of two mechanisms: ME-based GBA (GBA_ME), which reuses legacy UMTS AKA procedure and GBA with UICC-based enhancements (GBA_U) which requires a specific AKA procedure with the ISIM/USIM. GBA_U thus requires the definition of some procedures in the USIM-ME interface.
Summary of change:	⌘	The following changes are included: -New Service in UST for GBA -Storage of parameters associated with a GBA bootstrapping procedure. -New GBA security context in AUTHENTICATE command with two specific modes: Bootstrapping Mode, NAF Derivation Mode
Consequences if not approved:	⌘	Required GBA_U functionalities will not be supported. Additionally, functionalities from other work Items where GBA_U is mandated (i.e. MBMS) will not be supported

Clauses affected:	⌘	2, 3.3, 4.2.8, 4.2.x (new), 5.2.x(new), 5.2.y(new), 7.1, Annex A, Annex E

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

Other comments:	⌘	Note: Further evolutions of 33.220 in GBA_U key derivation procedure may require minor changes to the proposed text.

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: "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] ETSI TS 102 221 "Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 4)"

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

[39] ETSI TS 102 222 "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"

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

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	3rd Generation Partnership Project
AC	Access Condition
ACL	APN Control List
ADF	Application Dedicated File
AID	Application IDentifier
AK	Anonymity key
ALW	ALWays
AMF	Authentication Management Field
AoC	Advice of Charge
APN	Access Point Name
ASN.1	Abstract Syntax Notation One
AuC	Authentication Centre
AUTN	Authentication token
BDN	Barred Dialling Number
BER-TLV	Basic Encoding Rule - TLV
B-TID	Bootstrapping Transaction IDentifier
CCP	Capability Configuration Parameter
CK	Cipher key
CLI	Calling Line Identifier
CNL	Co-operative Network List
CPBCCH	COMPACT Packet BCCH
CS	Circuit switched
DCK	Depersonalisation Control Keys
DF	Dedicated File
DO	Data Object
EF	Elementary File
FCP	File Control Parameters
FFS	For Further Study
GSM	Global System for Mobile communications
HE	Home Environment
ICC	Integrated Circuit Card
ICI	Incoming Call Information
ICT	Incoming Call Timer
ID	IDentifier
IEI	Information Element Identifier
IK	Integrity key
IMSI	International Mobile Subscriber Identity
K	USIM Individual key
K_C	Cryptographic key used by the cipher A5
KSI	Key Set Identifier
LI	Language Indication
LSB	Least Significant Bit
MAC	Message authentication code
MAC-A	MAC used for authentication and key agreement
MAC-I	MAC used for data integrity of signalling messages
MCC	Mobile Country Code
MExE	Mobile Execution Environment
MF	Master File
MMI	Man Machine Interface
MNC	Mobile Network Code
MODE	Indication packet switched/circuit switched mode
MSB	Most Significant Bit
NEV	NEVer
NPI	Numbering Plan Identifier
OCI	Outgoing Call Information

OCT	Outgoing Call Timer
PBID	Phonebook Identifier
PIN	Personal Identification Number
PL	Preferred Languages
PS	Packet switched
PS_DO	PIN Status Data Object
RAND	Random challenge
$RAND_{MS}$	Random challenge stored in the USIM
RES	User response
RFU	Reserved for Future Use
RST	Reset
SDN	Service dialling number
SE	Security Environment
SFI	Short EF Identifier
SGSN	Serving GPRS Support Node
SN	Serving Network
SQN	Sequence number
SRES	Signed RESponse calculated by a USIM
SW	Status Word
TLV	Tag Length Value
USAT	USIM Application Toolkit
USIM	Universal Subscriber Identity Module
VLR	Visitor Location Register
XRES	Expected user RESponse

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 SSID list
	Service n°63	Operator controlled SSID list
	Service n°64	VGCS security
	Service n°xx	Generic Bootstrapping Architecture (GBA)

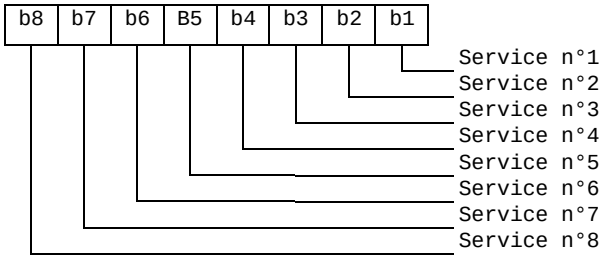
The EF shall contain at least one byte. Further bytes may be included, but if the EF includes an optional byte, then it is mandatory for the EF to also contain all bytes before that byte. Other services are possible in the future and will be coded on further bytes in the EF. The coding falls under the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

Coding:

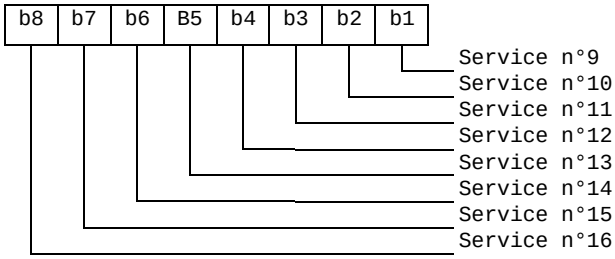
1 bit is used to code each service:
bit = 1: service available;
bit = 0: service not available.

- 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 Contents of files at the USIM ADF (Application DF) level

4.2.x EF_{GBABP} (GBA Bootstrapping parameters)

This EF contains the AKA Random challenge (RAND) and Bootstrapping Transaction Identifier (B-TID) associated with a GBA bootstrapping procedure. This file shall be present if the GBA service (service number xx) is allocated in EF_{UST} (USIM Service Table).

Identifier: '6FXX'	Structure: transparent	Optional
File length: L+X +2 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Length of RAND (X)	M	1 byte
2 to (X +1)	RAND	M	X bytes
X+2	Length of B-TID (L)	M	1 byte
(X+2) to (X+1+L)	B-TID	M	L bytes

- Length of RAND
  Contents: number of bytes, not including this length byte, of RAND field

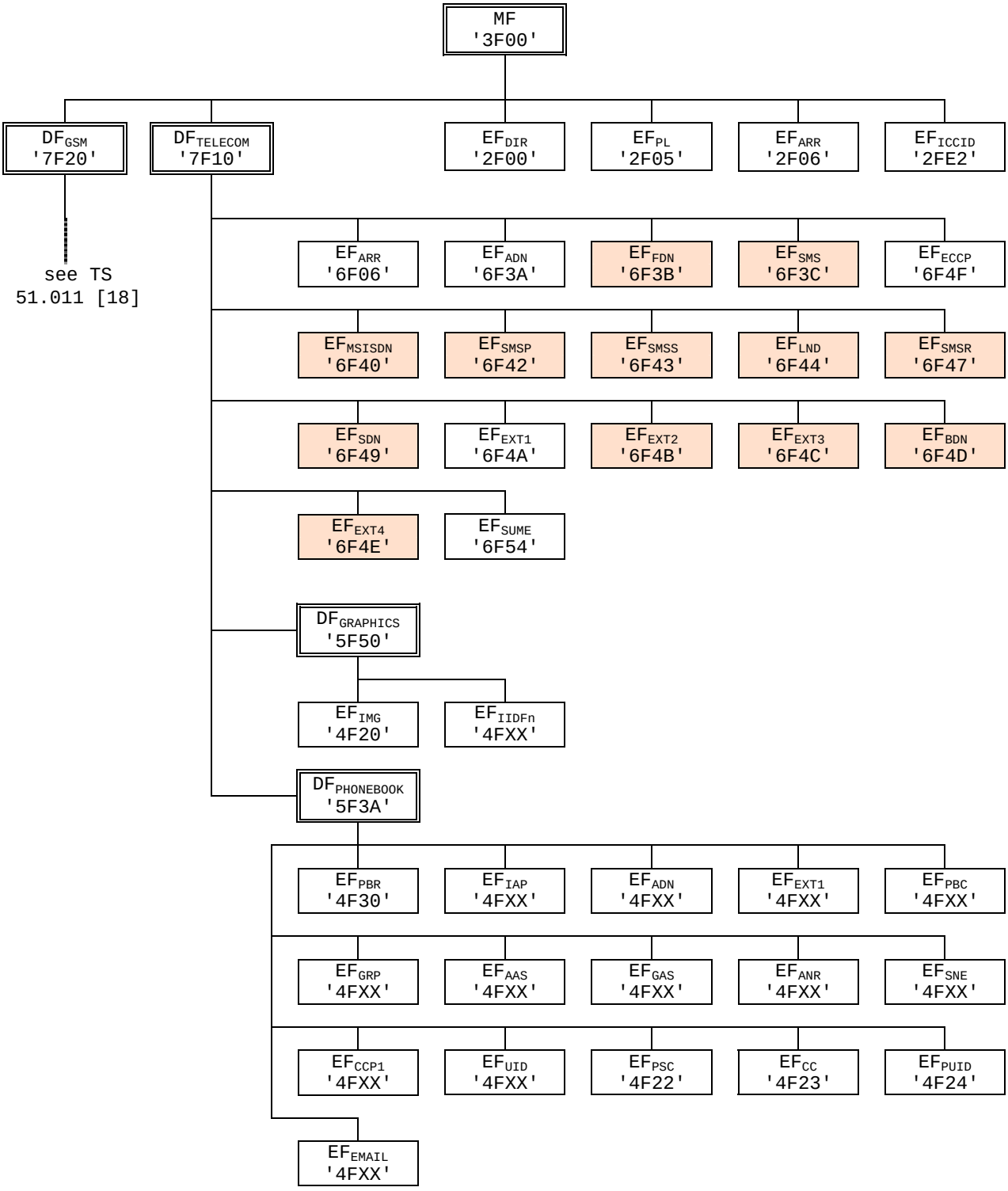
- RAND
  Contents: Random challenge used in the GBA_U bootstrapping procedure.
  Coding: as defined in 33.103 [13]

- Length of B-TID
  Contents: number of bytes, not including this length byte, of B-TID field

- B-TID
  Content: Bootstrapping Transaction Identifier the GBA_U bootstrapped keys
  Coding: As defined in TS 33.220[xx]

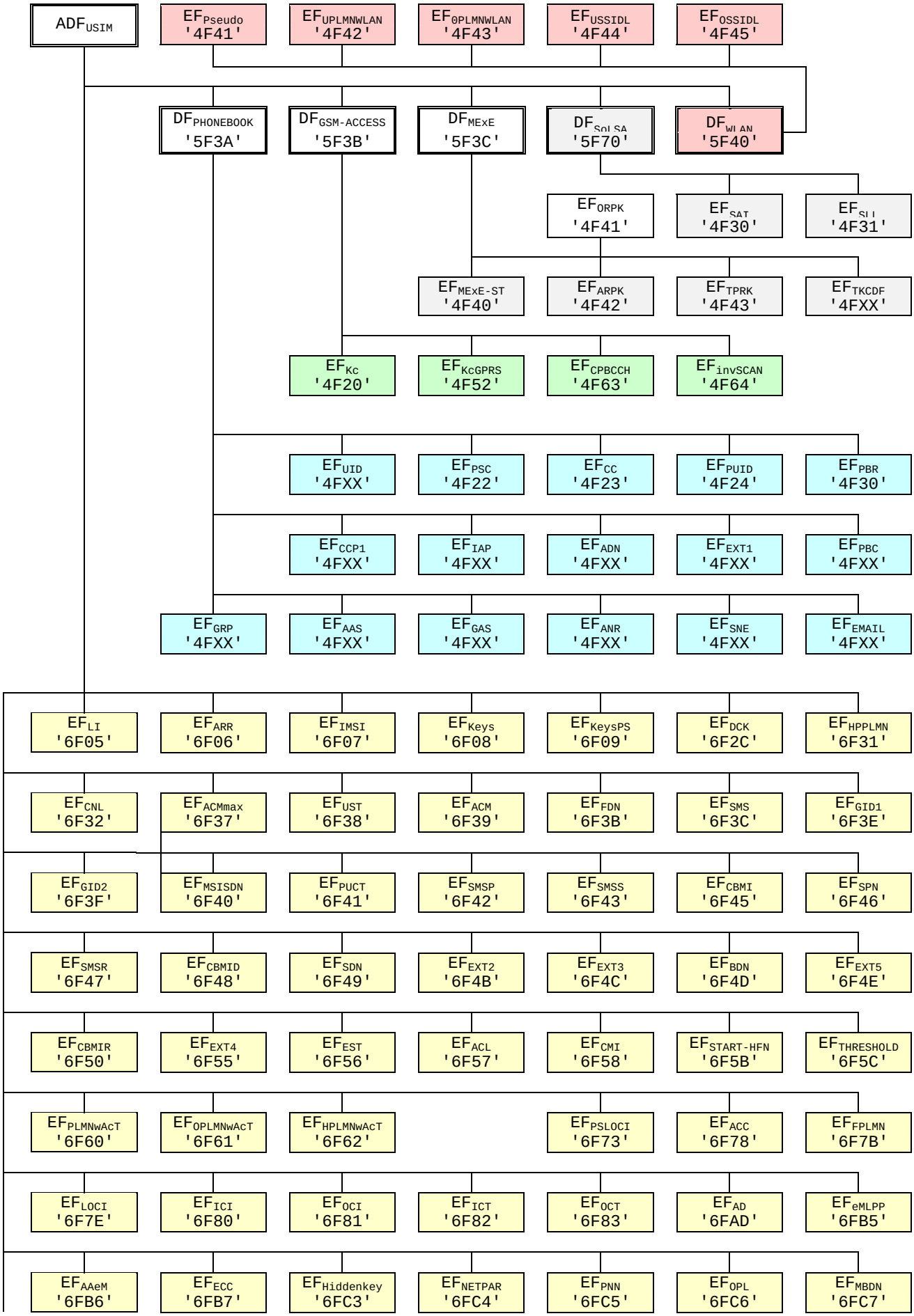
4.7 Files of USIM

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'
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 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'

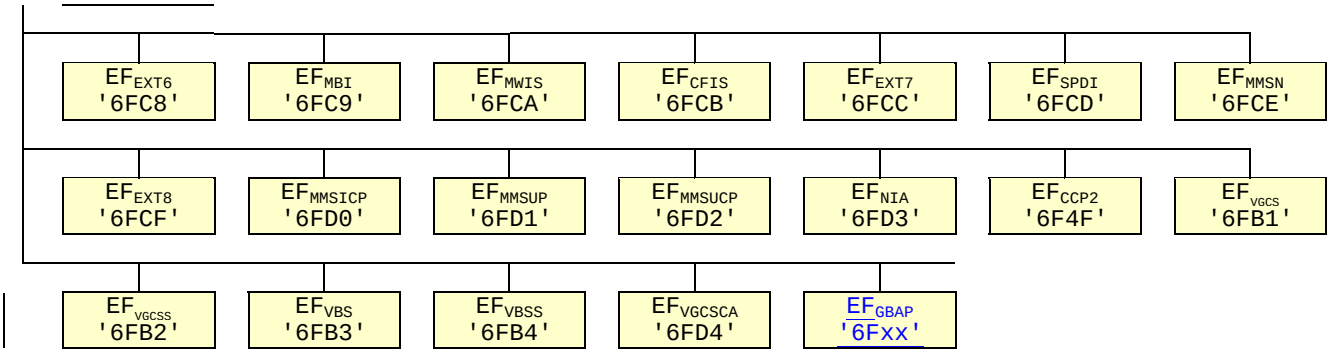


Figure 4.2: File identifiers and directory structures of USIM

5.2 USIM security related procedures

5.2.x 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 in EF_{GBABP}

5.2.y Generic Bootstrapping architecture (NAF Derivation)

The ME shall first read EF_{GBABP}. The ME then uses the AUTHENTICATE command in GBA security context (NAF Derviation Mode) (see 7.1.1). The response is sent to the ME.

7.1 AUTHENTICATE

7.1.1 Command description

The function can be used in several different contexts:

- a 3G security context, when 3G authentication vectors (RAND, XRES, CK, IK, AUTN) are available (i.e. the UE is located in the UTRAN, or in a GSM radio access network which is connected to a 3G or 3G capable VLR/SGSN), or

- a GSM security context, when GSM authentication data are available only (i.e. the UE is located in the GSM radio access network which is connected to a non-3G capable VLR/SGSN).

- an VGCS security context, when VGCS authentication data is available

- a GBA_U security context, when a GBA bootstrapping procedure is requested

The function is used in GSM or 3G security context during the procedure for authenticating the USIM to its HE and vice versa. In addition, a cipher key and an integrity key are calculated. For the execution of the command the USIM uses the subscriber authentication key K, which is stored in the USIM.

The function is used in VGCS security context during the procedure for retrieving the VGCS Short Term Key (VSTK) used by the terminal to in establishing VGCS calls.

The function is used in GBA security context in two different modes:

a) Bootstrapping Mode: during the procedure for muthual authenticating of the USIM and the Bootstrapping Server Function (BSF) and for deriving bootstrapped key material from the AKA run.

b) NAF Derivation Mode: during the procedure for deriving Network Application Function (NAF) specific keys from previous bootstrapped key material.

The function is related to a particular USIM and shall not be executable unless the USIM application has been selected and activated, and the current directory is the USIM ADF or any subdirectory under this ADF and a successful PIN verification procedure has been performed (see clause 5).

7.1.1.x GBA security context (Bootstrapping Mode)

USIM operations in GBA security context are supported if service n°xx 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 [xx]). 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 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 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.

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

Input:

- RAND, AUTN

Output:

- RES

or

- AUTS

7.1.1.y GBA security context (NAF Derivation Mode)

USIM operations in GBA security context are supported if service n°xx 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 [xx] 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.

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

7.1.2 Command parameters and data

Code	Value
CLA	As specified in TS 31.101
INS	'88'
P1	'00'
P2	See table below
Lc	See below
Data	See below
Le	'00', or maximum length of data expected in response

Parameter P2 specifies the authentication context as follows:

Coding of the reference control P2

Coding b8-b1	Meaning
'1-------'	Specific reference data (e.g. DF specific/application dependant key)
'-----X-XX'	Authentication context: 000 GSM context 001 3G context 010 VGCS context 100 GBA context

All other codings are RFU.

Command parameters/data:

7.1.2.1 GSM/3G security context

Byte(s)	Description	Length
1	Length of RAND (L1)	1
2 to (L1+1)	RAND	L1
(L1+2)	Length of AUTN (L2) (see note)	1
(L1+3) to (L1+L2+2)	AUTN (see note)	L2
Note: Parameter present if and only if in 3G security context.		

The coding of AUTN is described in TS 33.102 [13]. The most significant bit of RAND is coded on bit 8 of byte 2. The most significant bit of AUTN is coded on bit 8 of byte (L1+3).

Response parameters/data, case 1, 3G security context, command successful:

Byte(s)	Description	Length
1	"Successful 3G authentication" tag = 'DB'	1
2	Length of RES (L3)	1
3 to (L3+2)	RES	L3
(L3+3)	Length of CK (L4)	1
(L3+4) to (L3+L4+3)	CK	L4
(L3+L4+4)	Length of IK (L5)	1
(L3+L4+5) to (L3+L4+L5+4)	IK	L5
(L3+L4+L5+5)	Length of K_C (= 8) (see note)	1
(L3+L4+L5+6 to (L3+L4+L5+13)	K_C (see note)	8
Note: Parameter present if and only if Service n°27 is "available".		

The most significant bit of RES is coded on bit 8 of byte 3. The most significant bit of CK is coded on bit 8 of byte (L3+4). The most significant bit of IK is coded on bit 8 of byte (L3+L4+5).

Response parameters/data, case 2, 3G security context, synchronisation failure:

Byte(s)	Description	Length
1	"Synchronisation failure" tag = 'DC'	1
2	Length of AUTS (L1)	1
3 to (L1+2)	AUTS	L1

The coding of AUTS is described in TS 33.102 [13]. The most significant bit of AUTS is coded on bit 8 of byte 3.

Response parameters/data, case 3, GSM security context, command successful:

Byte(s)	Description	Length
1	Length of SRES (= 4)	1
2 to 5	SRES	4
6	Length of K_C (= 8)	1
7 to 14	K_C	8

The most significant bit of SRES is coded on bit 8 of byte 2. The most significant bit of Kc is coded on bit 8 of byte 7.

7.1.2.2 VGCS security context

Byte(s)	Description	Length
1	Length of VGCS_ID (L1)	1
2 to (L1+1)	VGCS_ID	L1
(L1+2)	Length of VK_ID (L2)	1
(L1+3) to (L1+L2+2)	VK_ID	L2
(L1+L2+3)	Length of VSTK_RAND	1
(L1+L2+4) to (L1+L2+7)	VSTK_RAND	4

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

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

7.1.2.x GBA security context (Bootstrapping Mode)

Byte(s)	Description	Length
1	“GBA Security Context Bootstrapping Mode” tag = ‘DD’	1
2	Length of RAND (L1)	1
3 to (L1+2)	RAND	L1
(L1+3)	Length of AUTN (L2)	1
(L1+4) to (L1+L2+3)	AUTN	L2

Response parameters/data, GBA security context (Bootstrapping Mode), synchronisation failure:

Byte(s)	Description	Length
1	"Synchronisation failure" tag = 'DC'	1
2	Length of AUTS (L1)	1
3 to (L1+2)	AUTS	L1

AUTS coded as for UMTS Security context.

Response parameters/data, GBA security context (Bootstrapping Mode), command successful:

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

RES coded as for UMTS Security context.

7.1.2.y GBA security context (NAF Derivation Mode)

Byte(s)	Description	Length
1	“GBA Security Context NAF Derivation Mode” tag = ‘DE’	1
2	Length of NAF_ID (L1)	1
3 to (L1+2)	NAF_ID	L1
(L1+3)	Length of IMPI (L2)	1
(L1+4) to (L1+L2+3)	IMPI	L2

Response parameters/data, GBA security context (NAF Derivation Mode), command successful:

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

Coding of Ks_ext_NAF as described in TS 33.220 [xx].

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 SSID List	No
'4F45'	Operator controlled SSID List	Caution
'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

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
'6FXX'	GBA Bootstrapping parameters	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 SSID list	'00FF…FF'
'4F45'	Operator controlled SSID list	Operator dependant
'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'
'6FXX'	GBA Bootstrapping parameters	'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 #32
New York, USA, 10-13 August 2004,

Tdoc ⌘ T3-040545

CR-Form-v7

CHANGE REQUEST

⌘ **31.102** **CR** 238 ⌘ **rev** **-** ⌘ Current version: **6.6.0** ⌘

*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 WLAN fast re-authentication information
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	06/07/2004
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:

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

Reason for change:	⌘	As requested by CN1 in their LS to T3 (T3-040427) the USIM shall support the storage of all temporary identities for EAP authentication, including re-authentication identity and associated security parameters. In addition, 3GPP TS 24.234 mandates in §6.1.1 the storage of re-authentication information (i.e. re-authentication identity, Master Key and Counter value) on the USIM.There are also clear SA1 service requirements (S1-040257) and SA3 recommendations (S3-040019) on that.
Summary of change:	⌘	The following changes are included: - Addition of EF_{RI} (Reauthentication Identity) under DF_{WLAN} - Addition of related procedures
Consequences if not approved:	⌘	Lack of description of needed parameters and features in the USIM related to WLAN fast re-authentication procedure

Clauses affected:	⌘	4.2.8, 4.4.5, 4.4.5.x (new), 4.7, 5.6.x (new), Annex A, Annex E			
Other specs affected:	⌘	**Y**	**N**		
		[ ]	[ ]	Other core specifications	⌘
		[ ]	[ ]	Test specifications	
		[ ]	[ ]	O&M Specifications	
Other comments:	⌘				

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

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

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

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

4.2.8 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 SSID list
	Service n°63	Operator controlled SSID list
	Service n°64	VGCS security
	Service n°xx	WLAN Reauthentication Identity

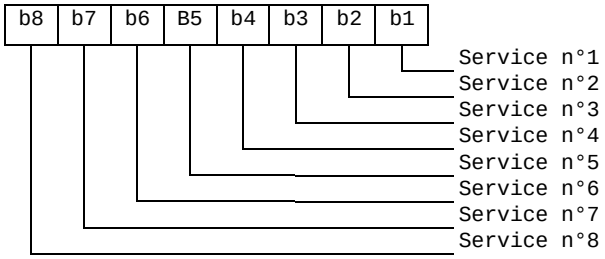
The EF shall contain at least one byte. Further bytes may be included, but if the EF includes an optional byte, then it is mandatory for the EF to also contain all bytes before that byte. Other services are possible in the future and will be coded on further bytes in the EF. The coding falls under the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

Coding:

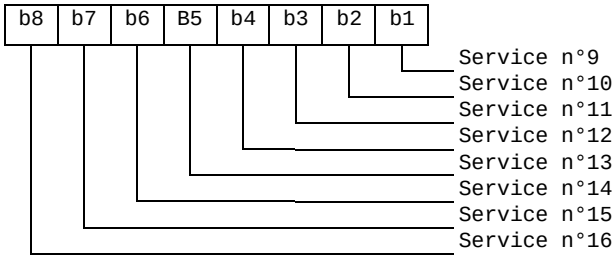
1 bit is used to code each service:
bit = 1: service available;
bit = 0: service not available.

- 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.

4.4.5 Contents of files at the DF WLAN level

This clause describes the additional files that are used for WLAN purposes.

DF_{WLAN} shall be present at the ADF_{USIM} level if either of the services nº59, nº60, nº61, nº62, ~~or~~ nº63 or nºxx are allocated in the corresponding EF_{UST} (USIM Service Table).

4.4.5.x EF_{RWRI} (WLAN Reauthentication Identity)

This EF contains a list of parameters linked to a re-authentication identity to be used in fast re-authentication. Re-authentication identities and related parameters (Master Key and Counter Value) are provided as part of a previous authentication sequence. This file shall be present if service n°xx is allocated in EF_{UST}.

Identifier: '4FXX'	Structure: Transparent	Optional
SFI: 'XX'		
File size: n bytes (n≥J+K+L+6)	Update activity: high	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1	Reauthentication Identity Tag '80'	M	1 byte
2	Re-authentication Identity Length	M	1 byte
3-J+2	Re-authentication Identity Value	M	J bytes
J+3	Master Key Tag '81'	M	1 byte
J+4	Master Key Length	M	1 byte
J+5-J+K+4	Master Key Value	M	K bytes
J+K+5	Counter Tag '82'	M	1 byte
J+K+6	Counter Length	M	1 byte
J+K+7-J+K+L+6	Counter Value	M	L bytes

- Reauthentication Identity

  Contents:
  - Re-authentication identity TLV to be used as the username part of the NAI.

  Coding:

  Tag '80'
  Unsigned length on 1 byte
  Value: As described for the user portion of the NAI in TS 33.234 [41]. Unused bytes shall be set to 'FF' and shall not be considered as a part of the value.

- Master Key

  Contents:
  - Master Key TLV.

  Coding:

  Tag '81'
  Unsigned length on 1 byte
  Value: As described in TS 33.234 [41].

- Counter

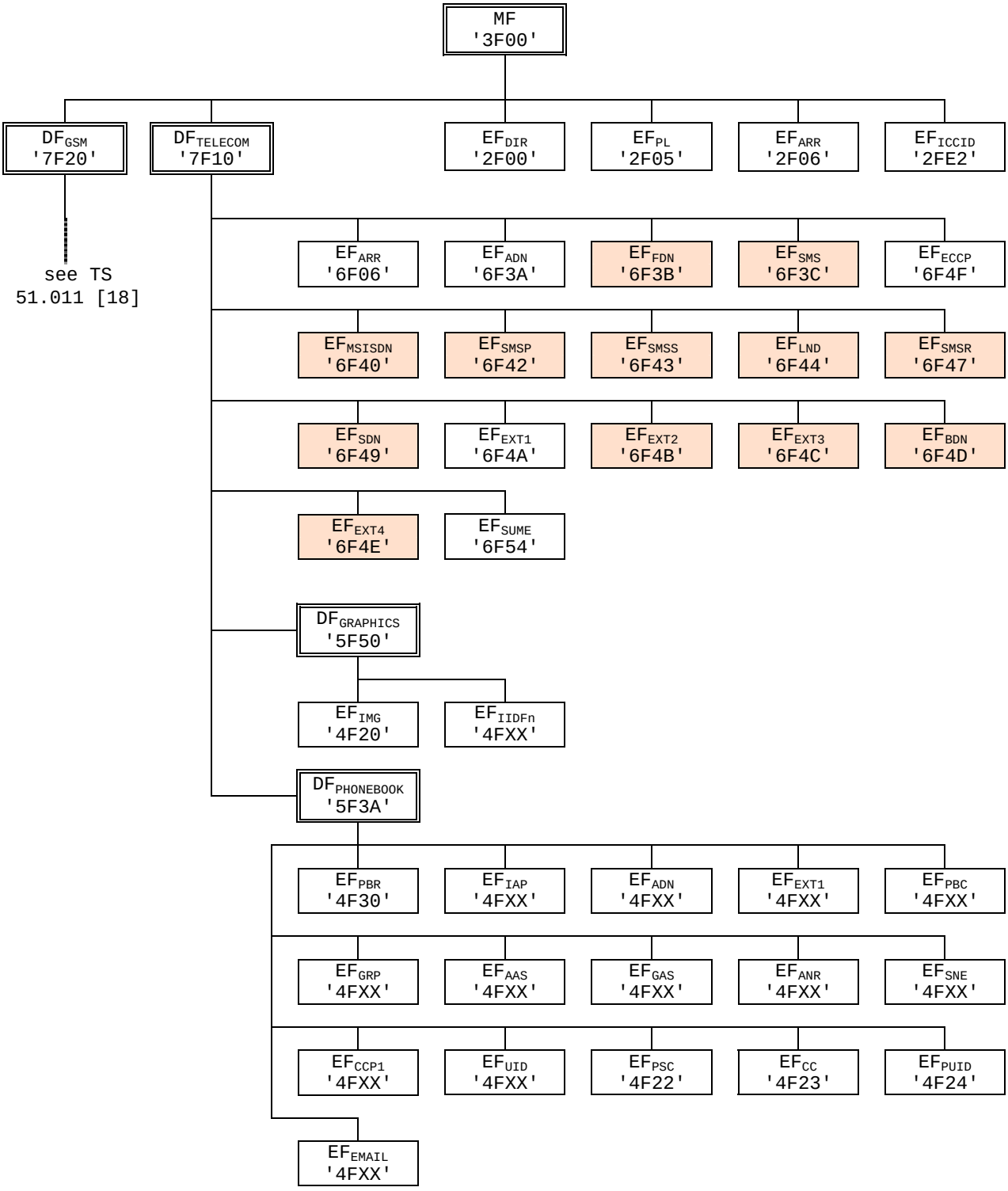
  Contents:
  - Counter TLV

  Coding:

  Tag '82'
  Unsigned length on 1 byte
  Value: As described in TS 33.234 [41].

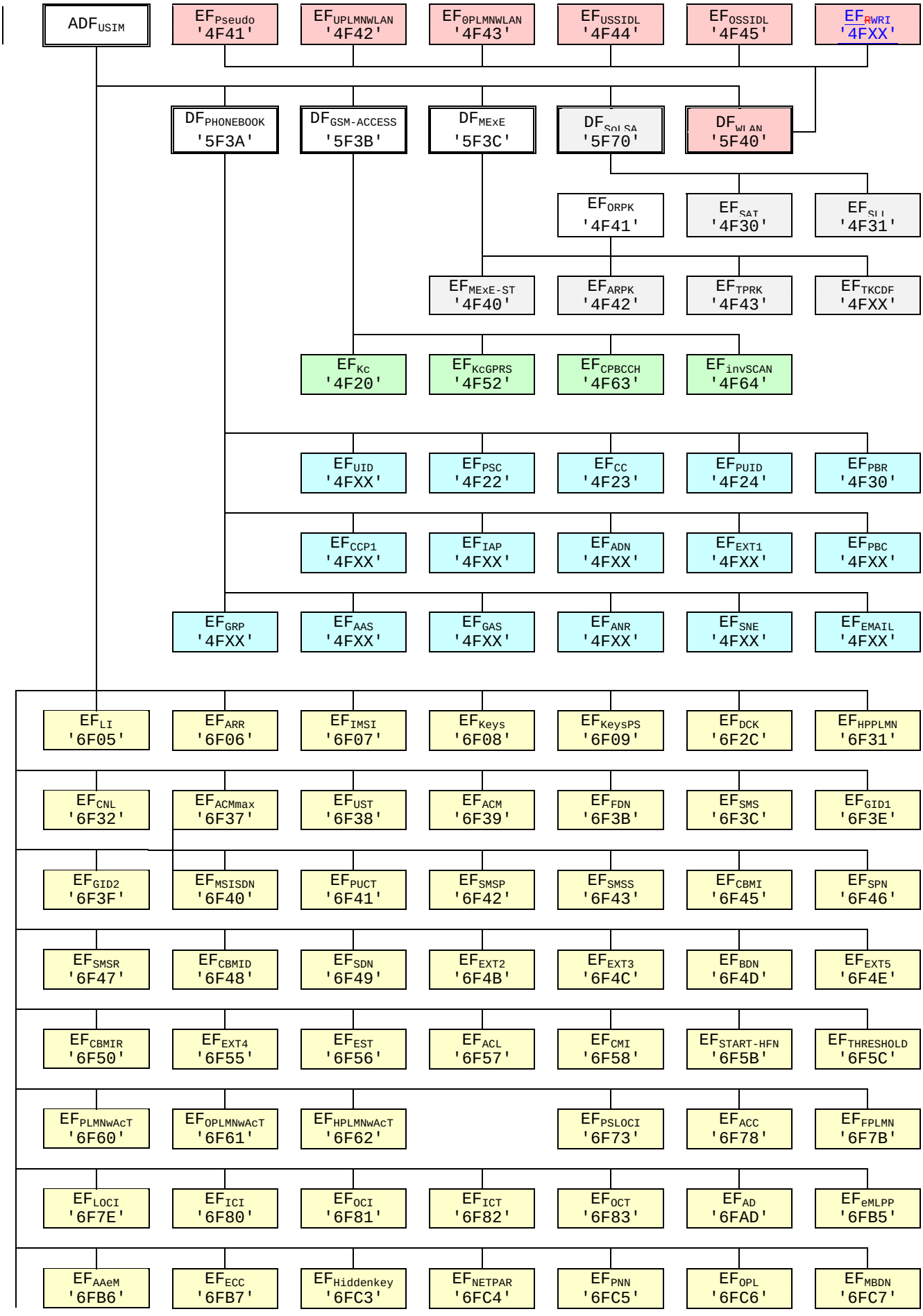
4.7 Files of USIM

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 RWRI '4FXX'
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 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'

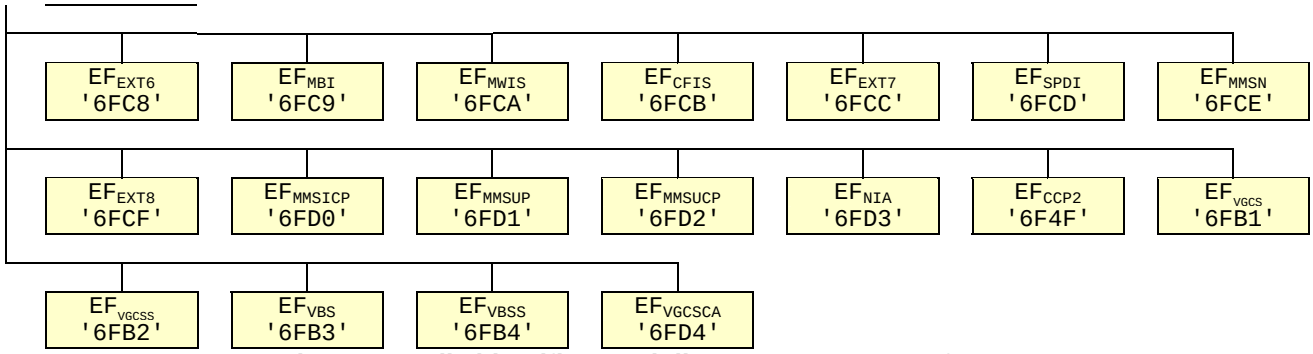


Figure 4.2: File identifiers and directory structures of USIM

5.6.x WLAN access re-authentication related procedures

Requirement: service n°xx "available"

When the ME tries a fast re-authentication, it shall inspect if a valid reauthentication identity is available in EF_{RWRI} and use it as the user name portion of the NAI for WLAN access re-authentication following the procedures described in TS 24.234 [40].

The ME shall manage re-authentiction identities, Master Key and counter values as described in TS 24.234 [40].

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 SSID List	No
'4F45'	Operator controlled SSID List	Caution
'4FXX'	WLAN Reauthentication Identity	No
'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

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
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 SSID list	'00FF…FF'
'4F45'	Operator controlled SSID list	Operator dependant
'4FXX'	WLAN Reauthentication Identity	'~~00~~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'

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#32
New York, USA, 10-13 August 2004

Tdoc ⌘ T3-040572

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.102** **CR** 239 ⌘ **rev** **-** ⌘ Current version: **6.6.0** ⌘

*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
Source:	⌘	T3
Work item code:	⌘	MBMS
Date:	⌘	19/07/2004
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:	⌘	As defined in TS 33.246, Multicast Broadcast Multimedia Services (MBMS) security requires the definition of some procedures in the USIM-ME interface. These procedures apply for MBMS key management for the storage and transport of the MBMS Service Key (MSK) and for the generation and validation of MBMS Traffic Key (MTK) in the UICC
Summary of change:	⌘	The following changes are included: -New Service in UST for MBMS security -Storage of MBMS Key Group Ids and associatd MSKs parameters. -Storage of MBMS user Key Ids and associated parameter -New MBMS security context in AUTHENTICATE command with three specific modes: MSK Update, MSK Verification and MTK Generation
Consequences if not approved:	⌘	Required MBMS functionalities will not be supported.

Clauses affected:	⌘	2, 4.2.8, 4.2.x (new), 4.2.y (new), 7.1, 7.3.1, Annex A, Annex E

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

Other comments:	⌘	Condtionally approved subject to 33.246 being approved.

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: "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] ETSI TS 102 221 "Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 4)"

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

[39] ETSI TS 102 222 "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"

[xx] 3GPP TS 33.246: "Security of Multimedia Broadcast/Multicast Service (Release 6) "

**********NEXT CHANGE**********

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	3rd Generation Partnership Project
AC	Access Condition
ACL	APN Control List
ADF	Application Dedicated File
AID	Application IDentifier
AK	Anonymity key
ALW	ALWays
AMF	Authentication Management Field
AoC	Advice of Charge
APN	Access Point Name
ASN.1	Abstract Syntax Notation One
AuC	Authentication Centre
AUTN	Authentication token
BDN	Barred Dialling Number

BER-TLV	Basic Encoding Rule - TLV
CCP	Capability Configuration Parameter
CK	Cipher key
CLI	Calling Line Identifier
CNL	Co-operative Network List
CPBCCH	COMPACT Packet BCCH
CS	Circuit switched
DCK	Depersonalisation Control Keys
DF	Dedicated File
DO	Data Object
EF	Elementary File
FCP	File Control Parameters
FFS	For Further Study
GSM	Global System for Mobile communications
HE	Home Environment
ICC	Integrated Circuit Card
ICI	Incoming Call Information
ICT	Incoming Call Timer
ID	IDentifier
IEI	Information Element Identifier
IK	Integrity key
IMSI	International Mobile Subscriber Identity
K	USIM Individual key
K_C	Cryptographic key used by the cipher A5
KSI	Key Set Identifier
LI	Language Indication
LSB	Least Significant Bit
MAC	Message authentication code
MAC-A	MAC used for authentication and key agreement
MAC-I	MAC used for data integrity of signalling messages
MBMS	Multimedia Broadcast/Multicast Service
MCC	Mobile Country Code
MExE	Mobile Execution Environment
MF	Master File
MGV-F	MTK Generation and Validation Function
MIKEY	Multimedia Internet KEYing
MMI	Man Machine Interface
MNC	Mobile Network Code
MODE	Indication packet switched/circuit switched mode
MSB	Most Significant Bit
MSK	MBMS Service Key
MTK	MBMS Traffic Key
MUK	MBMS User Key
NEV	NEVer
NPI	Numbering Plan Identifier
OCI	Outgoing Call Information
OCT	Outgoing Call Timer
PBID	Phonebook Identifier
PIN	Personal Identification Number
PL	Preferred Languages
PS	Packet switched
PS_DO	PIN Status Data Object
RAND	Random challenge
$RAND_{MS}$	Random challenge stored in the USIM
RES	User response
RFU	Reserved for Future Use
RST	Reset
SDN	Service dialling number
SE	Security Environment
SEQs	Sequence number for MGV-F
SEQp	Sequence number for MGV-F stored in the USIM
SFI	Short EF Identifier

SGSN	Serving GPRS Support Node
SN	Serving Network
SQN	Sequence number
SRES	Signed RESponse calculated by a USIM
SW	Status Word
TLV	Tag Length Value
USAT	USIM Application Toolkit
USIM	Universal Subscriber Identity Module
VLR	Visitor Location Register
XRES	Expected user RESponse

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 SSID list
	Service n°63	Operator controlled SSID list
	Service n°64	VGCS security
	Service n°xx	MBMS security

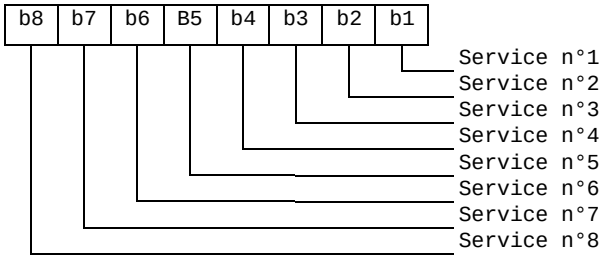
The EF shall contain at least one byte. Further bytes may be included, but if the EF includes an optional byte, then it is mandatory for the EF to also contain all bytes before that byte. Other services are possible in the future and will be coded on further bytes in the EF. The coding falls under the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

Coding:

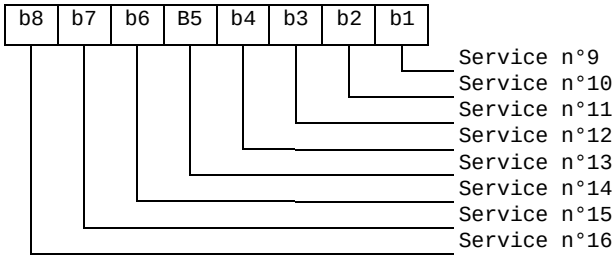
1 bit is used to code each service:
bit = 1: service available;
bit = 0: service not available.

- 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 CHANGE**********

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

4.2.x EF_{MSK} (MBMS Service Keys List)

This EF contains the list of MBMS Service Keys (MSK) and associated parameters, which are related to an MBMS Key Group. There are up to two MSKs per Network Id/Key Group ID pair. This file shall be present if the MBMS security service (service number xx) is allocated in EF_{UST} (USIM Service Table).

Identifier: '6FXX'	Structure: linear fixed	Optional
Record length: 17 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 3	Network ID	M	3 bytes
4 to 5	Key Group ID	M	2 bytes
6 to 7	1st MSK ID	M	2 bytes
8 to 11	1st Time Stamp Counter (TS)	M	4 bytes
12 to 13	2nd MSK ID	M	2 bytes
14 to 17	2nd Time Stamp Counter (TS)	M	4 bytes

- Network ID:
  Content: Identifier of the Network of the BMSC providing MBMS Service
  Coding: As defined in TS 33.246 [xx]

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

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

- 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 [xx]

4.2.y 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 xx) is allocated in EF_{UST} (USIM Service Table).

Identifier: '6FXX'	Structure: transparent	Optional
File length: Q+6 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Length of MUK ID (Q)	M	1 byte
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 [xx]

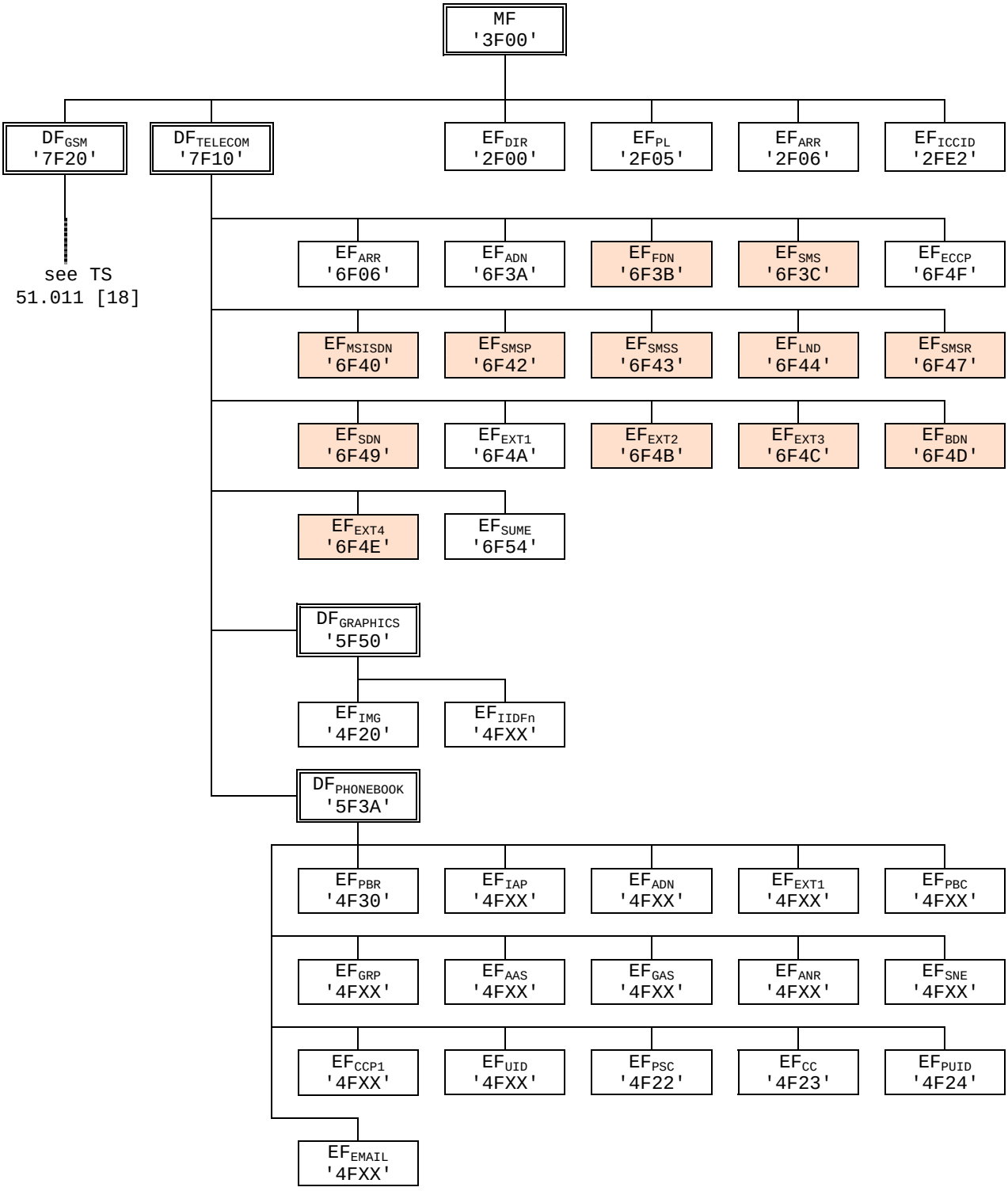
- Length of Time Stamp Counter (TS)
  Contents: number of bytes (=4), not including this length byte, of Time Stamp Counter (TS)field

- 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 [xx]

**********NEXT CHANGE**********

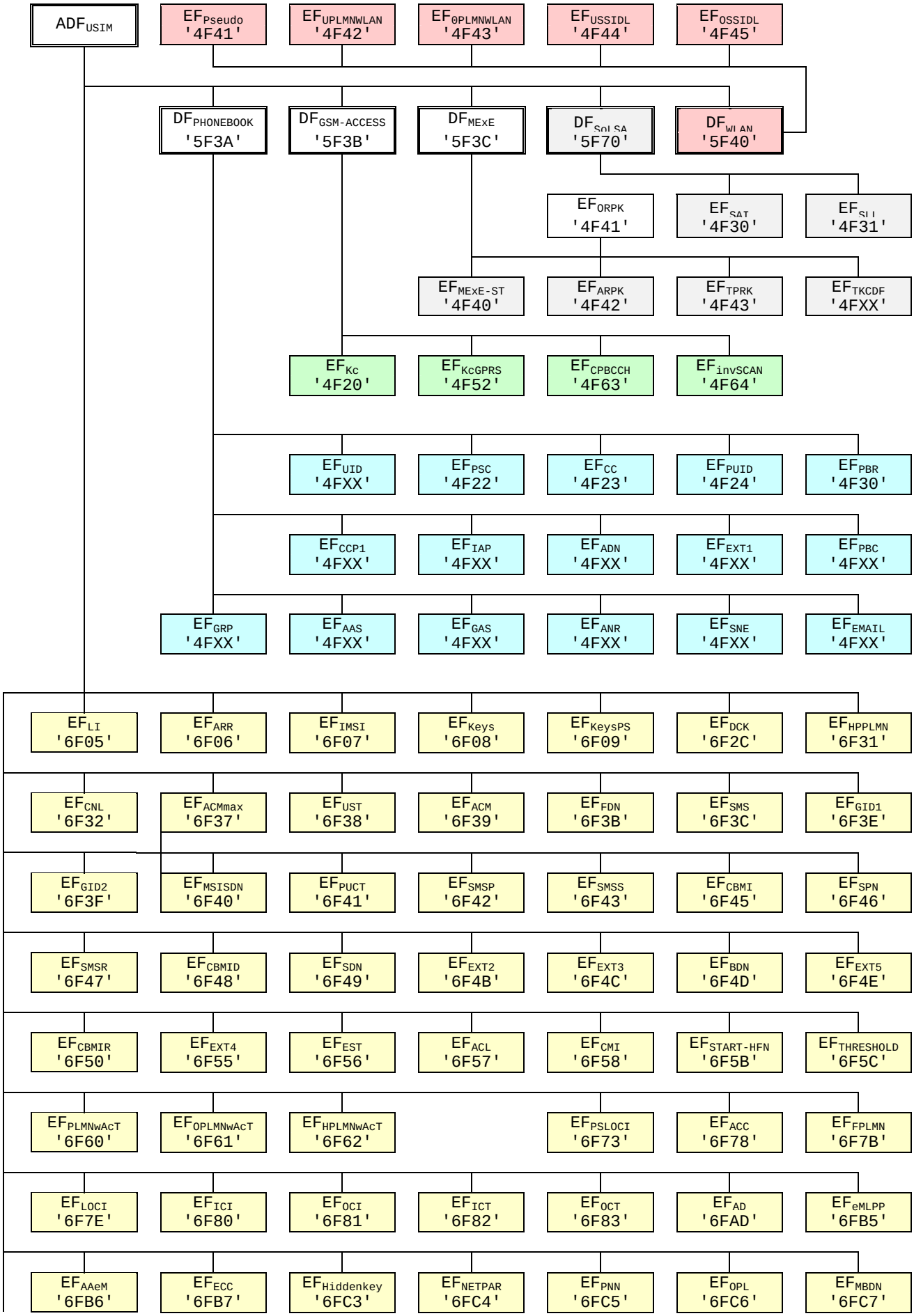
4.7 Files of USIM

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'
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 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'

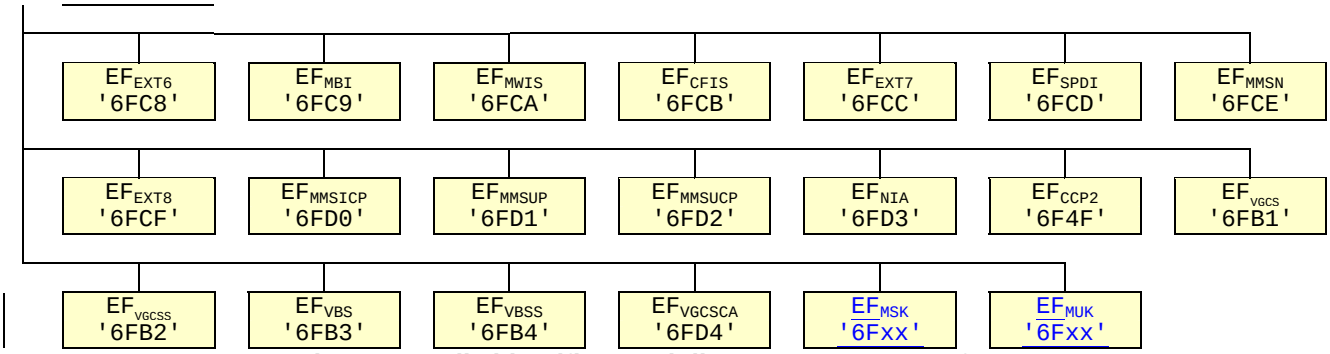


Figure 4.2: File identifiers and directory structures of USIM

**********NEXT CHANGE**********

5.2 USIM security related procedures

5.2.x MSK MIKEY Message Reception

The ME performs the reading of EF_{MUK} and retrieves the Time Stamp Counter Value associated with the involved MUK. Then it proceeds with Timestamp Payload checking as described in TS 33.246 [xx].

5.2.y MTK MIKEY Message Reception

The ME performs the reading of EF_{MSK} and retrieves the Time Stamp Counter Value associated with the involved MSK. Then it proceeds with Timestamp Payload checking as described in TS 33.246 [xx].

7.1 AUTHENTICATE

7.1.1 Command description

The function can be used in several different contexts:

- a 3G security context, when 3G authentication vectors (RAND, XRES, CK, IK, AUTN) are available (i.e. the UE is located in the UTRAN, or in a GSM radio access network which is connected to a 3G or 3G capable VLR/SGSN), or
- a GSM security context, when GSM authentication data are available only (i.e. the UE is located in the GSM radio access network which is connected to a non-3G capable VLR/SGSN).
- an VGCS security context, when VGCS authentication data is available
- a MBMS security context, when a MBMS security procedure is requested

The function is used in GSM or 3G security context during the procedure for authenticating the USIM to its HE and vice versa. In addition, a cipher key and an integrity key are calculated. For the execution of the command the USIM uses the subscriber authentication key K, which is stored in the USIM.

The function is used in VGCS security context during the procedure for retrieving the VGCS Short Term Key (VSTK) used by the terminal to in establishing VGCS calls.

The function is used in MBMS security context in three different modes:

a) MSK Update Mode: during the procedure for updating an MBMS Service Key (MSK).

b) MSK Verification Mode: during the procedure for computing the MSK Verification Message previously requested by an MSK update message.

c) MTK Generation Mode: during the procedure for retrieving the MBMS Traffic Key (MTK) used by the terminal to decrypt MBMS data.

The function is related to a particular USIM and shall not be executable unless the USIM application has been selected and activated, and the current directory is the USIM ADF or any subdirectory under this ADF and a successful PIN verification procedure has been performed (see clause 5).

**********NEXT CHANGE**********

7.1.1.x MBMS security context (MSK Update Mode)

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

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

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, 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 [xx].

After successful MSK Update procedure the USIM 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 [xx]) 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, Key Group ID already exists (without the same MSK_ID) and both MSK keys are present, the 1st MSK (and associated parameters) shall be replaced by the 2nd MSK, which is itself replaced by the new one.

-If a record with the given Network ID, Key Group ID does not exist, the USIM uses an empty record to include Network ID and Key Group ID values and then proceeds as in the second of the three previous cases.

Note: The policy of replacing Key Groups records when no more empty records are available in EF_{MSK} is HE specific. (e.g. delete Groups from visited Network Ids 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 fields under EF_{MUK}

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.y MBMS security context (MSK Verification Mode)

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

The USIM receives the NAF_ID and MIKEY packet containing an MIKEY verification message.

First, the USIM tests if the given NAF_ID corresponds to the 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 [xx] and sends back the complete MIKEY verification message.

Input:

- NAF_ID, MIKEY message

Output:

- MIKEY message

7.1.1.z MBMS security context (MTK Generation Mode)

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

The USIM receives the MIKEY message containing an MBMS MTK. First, the USIM retrieves the MSK identified by the Network ID, Key Group ID and MSK ID enclosed in the MIKEY message (as described in TS 33.246 [xx]).

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 [xx] 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 '98xx' (Authentication error, key freshness failure) is returned.

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.

Input:

- MIKEY message

Output:

- MTK

7.1.2 Command parameters and data

Code	Value
CLA	As specified in TS 31.101
INS	'88'
P1	'00'
P2	See table below
Lc	See below
Data	See below
Le	'00', or maximum length of data expected in response

Parameter P2 specifies the authentication context as follows:

Coding of the reference control P2

Coding b8-b1	Meaning
'1-------'	Specific reference data (e.g. DF specific/application dependant key)
'-----X-XX'	Authentication context: 000 GSM context 001 3G context 010 VGCS context 101 MBMS context

All other codings are RFU.

Command parameters/data:

7.1.2.1 GSM/3G security context

Byte(s)	Description	Length
1	Length of RAND (L1)	1
2 to (L1+1)	RAND	L1
(L1+2)	Length of AUTN (L2) (see note)	1
(L1+3) to (L1+L2+2)	AUTN (see note)	L2
Note: Parameter present if and only if in 3G security context.		

The coding of AUTN is described in TS 33.102 [13]. The most significant bit of RAND is coded on bit 8 of byte 2. The most significant bit of AUTN is coded on bit 8 of byte (L1+3).

Response parameters/data, case 1, 3G security context, command successful:

Byte(s)	Description	Length
1	"Successful 3G authentication" tag = 'DB'	1
2	Length of RES (L3)	1
3 to (L3+2)	RES	L3
(L3+3)	Length of CK (L4)	1
(L3+4) to (L3+L4+3)	CK	L4
(L3+L4+4)	Length of IK (L5)	1
(L3+L4+5) to (L3+L4+L5+4)	IK	L5
(L3+L4+L5+5)	Length of K_C (= 8) (see note)	1
(L3+L4+L5+6 to (L3+L4+L5+13)	K_C (see note)	8
Note: Parameter present if and only if Service n°27 is "available".		

The most significant bit of RES is coded on bit 8 of byte 3. The most significant bit of CK is coded on bit 8 of byte (L3+4). The most significant bit of IK is coded on bit 8 of byte (L3+L4+5).

Response parameters/data, case 2, 3G security context, synchronisation failure:

Byte(s)	Description	Length
1	"Synchronisation failure" tag = 'DC'	1
2	Length of AUTS (L1)	1
3 to (L1+2)	AUTS	L1

The coding of AUTS is described in TS 33.102 [13]. The most significant bit of AUTS is coded on bit 8 of byte 3.

Response parameters/data, case 3, GSM security context, command successful:

Byte(s)	Description	Length
1	Length of SRES (= 4)	1
2 to 5	SRES	4
6	Length of K_C (= 8)	1
7 to 14	K_C	8

The most significant bit of SRES is coded on bit 8 of byte 2. The most significant bit of Kc is coded on bit 8 of byte 7.

7.1.2.2 VGCS security context

Byte(s)	Description	Length
1	Length of VGCS_ID (L1)	1
2 to (L1+1)	VGCS_ID	L1
(L1+2)	Length of VK_ID (L2)	1
(L1+3) to (L1+L2+2)	VK_ID	L2
(L1+L2+3)	Length of VSTK_RAND	1
(L1+L2+4) to (L1+L2+7)	VSTK_RAND	4

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

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

7.1.2.2 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 (L)	1
3 to (L+2)	MTK	L

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

7.2 Void

7.3 Status Conditions Returned by the USIM

Status of the card after processing of the command is coded in the status bytes SW1 and SW2. This clause specifies the coding of the status bytes in the following tables, in addition to the ones defined in TS 31.101 [11].

7.3.1 Security management

SW1	SW2	Error description
'98'	'62'	- Authentication error, incorrect MAC
'98'	'64	- Authentication error, security context not supported
'98'	'xx'	- Authentication error, key freshness failure

7.3.2 Status Words of the Commands

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

Commands and status words

Status Words	AUTHENTICATE
90 00	*
91 XX	*
93 00	
98 50	
98 62	*
98 64	*
98 xx	*
62 00	*
62 81	
62 82	
62 83	
63 CX	
64 00	*
65 00	*
65 81	*
67 00	*
67 XX – (see note)	*
68 00	*
68 81	*
68 82	*
69 81	
69 82	*
69 83	
69 84	*
69 85	*
69 86	
6A 80	
6A 81	*
6A 82	
6A 83	
6A 86	*
6A 87	
6A 88	*
6B 00	*
6E 00	*
6F 00	*
6F XX – (see note)	*
NOTE: Except SW2 = '00'.	

**********NEXT CHANGE**********

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 SSID List	No
'4F45'	Operator controlled SSID List	Caution
'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

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
'6FXX'	MBMS Service Keys List	Caution
'6FXX'	MBMS User Key	Caution

NOTE1: If EF_{IMSI} is changed, the UICC should issue REFRESH as defined in TS 31.111 and update

File identification	Description	Change advised
	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 SSID list	'00FF…FF'
'4F45'	Operator controlled SSID list	Operator dependant
'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'
'6FXX'	MBMS Service Keys List	'FF…FF'
'6FXX'	MBMS User Key	'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 T WG3 Meeting #32
New-York, NY, USA, 10th – 13th August 2004

Tdoc T3-040584

CR-Form-v7

CHANGE REQUEST

⌘ **31.102** **CR** **240** ⌘ **rev** **-** ⌘ Current version: **5.9.0** ⌘

*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 a wrong reference to TS 102 221
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	12/08/2004
Category:	⌘	**F**
Release:	⌘	Rel-5

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

Use one of the following releases:

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

Reason for change:	⌘	In 31.102, there is an explicit reference to the Release 4 of the UICC platform specification (ETSI SCP TS 102 221). This is a serious mistake because the USIM might need to use features available only in Release 5 and further versions of the UICC
Summary of change:	⌘	Deleted the version in the reference to SCP TS 102 221
Consequences if not approved:	⌘	Wrong implementations of UICC and MEs.

Clauses affected:	⌘	2			
Other specs affected:	⌘	**Y**	**N**		
			X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘	Similar change needed for Rel-6: clause 8 is added for information			

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] Void.

[18] 3GPP TS 51.011: "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] ITU-T Recommendation T.50: "International Alphabet No. 5 Information technology - 7-bit coded character set for information interchange").

[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] ETSI TS 102 221 "Smart cards; UICC-Terminal interface; Physical and logical characteristics ~~(Release 4)~~"

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

[39] 3GPP TS 23.073: "Support of Localised Service Area (SoLSA); Stage 2".

8 UICC Characteristics

The UICC characteristics are defined in TS 31.101 [11]. As TS 31.101 [11] refers to TS 102 221 [37] for the details of the characteristics, and because the scope of TS 102 221 [37] also encompasses other mobile systems, it is necessary to list those issues which are not applicable to the USIM application, which deviate from TS 102 221 [37] or options which require further precision. This clause contains such information.

3GPP TSG T WG3 Meeting #32
New-York, NY, USA, 10th – 13th August 2004

Tdoc T3-040585

CR-Form-v7

CHANGE REQUEST

⌘ **31.102** **CR** **241** ⌘ **rev** **-** ⌘ Current version: **5.9.0** ⌘

*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:	⌘	Removal of a wrong reference to 102 221
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	12/08/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

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

Use one of the following releases:

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

Reason for change:	⌘	In 31.102, there is an explicit reference to the Release 4 of the UICC platform specification (ETSI SCP TS 102 221). This is a serious mistake because: - in Rel-6 the USIM might need to take benefit of Rel-6 features of the UICC - the 3GPP UICC platform is defined by 3GPP TS 31.101 which contains deltas to the SCP specification that need to be taken into account by any 3GPP application. Anyway TS 102 221 is not referred to from anywhere else in 31.102.
Summary of change:	⌘	Deletion of the reference to SCP TS 102 221. An additional & non-related editorial mistake is corrected in section 5.1.8
Consequences if not approved:	⌘	Wrong implementations of UICC and MEs.

Clauses affected:	⌘	2, 5.1.8

		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] Void.

[18] 3GPP TS 51.011: "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] ITU-T Recommendation T.50: "International Alphabet No. 5 Information technology - 7-bit coded character set for information interchange").

[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 ~~ETSI TS 102 221 "Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 4)"~~

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

[39] 3GPP TS 23.073: "Support of Localised Service Area (SoLSA); Stage 2".

5.1.7 USIM service table request

The ME performs the reading procedure with EF_{UST}.

5.1.8 VoidSpare

5.1.9 UICC presence detection

The ME checks for the presence of the UICC according to TS 31.101 [11] within all 30 s periods of inactivity on the UICC-ME interface during a call. If the presence detection according to TS 31.101 [11] fails the call shall be terminated as soon as possible but at least within 5s after the presence detection has failed. Here a call covers a circuit switched call, and/or an active PDP context.

3GPP TSG-T3 Meeting #32
Ney York, USA, 10-13 August 2004,

Tdoc ⌘ T3-040591

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.102** **CR** **233** ⌘ **rev** **1** ⌘ Current version: **6.6.0** ⌘

*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
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	11/08/2004
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:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	A new VGCS/VBS ciphering feature was introduced into rel-6 (TS 43.020). But only VGCS key derivation is currently supported in the TS 31.102. Therefore we need to encompass VBS security (T3-040438). Lack of description of needed parameters and features in the USIM related to VGCS/VBS support
Summary of change:	⌘	The following changes are included: - Including EF_{VBSCA} (Voice Broadcast Service Ciphering Algorithm) to store algorithm identifiers. - Extending the definition of the VGCS security context in AUTHENTICATE command to support VBS - Addition of a new field in EF_{VGCSCA} to assign a ciphering algorithm identifier for each group key (T3-040438)
Consequences if not approved:	⌘	Required functionalities will note be supported.

Clauses affected:	⌘	2, 4.2.8, 4.2.77, 4.2.y (new), 4.7, 7.1, Annex A, Annex E

Other specs affected: ⌘	Y	N		⌘
		X	Other core specifications	
			Test specifications	
			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: "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] ETSI TS 102 221 "Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 4)"

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

[39] ETSI TS 102 222 "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"

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

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 SSID list
	Service n°63	Operator controlled SSID list
	Service n°64	VGCS security
	Service n°xx	VBS security

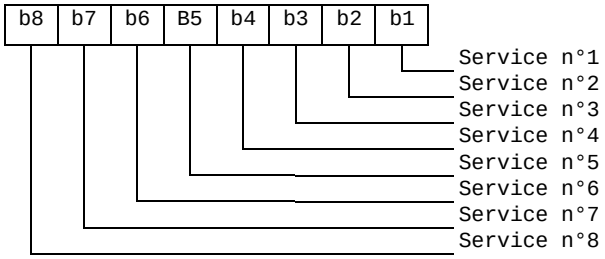
The EF shall contain at least one byte. Further bytes may be included, but if the EF includes an optional byte, then it is mandatory for the EF to also contain all bytes before that byte. Other services are possible in the future and will be coded on further bytes in the EF. The coding falls under the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

Coding:

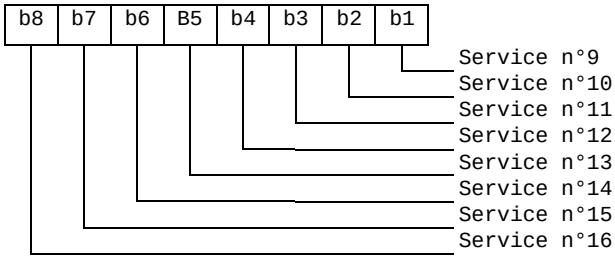
1 bit is used to code each service:
bit = 1: service available;
bit = 0: service not available.

- 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.

4.2.77 EF_{VGCSCA} (Voice Group Call Service Ciphering Algorithm)

This EF contains the ciphering algorithm identifiers for each of the Master Group Key (V_Ki) of each VGCS groups that the user has subscribed to (defined in EF_{VGCS}). This EF shall always be allocated if EF_{VGCS} is allocated.

If service n°64 is "available", this file shall be present.

Identifier: '6FD4'	Structure: transparent	Optional
File size: 2n bytes (n <= 50)	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	VGCS Group ciphering algorithm identifier for 1st V_Ki of Group 1	M	1 byte
2	VGCS Group ciphering algorithm identifier for 2nd V_Ki of Group 1	M	1 byte
32	VGCS Group ciphering algorithm identifier for 1st V_Ki of Group 2	O	1 byte
4	VGCS Group ciphering algorithm identifier for 2nd V_Ki of Group 2	O	1 byte
:	:	:	:
2n-1	VGCS Group ciphering algorithm identifier for 1st V_Ki of Group n	O	1 byte
2n	VGCS Group ciphering algorithm identifier for 2nd V_Ki of Group n	O	1 byte

- Ciphering Algorithm Identifier:

Contents: Ciphering Algorithm identifier for the specified Master Group Key of each Voice Call Group

Coding:

Value

'00' no ciphering
'01' ciphering with algorithm GSM A5/1
'02' ciphering with algorithm GSM A5/2
'03' ciphering with algorithm GSM A5/3
'04' ciphering with algorithm GSM A5/4
'05' ciphering with algorithm GSM A5/5
'06' ciphering with algorithm GSM A5/6
'07' ciphering with algorithm GSM A5/7
'08' to 'FF' RFU

4.2.y EF_{VBSCA} (Voice Broadcast Service Ciphering Algorithm)

This EF contains the ciphering algorithm identifiers for each of the Master Group Key (V_Ki) of each VBS group that the user has subscribed to (defined in EF_{VBS}).

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

Identifier: '6FXX'	Structure: transparent	Optional
File size: 2n bytes (n <= 50)	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	VBS Group ciphering algorithm identifier for 1st V_Ki of Group 1	M	1 byte
2	VBS Group ciphering algorithm identifier for 2nd V_Ki of Group 1	M	1 byte
3	VBS Group ciphering algorithm identifier for 1st V_Ki of Group 2	O	1 byte
4	VBS Group ciphering algorithm identifier for 2nd V_Ki of Group 2	O	1 byte
:	:	:	:
2n-1	VBS Group ciphering algorithm identifier for 1st V_Ki of Group n	O	1 byte
2n	VBS Group ciphering algorithm identifier for 2nd V_Ki of Group n	O	1 byte

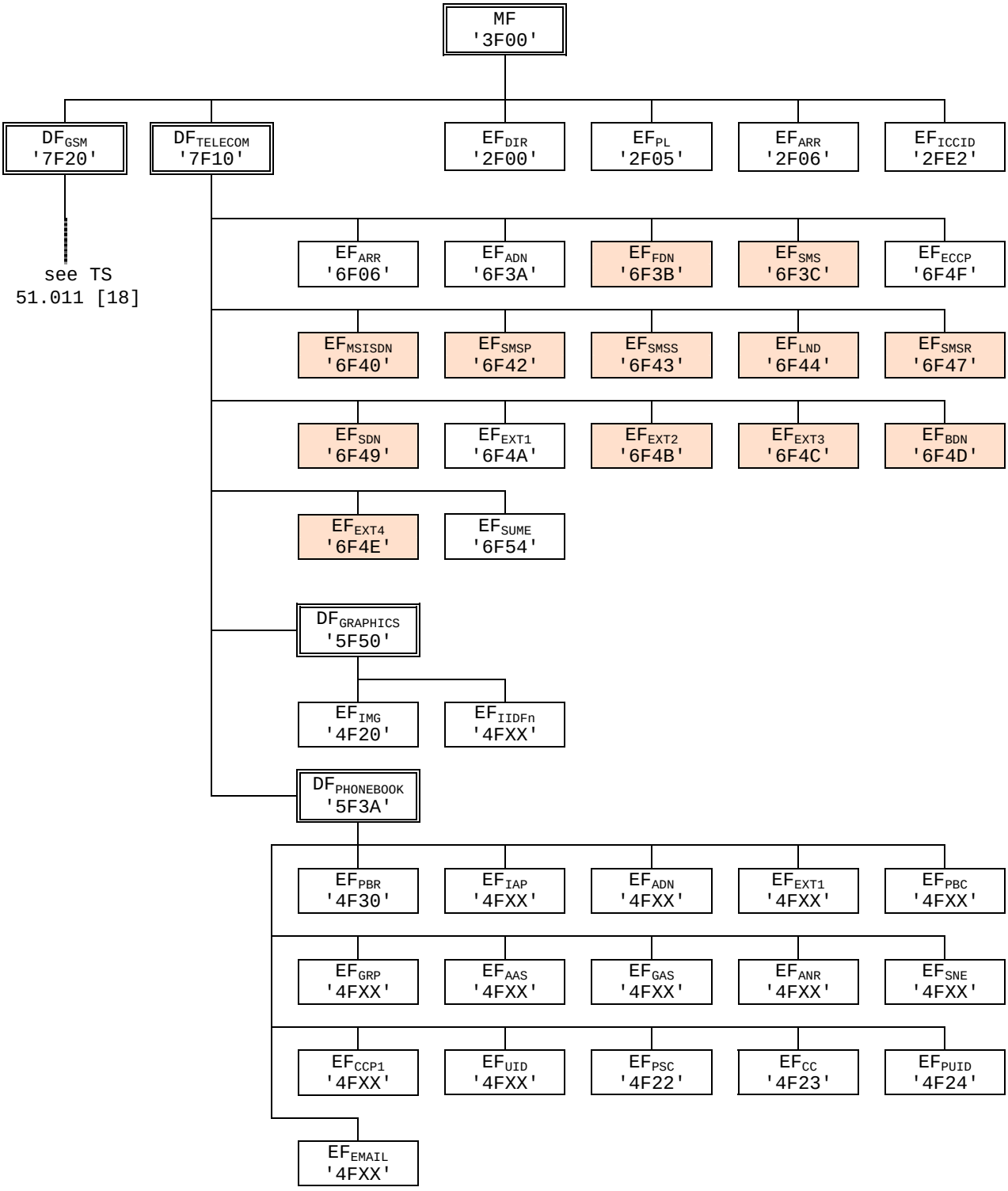
- Ciphering Algorithm Identifier:

  Contents: Ciphering Algorithm identifier for the specified Master Group Key of each Voice Broadcast Group

  Coding: See coding of EF_{VGCSCA}

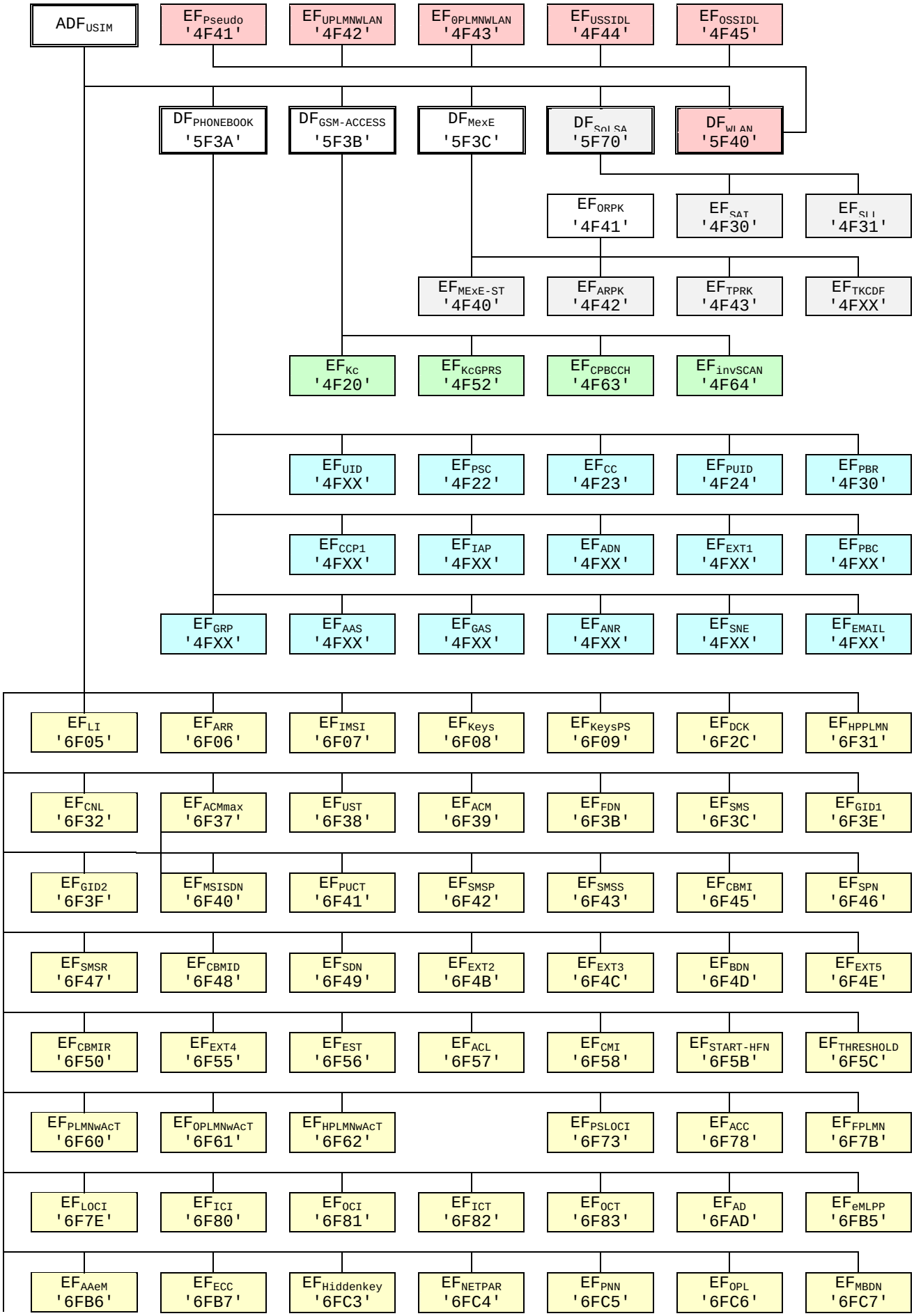
4.7 Files of USIM

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'
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 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'

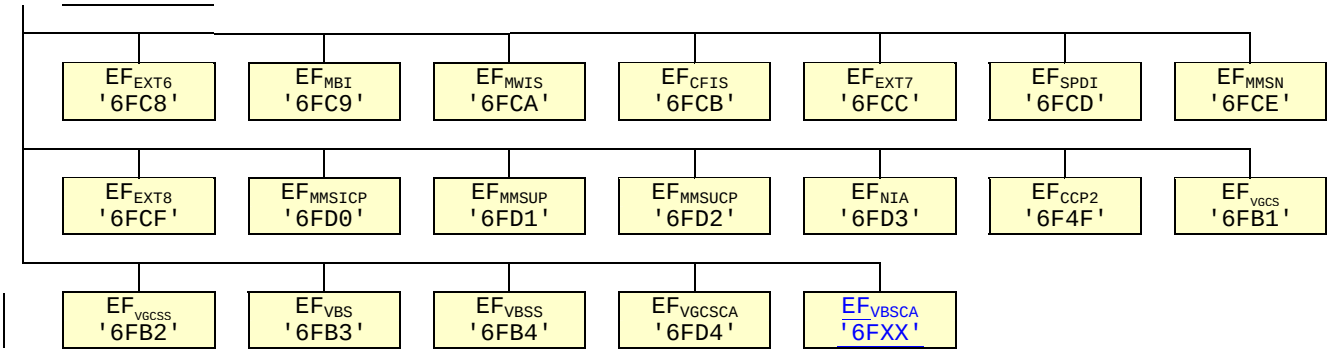


Figure 4.2: File identifiers and directory structures of USIM

7.1 AUTHENTICATE

7.1.1 Command description

The function can be used in several different contexts:

- a 3G security context, when 3G authentication vectors (RAND, XRES, CK, IK, AUTN) are available (i.e. the UE is located in the UTRAN, or in a GSM radio access network which is connected to a 3G or 3G capable VLR/SGSN), or
- a GSM security context, when GSM authentication data are available only (i.e. the UE is located in the GSM radio access network which is connected to a non-3G capable VLR/SGSN).
- a~~n~~ VGCS/VBS security context, when VGCS/VBS authentication data is available

The function is used in GSM or 3G security context during the procedure for authenticating the USIM to its HE and vice versa. In addition, a cipher key and an integrity key are calculated. For the execution of the command the USIM uses the subscriber authentication key K, which is stored in the USIM.

The function is used in VGCS/VBS security context during the procedure for retrieving the VGCS/VBS Short Term Key (VSTK) used by the terminal ~~to~~ in establishing VGCS/VBS calls.

The function is related to a particular USIM and shall not be executable unless the USIM application has been selected and activated, and the current directory is the USIM ADF or any subdirectory under this ADF and a successful PIN verification procedure has been performed (see clause 5).

7.1.1.3 VGCS/VBS security context

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

The USIM computes the ~~VGCS~~ Short Term Key (VSTK) associated with a particular VGCS/VBS ~~g~~Group Identifier (Group_Id). For this computation, the USIM uses the ~~VGCS~~ 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_Id)~~D~~.

The USIM shall first search if the ~~VGCS Group Identifier (VGCS_ID)~~ 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.~~search in the corresponding EF_{VGCSCA} for the VGCS Key Identifier (VK_ID) and retrieve the VK value to be used.~~

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 [xx]) in order to compute~~s~~ and return~~s~~ VSTK.

Input:

- Group_Id~~VGCS_ID~~, VK_Id~~D~~, VSTK_RAND

Output:

- VSTK.

7.1.2 Command parameters and data

Code	Value
CLA	As specified in TS 31.101
INS	'88'
P1	'00'
P2	See table below
Lc	See below
Data	See below
Le	'00', or maximum length of data expected in response

Parameter P2 specifies the authentication context as follows:

Coding of the reference control P2

Coding b8-b1	Meaning
'1-------'	Specific reference data (e.g. DF specific/application dependant key)
'------XX'	Authentication context: 00 GSM context 01 3G context 10 VGCS/VBS context

All other codings are RFU.

Command parameters/data:

7.1.2.2 VGCS/VBS security context

Byte(s)	Description	Length
1	Length of VGCS_ID (L1)	1
2 to 5~~(L1+1)~~	~~VGCS_ID~~Group_Id	4~~L1~~
6~~(L1+2)~~	Length of VK_Id~~D (L2)~~	1
7~~(L1+3) to (L1+L2+2)~~	VK_Id~~D~~	1~~L2~~
8~~(L1+L2+3)~~	Length of VSTK_RAND	1
~~(L1+L2+4) to (L1+L2+7)~~ 9 to L1+8	VSTK_RAND	~~4~~L1

Group_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 [xx]

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

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 SSID List	No
'4F45'	Operator controlled SSID List	Caution
'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

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
'6FXX'	Voice Broadcast Service Ciphering Algorithm	Yes
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 SSID list	'00FF…FF'
'4F45'	Operator controlled SSID list	Operator dependant
'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'
'6FXX'	Voice Broadcast Service Ciphering Algorithm	'00…00'

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 #32
New York, USA, 10-13 August 2004

Tdoc ⌘T3-040593

CR-Form-v7

CHANGE REQUEST

⌘ **31.102** **CR** 236 ⌘**rev** **-** ⌘ Current version: **6.6.0** ⌘

*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:	⌘	Introduction of M-IMAP and SIP as MMS implementations in MMS provisioning
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	11/08/04
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:

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

Reason for change:	⌘	3GPP2 SWG 1.4 is looking forward to store MMS connectivity paramenters in the R-UIM (Removable User Identification Module). In order not to create inconstinacy between the R-UIM and the USIM, SWG 1.4is willing to re-use the files defined in the USIM. But in order to be able to re-use those files, some changes must be done to allow the support of MMS implementations parameters used in 3GPP2, i.e. M-IMAP and SIP.
Summary of change:	⌘	Add SIP and M-IMAP in MMS implementaions field and adapt MMS Issuer / User Connectivity Parameters files to allow the storage of these new implementations.
Consequences if not approved:	⌘	

Clauses affected:	⌘	4.2.67,4.2.69

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

Other comments: ⌘

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: "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] ETSI TS 102 221 "Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 4)"

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

[39] ETSI TS 102 222 "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"

[xx] TIA/EIA-934: "Multimedia Messaging System Specification", May 2003

4.2.67 EF_{MMSN} (MMS Notification)

If service n°52 is "available", this file shall be present.

This EF contains information in accordance with 3GPP TS 23.140 [38] and TIA/EIA-934 [xx] comprising MMS notifications (and associated parameters) which have been received by the UE from the network. A 3GPP terminal needs only to support the MMS implementation specified in 3GPP TS 23.140 [38].

Identifier: '6FCE'	Structure: Linear fixed	Optional
Record length: 4+X bytes	Update activity: low	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to 2	MMS Status	M	2 bytes
3	MMS Implementation	M	1 byte
4 to X+3	MMS Notification	M	X bytes
X+4	Extension file record number	M	1 byte

- MMS Status

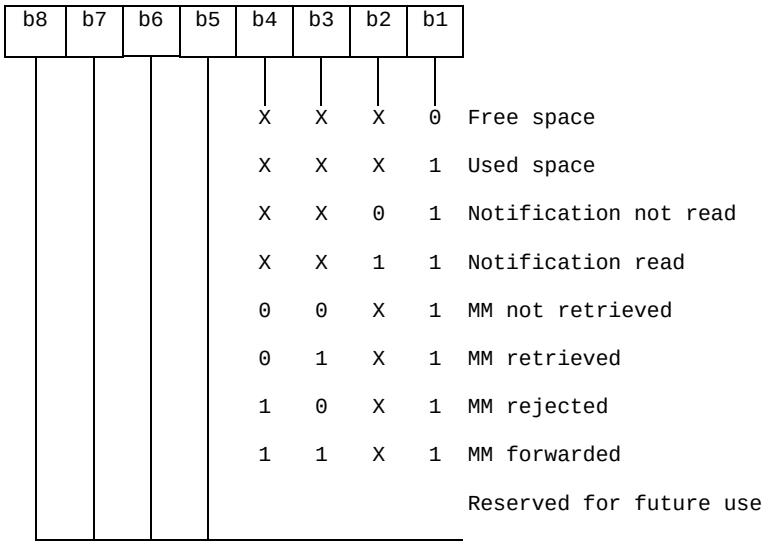
Content:

The status bytes contain the status information of the notification.

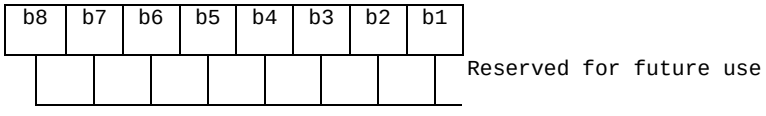
Coding:

b1 indicates whether there is valid data or if the location is free. b2 indicates whether the MMS notification has been read or not. Bits b3-b4 of the first byte indicate the MM retrieval, MM rejection, or MM forwarding status, Bits b5-b8 of the first byte and the entire second byte are reserved for future use.

First byte:



Second byte:



- MMS Implementation

Contents:

The MMS Implementation indicates the used implementation type, e.g. WAP.

Coding:

Allocation of bits:
Bit number Parameter indicated
1 WAP implementation of MMS
2 M-IMAP implementation of MMS as defined in TIA/EIA-934 [xx].
3 SIP implementation of MMS as defined in TIA/EIA-934 [xx].
4~~2~~-8 Reserved for future use

Bit value Meaning
0 Implementation not supported.
1 Implementation supported.

- MMS Notification
  Contents:
  The MMS Notification contains the MMS notification.
  Coding:
  The MMS Notification is coded according to the MMS Implementation as indicated in Byte 3.
  Any unused byte shall be set to 'FF'.

- Extension file record number
  Contents:
  - extension file record number. This byte identifies the number of a record in the EF_{EXT8} containing extension data for the notification information. The use of this byte is optional. If it is not used it shall be set to 'FF'.

  Coding:
  - binary.

4.2.69 EF_{MMSICP} (MMS Issuer Connectivity Parameters)

If service n°52 is "available", this file shall be present.

This EF contains values for Multimedia Messaging Connectivity Parameters as determined by the issuer, which can be used by the ME for MMS network connection. This file may contain one or more sets of Multimedia Messaging Issuer Connectivity Parameters. The first set of Multimedia Messaging Issuer Connectivity Parameters is used as the default set. Each set of Multimedia Messaging Issuer Connectivity Parameters may consist of one or more Interface to Core Network and Bearer information TLV objects, but shall contain only one MMS implementation TLV object, one MMS Relay/Server TLV object and one Gateway TLV object. The order of the Interface to Core Network and Bearer information TLV objects in the MMS Connectivity TLV object defines the priority of the Interface to Core Network and Bearer information, with the first TLV object having the highest priority.

Identifier: '6FD0'	Structure: Transparent	Optional
File Size: X_1+…+ X_n bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X_1	MMS Connectivity Parameters TLV object	M	X_1 bytes
X_1+1 to X_1 + X_2	MMS Connectivity Parameters TLV object	O	X_2 bytes
…	…		
X_1+…+ X_{n-1}+1 to X_1+…+ X_n	MMS Connectivity Parameters TLV object	O	X_n bytes

- MMS Connectivity Parameters tags

Description	Tag Value
MMS Connectivity Parameters Tag	'AB'
MMS Implementation Tag	‘80’
MMS Relay/Server Tag	‘81’
Interface to Core Network and Bearer Information Tag	'82'
GatewayTag	'83'
MMS Authentication Mechanism Tag	'84'
MMS Authentication User Name Tag	'85'

- MMS Connectivity Parameters contents

Description	Value	M/O	Length (bytes)

MMS Connectivity Parameters Tag	'AB'	M	1
Length	Note 1	M	Note 2
MMS Implementation Tag	'80'	M	1
Length	1	M	1
MMS Implementation Information	--	M	1
MMS Relay/Server Tag	'81'	M	1
Length	X1	M	Note 2
MMS Relay/Server Address	--	M	X1
MMS Authentication Mechanism Tag	'84'	C	1
Length	X2	C	Note 2
MMS Authentication Mechanism	--	C	1
MMS Authentication User Name Tag	'85'	C	1
Length	X3	C	Note 2
MMS Authentication User Name	--	C	X2
1st Interface to Core Network and Bearer Information Tag (highest priority)	'82'	~~M~~C	1
Length	Y1	~~M~~C	Note 2
1st Interface to Core Network and Bearer information	--	~~M~~C	Y1
2nd Interface to Core Network and Bearer Information Tag	'82'	~~M~~C	1
Length	Y2	~~M~~C	Note 2
2nd Interface to Core Network and Bearer information	--	~~M~~C	Y2
…			
Nth Interface to Core Network and Bearer Information Tag (lowest priority)	'82'	~~M~~C	1
Length	Y3	~~M~~C	Note 2
Nth Interface to Core Network and Bearer information	--	~~M~~C	Y3
GatewayTag	'83'	O	1
Length	Z	O	Note 2
Gateway Information	--	O	Z
Note 1: This is the total size of the constructed TLV object Note 2: The length is coded according to ISO/IEC 8825 [35]			

- MMS Implementation Tag '80'
  See section 4.2.67 for contents and coding.

- MMS Relay/server Tag '81'
  Contents:
  The MMS relay/server contains the address of the associated MMS relay/server.
  Coding:
  The MMS relay/server address is coded according to the guideline provided in 3GPP TS 23.140 [38].

- MMS Authentication Mechanism Tag '84'
  Contents:
  The MMS authentication mechanism contains the authentication mechanism used for M-IMAP and SIP.
  Coding:
  The MMS authentication mechanism is coded according to the guidelines provided in TIA-934 [xx].

MMS Authentication Mechanism Tag shall be present when M-IMAP and SIP implementations are indicated in MMS Implementation Tag '80'.

- MMS Authentication User Name Tag '85'
  Contents:
  The MMS Authentication User Name contains the authentication user name used for M-IMAP and SIP.
  Coding:
  The MMS authentication User Name is coded according to the guidelines provided in TIA-934 [xx].

MMS Authentication User Name Tag shall be present when M-IMAP and SIP implementations are indicated in MMS Implementation Tag '80'.

- Interface to Core Network and Bearer Information Tag '82'

  Contents:

  The Interface to Core Network and Bearer Information may contain the following information to set up the bearer: Bearer, Address, Type of address, Speed, Call type, Authentication type, Authentication id, Authentication password.

  Coding:

  The coding is according to the guideline provided in 3GPP TS 23.140 [38].

Interface to Core Network and Bearer Information Tag shall be present when WAP implementation is indicated in MMS Implementation Tag '80'.

- Gateway Tag '83'

  Contents:

  The Gateway may contain the following information; Address , Type of address, Port, Service, Authentication type , Authentication id and Authentication password.

  Coding:

  The coding is according to the guideline provided in 3GPP TS 23.140 [38].

Gateway Tag shall be present when WAP implementation is indicated in MMS Implementation Tag '80'.

Unused bytes shall be set to 'FF'.

An Example for the coding of these parameters can be found in Annex J.2.

3GPP TSG-T3#32
New York, USA, 10-13 August 2004

Tdoc ⌘ T3-040597

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.102** **CR** 237 ⌘ **rev** **1** ⌘ Current version: **6.6.0** ⌘

*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:	⌘	Editorial changes in WLAN identities lists
Source:	⌘	T3
Work item code:	⌘	I-WLAN
Date:	⌘	10/08/2004
Category:	⌘	**D**
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:	⌘	SA1 has confirmed in S1-040726 the need of two lists in the USIM for storage of Operator and User Preferred WLAN Identity list. These names do not correspond with the existing lists in the USIM and with the current naming in 24.234.
Summary of change:	⌘	The following changes are included: -Names of EF_{USSIDL} (User controlled SSID list) and EF_{OSSIDL} (Operator controlled SSID list) are changed into EF_{UWSIDL} "User Controlled WLAN specific identifier list" and EF_{OWSIDL} "Operator Controlled WLAN specific Identifier list" respectively -Length of WSID is left undefined to support other WSID different from 802.11 SSID -SSID is modified into WLAN specific Identifier (WSID) in line with 24.234
Consequences if not approved:	⌘	Misalignement with exisiting naming in other 3GPP specs

Clauses affected:	⌘	4.2.8, 4.4.5.4, 4.4.5.5, Annex A, Annex E, Annex H

	Y	N		
Other specs affected: ⌘		X	Other core specifications	⌘
			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°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

4.4.5.4 $EF_{UWSSIDL}$ (User controlled WLAN Specific IDentifier~~SSID~~ L~~l~~ist)

This file contains the user preferred list of WLAN specific identifier (~~-~~WS~~S~~ID) for WLAN selection ~~on IEEE 802.11 WLANs~~ in priority order. This file is used for ~~manual and automatic~~ WLAN selection as described in [40]. This file shall be present if service n°62 is allocated in EF_{UST}.

Identifier: '4F44'	Structure: linear fixed	Optional
SFI: '04'		
Record size: ~~33~~ X+1 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Length	M	1 bytes
2 to ~~33~~X + 1	WS~~S~~ID value	M	~~32~~ X bytes

-Length

Contents:

- this byte gives the number of bytes of the following data item containing the WS~~S~~ID value.

Coding:

- unsigned length coded on one byte

-WS~~S~~ID Value

Contents:

- ~~service~~ WLAN specific~~set~~ identifier (WS~~S~~ID) as defined in 3GPP TS 24.234 [40].~~-~~

Coding:

- binary. Unused bytes shall be set to 'FF' and not used either as a part of the value or for length calculation.

4.4.5.5 $EF_{OWSSIDL}$ (Operator controlled WLAN Specific IDentifier~~SSID~~ L~~l~~ist)

This file contains the operator preferred list of WLAN specific identifier (~~-~~WS~~S~~ID) for WLAN selection ~~on IEEE 802.11 WLANs~~ in priority order. This file is used for ~~manual and automatic~~ WLAN selection as described in [40]. This file shall be present if service n°63 is allocated in EF_{UST}.

Identifier: '4F45'	Structure: linear fixed	Optional
SFI: '05'		
Record size: ~~33~~ X + 1 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Length	M	1 bytes
2 to ~~33~~X + 1	WS~~S~~ID value	M	~~32~~ X bytes

-Length

Contents:

- this byte gives the number of bytes of the following data item containing the WS~~S~~ID value.

Coding:
- unsigned length coded on one byte

-WSSID Value
Contents:
- WLAN specific identifier (WSID) as defined in 3GPP TS 24.234 [40].~~service set identifier (SSID).~~

Coding:
- binary. Unused bytes shall be set to 'FF' and not used either as a part of the value or for length calculation.

5.6.1 WLAN ~~SSID~~ Selection related Procedures

Prerequisite: service n°62 or n°63 “available”

The ME shall read the User and Operator controlled WSSIDs from the corresponding list files (i.e. $EF_{UWSSIDL}$ and $EF_{OWSSIDL}$ to perform ~~manual or automatic IEEE 802.11~~ WLAN selection procedures as described in [40].

The user may change the User controlled WSSIDs.

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 WSSID List	No
'4F45'	Operator controlled WSSID List	Caution
'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

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
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 ~~SSID~~ WSID list	'00FF…FF'
'4F45'	Operator controlled W~~S~~SID list	Operator dependant
'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'

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].

H.3 List of SFI Values at the DF WLAN Level

File Identification	SFI	Description
'4F41'	'01'	Pseudonym
'4F42'	'02'	User controlled PLMN for WLAN
'4F43'	'03'	Operator controlled PLMN for WLAN
'4F44'	'04'	User controlled WSSID list
'4F45'	'05'	Operator controlled WSSID list

All other SFI values are reserved for future use.

3GPP TSG-T3 Meeting #32
New York, USA, 10 - 13 August 2004

Tdoc ⌘ T3-040603

CR-Form-v7

CHANGE REQUEST

⌘ **31.102** **CR** 242 ⌘ **rev** **-** ⌘ Current version: **6.6.0** ⌘

*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: ⌘	Alignement with requirements regarding USSD usage	
Source: ⌘	T3	
Work item code: ⌘	TEI	***Date:*** ⌘ 13/08/2004
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:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)

Reason for change: ⌘

In the TS 22.090 it is stated that a USSD message which arrives to the ME shall be able to arrive to the USIM:

"***6.3.2 Action at the mobile station***

The MS shall pass the message to the ME, to the SIM or to the TE as indicated in the message."

Another requirement exists in the TS 23.090:

"***5.2.5 Handling of unstructured SS operation at the MS***

(…)If the data coding schemes corresponds to the application mode:

- *For a USSD request, the MS shall pass the message to the application addressed in the ME, SIM or TE, and await application response . If the application responds, the MS shall pass the response to the MSC, maintaining the transaction. If the application releases the transaction, the MS shall release the transaction.*
- For a USSD notification, the MS shall pass the message to the application addressed in the ME, SIM or TE, and send back a response."

Due to these requirements a CR on TS 31.111 is proposed, and to be coherent with this CR, the TS 31.102 should also be corrected.

Summary of change: ⌘ Addition of a service code and correction of the SIM application toolkit related procedures.

Consequences if not approved:	⌘	Inconsistancy with the requirements will remain.

Clauses affected:	⌘	4.2.8; 5.4.x(new)			
Other specs affected:	⌘	**Y** / **N** **X** / ( ) ( ) / **X** ( ) / **X**	Other core specifications Test specifications O&M Specifications	⌘	31.111
Other comments:	⌘	Linked to Tdoc-040551			

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	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 SSID list
	Service n°63	Operator controlled SSID list
	Service n°64	VGCS security
	Service n°xx	Data download via USSD and USSD application mode

[…]

5.4 USAT related procedures

[…]

5.4.x Data Download via USSD and USSD application mode

Requirement: Service n°xx "allocated and activated".

The procedures and commands for Data Download via USSD and USSD application mode are defined in TS 31.111 [12]

3GPP TSG-T3 Meeting #32
New York, USA, 10-13 August 2004,

Tdoc ⌘ T3-040606
Superseeds *T3-040471*

CR-Form-v7.1

CHANGE REQUEST

⌘ **31.102** **CR** 243 ⌘ **rev** **-** ⌘ Current version: **5.9.0** ⌘

*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 PPS procedure
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	13/08/2004
Category:	⌘	**F**
Release:	⌘	Rel-5

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

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	The terminal may not invoke the PPS procedure as defined in TS 31.101 if the content of TA1 in the ATR is not rrecognised by the terminal. The terminal is according to the specification capable of operating with other than default values and the terminal invokes the PPS procedure in order to try to select another value before using the default values
Summary of change:	⌘	Introduce the PPS procedure
Consequences if not approved:	⌘	Terminals that not can support/recognise the value in TA1 in the ATR may not invoke the PPS procedure to increase the speed on the interface according to its capabilities

Clauses affected:	⌘	8.x (new)

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

8.x PPS procedure

If the value of TA1 in the ATR is not '11' or '01', the PPS procedure shall be used.

When the terminal does not support or cannot recognize the values indicated by the card in character TA1 of the ATR, it shall initiate at least one PPS procedure indicating Fi and Di values specified in TS 31.101 [11] before issuing a PPS with default values.