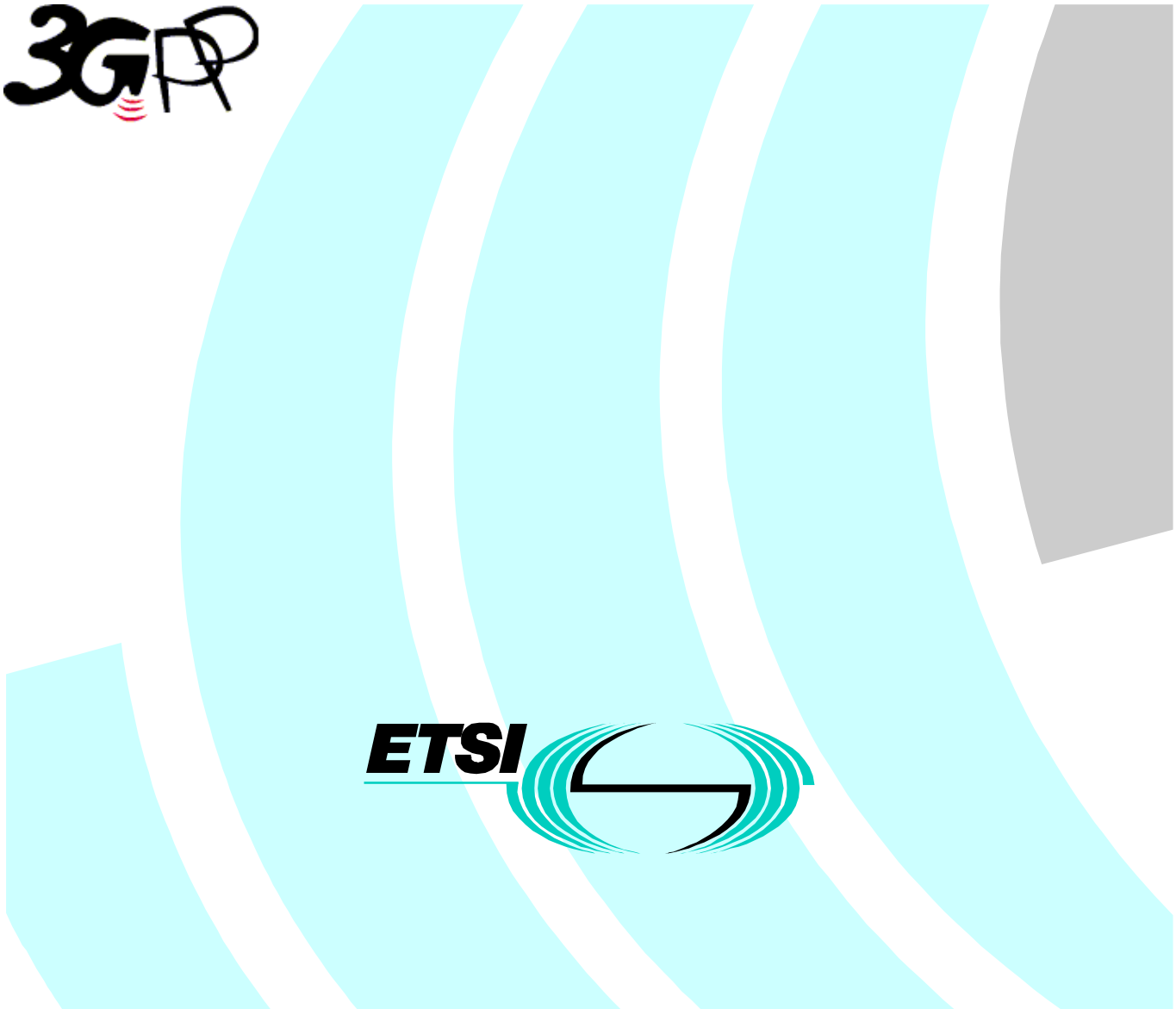
ETSI TS 131 102 V3.5.0 (2001-03)

Technical Specification

Universal Mobile Telecommunications System (UMTS); Characteristics of the USIM Application (3GPP TS 31.102 version 3.5.0 Release 1999)



Reference
RTS/TSGT-0331102UR5

Keywords
UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.org/ipr).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by the ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under www.etsi.org/key .

Contents

Foreword

This Technical Specification (TS) has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

The present document defines the Universal Subscriber Identity Module (USIM) application. This application resides on the UICC, an IC card specified in 3G TS 31.101 [11]. In particular, 3G TS 31.101 [11] specifies the application independent properties of the UICC/terminal interface such as the physical characteristics and the logical structure.

1 Scope

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

The present document specifies:

- specific command parameters;
- file structures;
- contents of EFs (Elementary Files);
- security functions;
- application protocol to be used on the interface between UICC (USIM) and ME.

This is to ensure interoperability between a USIM and an ME independently of the respective manufacturer, card issuer or operator.

The present document does not define any aspects related to the administrative management phase of the USIM. Any internal technical realisation of either the USIM or the ME is only specified where these are reflected over the interface. The present document does not specify any of the security algorithms which may be used.

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 Mobile Station (MS)".

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

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

[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".

[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: "3G Security Architecture".

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

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

[16] 3GPP TS 23.041: "Technical realization of Short Message Service Cell Broadcast (SMSCB)".

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

[18] 3GPP TS 11.11: "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: "Numbering plan for the ISDN era".

[23] ITU-T Recommendation T.50: "International Alphabet No. 5". (ISO 646 (1983): "Information processing - ISO 7-bits coded characters 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 FCD 7816-9 (1999): "Identification cards - Integrated circuit(s) cards with contacts, Part 9: Additional Interindustry commands and security attributes".

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

[28] 3GPP TS 04.18 "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 Station Application 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 05.05: "Radio Transmission and Reception"

[35] ISO/IEC 8825(1990): "Specification of Basic Encoding Rules for Abstract Syntax Notation One" Second Edition.

3 Definitions, symbols, abbreviations and coding conventions

3.1 Definitions

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

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

3.2 Symbols

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

||	Concatenation
⊕	Exclusive or
f1	Message authentication function used to compute MAC
f1*	A message authentication code (MAC) function with the property that no valuable information can be inferred from the function values of f1* about those of f1, ... , f5 and vice versa
f2	Message authentication function used to compute RES and XRES
f3	Key generating function used to compute CK
f4	Key generating function used to compute IK
f5	Key generating function used to compute AK

3.3 Abbreviations

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

3GPP	3rd Generation Partnership Project
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
EMUI	Encrypted Mobile User Identity
FCP	File Control Parameters
FFS	For Further Study
GMSI	Group Identity
GSM	Global System for Mobile communications
HE	Home Environment
ICC	Integrated Circuit Card
ICI	Incoming Call Information
ICT	Incoming Call Timer
ID	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
OFM	Operational Feature Monitor
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

3.4 Coding Conventions

The following coding conventions apply to the present document.

All lengths are presented in bytes, unless otherwise stated. Each byte is represented by bits b8 to b1, where b8 is the most significant bit (MSB) and b1 is the least significant bit (LSB). In each representation, the leftmost bit is the MSB.

The coding of Data Objects in the present document is according to ISO/IEC 7816-6 [32].

'XX': Single quotes indicate hexadecimal values. Valid elements for hexadecimal values are the numbers '0' to '9' and 'A' to 'F'.

4 Contents of the Files

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

EFs or data items having an unassigned value, or, which during the 3G session, are cleared by the ME, shall have their bytes set to 'FF'. After the administrative phase all data items shall have a defined value or have their bytes set to 'FF'. If a data item is 'deleted' during a 3G session by the allocation of a value specified in another 3G TS, then this value shall

be used and the data item is not unassigned. For example, for a deleted LAI in EF_{LOCI} the last byte takes the value 'FE' (3G TS 24.008 [9] refers).

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

When the coding is according to ITU-T Recommendation T.50 [23], bit 8 of every byte shall be set to 0.

For an overview containing all files see figures 4.1 and 4.2.

4.1 Contents of the EFs at the MF level

There are four EFs at the Master File (MF) level. These EFs are specified in 3G TS 31.101 [11].

4.1.1 EF_{DIR}

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

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

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

Contents:

- according to 3G TS 31.101 [11].

Coding:

- according to 3G TS 31.101 [11].

4.1.2 EF_{ICCID} (ICC Identity)

This EF provides a unique identification number for the ICC.

Contents:

according to 3G TS 31.101 [11].

Coding:

according to 3G TS 31.101 [11].

4.1.3 EF_{PL} (Preferred Languages)

This EF contains the codes for up to n languages. This information, determined by the user/operator, defines the preferred languages of the user in order of priority. This information may be used by the ME for MMI purposes.

This information may also be used for the screening of Cell Broadcast messages in a preferred language, as follows.

When the CB Message Identifier capability is available, the ME selects only those CB messages the language of which corresponds to an entry in this EF or in $EF_{LI,}$ whichever of these EFs is used (see subclause 5.1.1). The CB message language is defined by the Data Coding Scheme (see 3G TS 23.038 [5]) received with the CB message. The ME shall be responsible for translating the language coding indicated in the Data Coding Scheme for the Cell Broadcast Service (as defined in 3G TS 23.038 [5]) to the language coding as defined in ISO 639 [19] if it is necessary to check the language coding in EF_{PL}.

Contents:

- according to 3G TS 31.101 [11].

Coding:

- according to 3G TS 31.101 [11].

4.1.4 EF_{ARR} (Access Rule Reference)

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

Contents:

- according to 3G TS 31.101 [11].

Coding:

- according to 3G TS 31.101 [11].

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

The EFs in the USIM ADF contain service and network related information.

4.2.1 EF_{LI} (Language Indication)

This EF contains the codes for one or more languages. This information, determined by the user/operator, defines the preferred languages of the user in order of priority. This information may be used by the ME for MMI purposes. This information may also be used for the screening of Cell Broadcast messages in a preferred language, as follows.

When the CB Message Identifier capability is available, the ME selects only those CB messages the language of which corresponds to an entry in this EF or in $EF_{PL,}$ whichever of these EFs is used (see subclause 5.1.1). The CB message language is defined by the Data Coding Scheme (DCS: see 3G TS 23.038 [5]) received with the CB message. The ME shall be responsible for translating the language coding indicated in the Data Coding Scheme for the Cell Broadcast Service (as defined in 3G TS 23.038 [5]) to the language coding as defined in ISO 639 [19] if it is necessary to check the language coding in EF_{PL}.

Identifier: '6F 05'	Structure: transparent	Optional
SFI: '02'		
File size: 2n bytes	Update activity: low	
Access Conditions: READ ALW UPDATE PIN DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to 2	1st language code (highest prior).	M	2 bytes
3 to 4	2nd language code	O	2 bytes
2n-1 to 2n	Nth language code (lowest prior).	O	2 bytes

Coding:

- each language code is a pair of alpha-numeric characters, defined in ISO 639 [19]. Each alpha-numeric character shall be coded on one byte using the SMS default 7-bit coded alphabet as defined in 3G TS 23.038 [5] with bit 8 set to 0.

Unused language entries shall be set to 'FF FF'.

4.2.2 EF_{IMSI} (IMSI)

This EF contains the International Mobile Subscriber Identity (IMSI).

Identifier: '6F07'	Structure: transparent	Mandatory
SFI: '07'		
File size: 9 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Length of IMSI	M	1 byte
2 to 9	IMSI	M	8 bytes

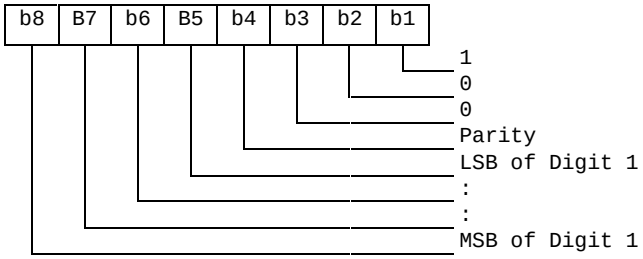
- Length of IMSI
  Contents:
  - the length indicator refers to the number of significant bytes, not including this length byte, required for the IMSI.

  Coding:
  - according to 3G TS 24.008 [9].

- IMSI
  Contents:
  - International Mobile Subscriber Identity.

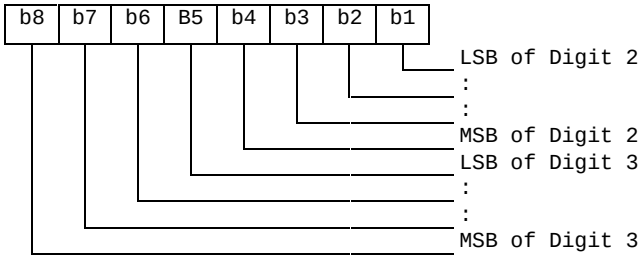
  Coding:
  - this information element is of variable length. If a network operator chooses an IMSI of less than 15 digits, unused nibbles shall be set to 'F'.

Byte 2:



For the parity bit, see 3G TS 24.008 [9].

Byte 3:



etc.

4.2.3 EF_{Keys} (Ciphering and Integrity Keys)

This EF contains the ciphering key CK, the integrity key IK and the key set identifier KSI.

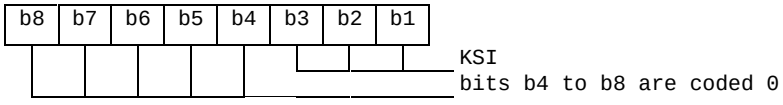
Identifier: '6F08'	Structure: transparent	Mandatory
SFI: '08'		
File size: 33 bytes	Update activity: high	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

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

- Key Set Identifier KSI.
  Coding:



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

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

4.2.4 EF_{KeysPS} (Ciphering and Integrity Keys for Packet Switched domain)

This EF contains the ciphering key CKPS, the integrity key IKPS and the key set identifier KSIPS for the packet switched (PS) domain.

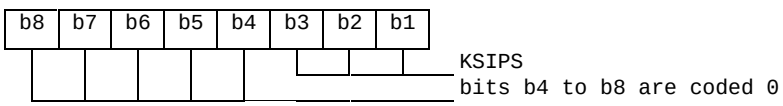
Identifier: '6F09'	Structure: transparent	Mandatory
SFI: '09'		
File size: 33 bytes	Update activity: high	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Key set identifier KSIPS	M	1 byte
2 to 17	Ciphering key CKPS	M	16 bytes
18 to 33	Integrity key IKPS	M	16 bytes

- Key Set Identifier KSIPS.
  Coding:



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

4.2.5 $EF_{PLMNwAcT}$ (User controlled PLMN selector with Access Technology)

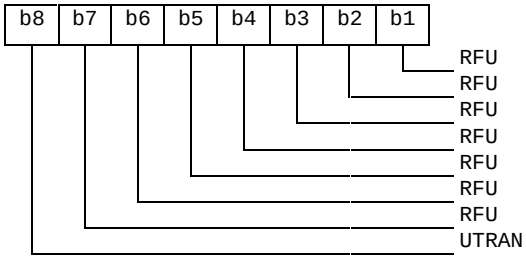
This EF contains the coding for n PLMNs, where n is at least eight. This information is determined by the user and defines the preferred PLMNs of the user in priority order. The first record indicates the highest priority and the nth record indicates the lowest. The EF also contains the Access Technologies for each PLMN in this list. (see TS 23.122 [31])

Identifier: '6F60'	Structure: transparent	Optional
SFI: '0A'		
File size: 5n (where n ≥8 bytes)	Update activity: low	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM		

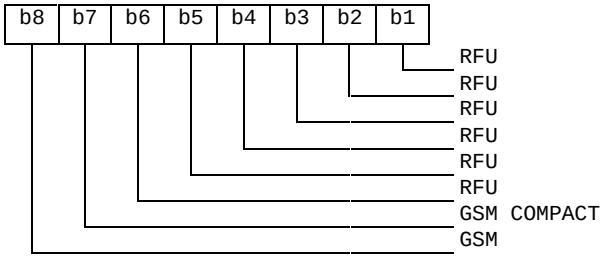
Bytes	Description	M/O	Length
1 to 3	1st PLMN (highest priority)	M	3 bytes
4 to 5	1st PLMN Access Technology Identifier	M	2 bytes
6 to 8	2nd PLMN	M	3 bytes
9 to 10	2nd PLMN Access Technology Identifier	M	2 bytes
:	:		
36 to 38	8th PLMN	M	3 bytes
39 to 40	8th PLMN Access Technology Identifier	M	2 bytes
41 to 43	9th PLMN	O	3 bytes
44 to 45	9th PLMN Access Technology Identifier	O	2 bytes
:	:		
(5n-4) to (5n-2)	Nth PLMN (lowest priority)	O	3 bytes
(5n-1) to 5n	Nth PLMN Access Technology Identifier	O	2 bytes

- PLMN
  Contents:
  - Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).
  Coding:
  - according to 3G TS 24.008 [9].
- Access Technology Identifier:
  Coding:
  - 2 bytes are used to select the access technology where the meaning of each bit is as follows:
    - bit = 1: access technology selected;
    - bit = 0: access technology not selected.

Byte5n-1:



Byte 5n:



4.2.6 EF_{HPLMN} (HPLMN search period)

This EF contains the interval of time between searches for the HPLMN (see 3G TS 22.011 [2]).

Identifier: '6F31'	Structure: transparent	Mandatory
SFI: '12'		
File size: 1 byte	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Time interval	M	1 byte

- Time interval.
  Contents:
  the time interval between two searches.
  Coding:
  the time interval is coded in integer multiples of n minutes. The range is from n minutes to a maximum value. The value '00' indicates that no attempts shall be made to search for the HPLMN. The encoding is:

  - '00': No HPLMN search attempts;
  - '01': n minutes;
  - '02': 2n minutes;
  - : :
  - 'YZ': (16Y+Z)n minutes (maximum value).

- All other values shall be interpreted by the ME as a default period.

For specification of the integer timer interval n, the maximum value and the default period refer to 3G TS 22.011 [2].

4.2.7 EF_{ACMmax} (ACM maximum value)

This EF contains the maximum value of the accumulated call meter. This EF shall always be allocated if EF_{ACM} is allocated.

Identifier: '6F37'	Structure: transparent	Optional
File size: 3 bytes	Update activity: low	

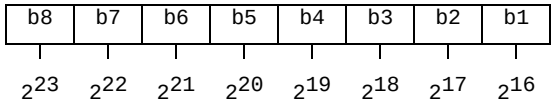
Access Conditions:

READ	PIN
UPDATE	PIN/PIN2 (fixed during administrative management)
DEACTIVATE	ADM
ACTIVATE	ADM

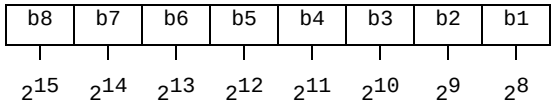
Bytes	Description	M/O	Length
1 to 3	Maximum value	M	3 bytes

- Maximum value.
  Contents:
  - maximum value of the Accumulated Call Meter (ACM).
  Coding:

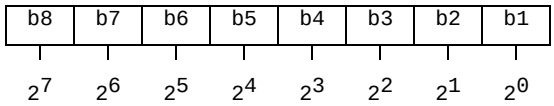
First byte:



Second byte:



Third byte:



For instance, '00' '00' '30' represents 2^5+2^4.

All ACM data is stored in the USIM and transmitted over the USIM/ME interface as binary.

ACMmax is not valid, as defined in 3G TS 22.024 [3], if it is coded '000000'.

If a GSM application is present on the UICC and the ACMmax value is to be shared between the GSM and the USIM application this file shall be shared between the two applications.

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

Service n°1 : Local Phone Book

Contents:

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: Not used (reserved for 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

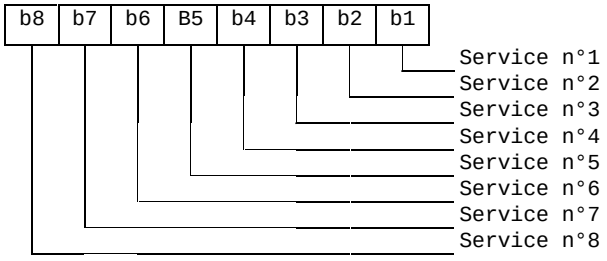
The EF shall contain at least one byte. Further bytes may be included, but if the EF includes an optional byte, then it is mandatory for the EF to also contain all bytes before that byte. Other services are possible in the future and will be coded on further bytes in the EF. The coding falls under the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

Coding:

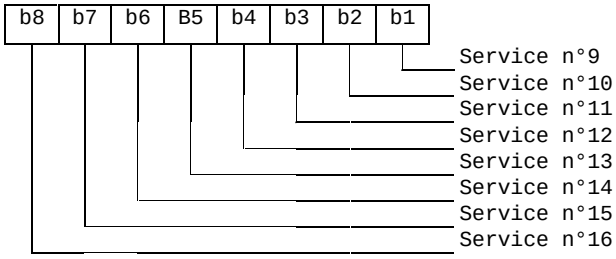
1 bit is used to code each service:
bit = 1: service available;
bit = 0: service not available.

- 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.

4.2.9 EF_{ACM} (Accumulated Call Meter)

This EF contains the total number of units for both the current call and the preceding calls.

NOTE: The information may be used to provide an indication to the user for advice or as a basis for the calculation of the monetary cost of calls (see 3G TS 22.086 [15]).

Identifier: '6F39'	Structure: cyclic	Optional
SFI: Recommended		
Record length: 3 bytes	Update activity: high	

Access Conditions:

READ	PIN
UPDATE	PIN/PIN2 (fixed during administrative management)
INCREASE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 3	Accumulated count of units	M	3 bytes

- Accumulated count of units
  Contents:
  value of the ACM.
  Coding:
  see the coding of EF_{ACMmax}.

If a GSM application is present on the UICC and the ACM value is to be shared between the GSM and the USIM application this file shall be shared between the two applications.

4.2.10 EF_{GID1} (Group Identifier Level 1)

This EF contains identifiers for particular USIM-ME associations. It can be used to identify a group of USIMs for a particular application.

Identifier: '6F3E'	Structure: transparent	Optional
File size: 1-n bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to n	USIM group identifier(s)	O	n bytes

4.2.11 EF_{GID2} (Group Identifier Level 2)

This EF contains identifiers for particular USIM-ME associations. It can be used to identify a group of USIMs for a particular application.

Identifier: '6F3F'	Structure: transparent	Optional
File size: 1-n bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to n	USIM group identifier(s)	O	n bytes

NOTE: The structure of EF_{GID1} and EF_{GID2} is identical. They are provided to allow the network operator to enforce different levels of security dependant on an application.

4.2.12 EF_{SPN} (Service Provider Name)

This EF contains the service provider name and appropriate requirements for the display by the ME.

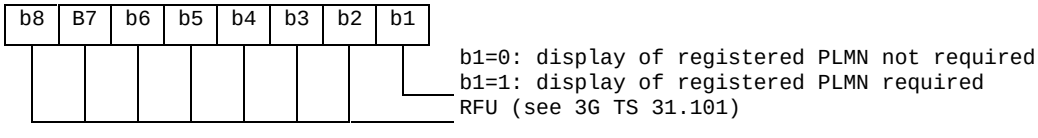
Identifier: '6F46'	Structure: transparent	Optional
File Size: 17 bytes	Update activity: low	

Access Conditions:

READ	ALWAYS
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Display Condition	M	1 byte
2 to 17	Service Provider Name	M	16 bytes

- Display Condition
  Contents: display condition for the service provider name in respect to the registered PLMN (see GSM 02.07 [17]).
  Coding:



- Service Provider Name

Contents:
service provider string to be displayed
Coding:
the string shall use:
- either the SMS default 7-bit coded alphabet as defined in 3G TS 23.038 [5] with bit 8 set to 0. The string shall be left justified. Unused bytes shall be set to 'FF'.
- or one of the UCS2 code options defined in the annex of 3G TS 31.101 [11].

4.2.13 EF_{PUCT} (Price per Unit and Currency Table)

This EF contains the Price per Unit and Currency Table (PUCT). The PUCT is Advice of Charge related information which may be used by the ME in conjunction with EF_{ACM} to compute the cost of calls in the currency chosen by the subscriber, as specified in 3G TS 22.024 [3]. This EF shall always be allocated if EF_{ACM} is allocated.

Identifier: '6F41'	Structure: transparent	Optional
File size: 5 bytes	Update activity: low	

Access Conditions:

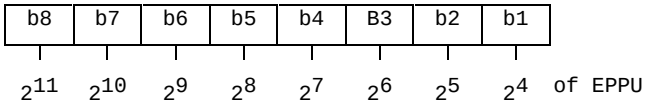
READ	PIN
UPDATE	PIN/PIN2 (fixed during administrative management)
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 3	Currency code	M	3 bytes
4 to 5	Price per unit	M	2 bytes

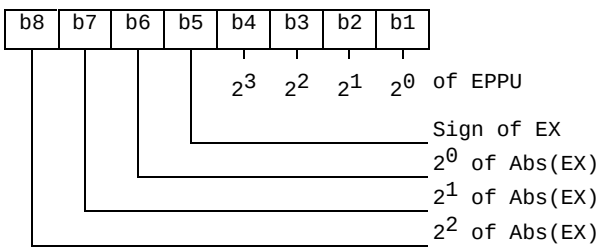
- Currency code
  Contents:
  the alpha-identifier of the currency code.
  Coding:
  bytes 1, 2 and 3 are the respective first, second and third character of the alpha identifier. This alpha-tagging shall use the SMS default 7-bit coded alphabet as defined in 3G TS 23.038 [5] with bit 8 set to 0.

- Price per unit
  Contents:
  price per unit expressed in the currency coded by bytes 1-3.
  Coding:
  byte 4 and bits b1 to b4 of byte 5 represent the Elementary Price per Unit (EPPU) in the currency coded by bytes 1-3. Bits b5 to b8 of byte 5 are the decimal logarithm of the multiplicative factor represented by the absolute value of its decimal logarithm (EX) and the sign of EX, which is coded 0 for a positive sign and 1 for a negative sign.

Byte 4:



Byte 5:



- The computation of the price per unit value is made by the ME in compliance with 3G TS 22.024 [3] by the following formula:

price per unit = EPPU * 10^{EX}.

- The price has to be understood as expressed in the coded currency.

If a GSM application is present on the UICC and the PUCT information is to be shared between the GSM and the USIM application, then this file shall be shared between the two applications.

4.2.14 EF_{CBMI} (Cell Broadcast Message identifier selection)

This EF contains the Message Identifier Parameters which specify the type of content of the cell broadcast messages that the subscriber wishes the UE to accept.

Any number of CB Message Identifier Parameters may be stored in the USIM. No order of priority is applicable.

Identifier: '6F45'	Structure: transparent	Optional
File size: 2 n bytes	Update activity: low	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to 2	CB Message Identifier 1	O	2 bytes
3 to 4	CB Message Identifier 2	O	2 bytes
2n-1 to 2n	CB Message Identifier n	O	2 bytes

- Cell Broadcast Message Identifier
  Coding:
  - as in 3G TS 23.041 [16], "Message Format on BTS-MS Interface - Message Identifier";
  - values listed show the types of message which shall be accepted by the UE;
  - unused entries shall be set to 'FF FF'.

4.2.15 EF_{ACC} (Access Control Class)

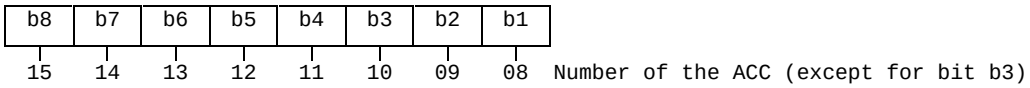
This EF contains the assigned access control class(es). The access control class is a parameter to control the access attempts. 15 classes are split into 10 classes randomly allocated to normal subscribers and 5 classes allocated to specific high priority users. For more information see 3G TS 22.011 [2].

Identifier: '6F78'	Structure: transparent	Mandatory
SFI: '06'		
File size: 2 bytes	Update activity: low	
Access Conditions: READ PIN UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

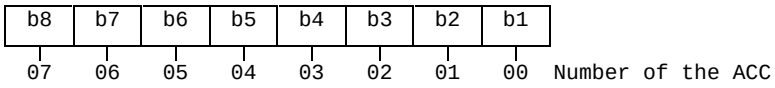
Bytes	Description	M/O	Length
1 to 2	Access control classes	M	2 bytes

- Access control classes
  Coding:
  - each ACC is coded on one bit. An ACC is "allocated" if the corresponding bit is set to 1 and "not allocated" if this bit is set to 0. Bit b3 of byte 1 is set to 0.

Byte 1:



Byte 2:



4.2.16 EF_{FPLMN} (Forbidden PLMNs)

This EF contains the coding for n Forbidden PLMNs (FPLMN). It is read by the ME as part of the USIM initialization procedure and indicates PLMNs which the UE shall not automatically attempt to access.

A PLMN is written to the EF if a network rejects a Location Update with the cause "PLMN not allowed". The ME shall manage the list as follows.

When n FPLMNs are held in the EF, and rejection of a further PLMN is received by the ME from the network, the ME shall modify the EF using the UPDATE command. This new PLMN shall be stored in the n^{th} position, and the existing list "shifted" causing the previous contents of the first position to be lost.

When less than n FPLMNs exist in the EF, storage of an additional FPLMN shall not cause any existing FPLMN to be lost.

Dependent upon procedures used to manage storage and deletion of FPLMNs in the EF, it is possible, when less than n FPLMNs exist in the EF, for 'FFFFFF' to occur in any position. The ME shall analyse all the EF for FPLMNs in any position, and not regard 'FFFFFF' as a termination of valid data.

Identifier: '6F7B'	Structure: transparent	Mandatory
SFI: '0D'		
File size: n*3 bytes (n>3)	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 3	PLMN 1	M	3 bytes
4 to 6	PLMN 2	M	3 bytes
7 to 9	PLMN 3	M	3 bytes
10 to 12	PLMN 4	M	3 bytes
(3n-2) to 3n	PLMN n	O	3 bytes

- PLMN

  Contents:

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

  Coding:

  according to 3G TS 24.008 [9].

  For instance, using 246 for the MCC and 81 for the MNC and if this is stored in PLMN 3 the contents is as follows:

  Bytes 7-9: '42' 'F6' '18'.

  If storage for fewer than n PLMNs is required, the unused bytes shall be set to 'FF'.

4.2.17 EF_{LOCI} (Location Information)

This EF contains the following Location Information:

- Temporary Mobile Subscriber Identity (TMSI);
- Location Area Information (LAI);
- Location update status.

See subclause 5.2.5 for special requirements when updating EF_{LOCI}.

Identifier: '6F7E'	Structure: transparent	Mandatory
SFI: '0B'		
File size: 11 bytes	Update activity: high	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 4	TMSI	M	4 bytes
5 to 9	LAI	M	5 bytes
10	RFU	M	1 byte
11	Location update status	M	1 byte

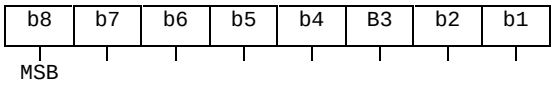
- TMSI

  Contents:

  Temporary Mobile Subscriber Identity.

  Coding:

  according to 3G TS 24.008 [9].



- LAI

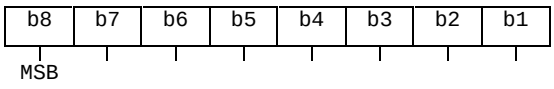
  Contents:

  Location Area Information.

  Coding:

  according to 3G TS 24.008 [9].

  Byte 5: first byte of LAI



- Location update status

  Contents:

  status of location update according to 3G TS 24.008 [9].

  Coding:

  Byte 11:

  Bits: b3 b2 b1

  0 0 0 : updated.
  0 0 1 : not updated.
  0 1 0 : PLMN not allowed.
  0 1 1 : Location Area not allowed.
  1 1 1 : reserved.

  Bits b4 to b8 are RFU (see 3G TS 31.101 [11]).

4.2.18 EF_{AD} (Administrative Data)

This EF contains information concerning the mode of operation according to the type of USIM, such as normal (to be used by PLMN subscribers for 3G operations), type approval (to allow specific use of the ME during type approval procedures of e.g. the radio equipment), cell testing (to allow testing of a cell before commercial use of this cell), manufacturer specific (to allow the ME manufacturer to perform specific proprietary auto-test in its ME during e.g. maintenance phases).

It also provides an indication of whether some ME features should be activated during normal operation as well as information about the length of the MNC, which is part of the International Mobile Subscriber Identity (IMSI).

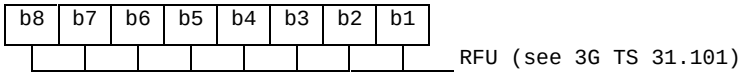
Identifier: '6FAD'	Structure: transparent	Mandatory
SFI: '03'		
File size: 4+X bytes	Update activity: low	
Access Conditions: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1	UE operation mode	M	1 byte
2 to 3	Additional information	M	2 bytes
4	length of MNC in the IMSI	M	1 byte
5 to 4+X	RFU	O	X bytes

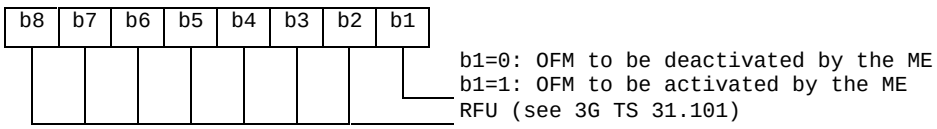
- UE operation mode:
  Contents:
  mode of operation for the UE
  Coding:
  Initial value
  - '00' normal operation.
  - '80' type approval operations.
  - '01' normal operation + specific facilities.
  - '81' type approval operations + specific facilities.
  - '02' maintenance (off line).
  - '04' cell test operation.

- Additional information:
  Coding:
  - specific facilities (if b1=1 in byte 1);

  Byte 2 (first byte of additional information):

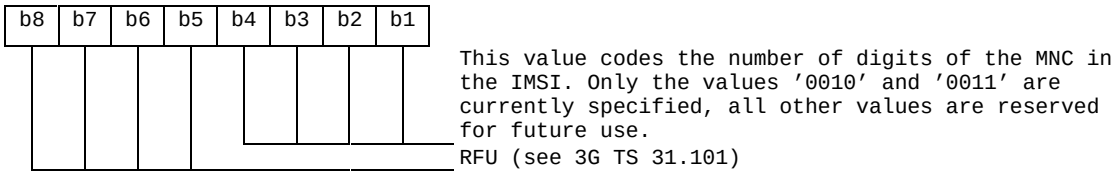


  Byte 3:



- Length of MNC in the IMSI :
  Contents:
  The length indicator refers to the number of digits, used for extracting the MNC from the IMSI
  Coding:

Byte 4:



The OFM bit is used to control the Ciphering Indicator as specified in GSM 02.07 [17].

ME manufacturer specific information (if b2=1 in byte 1).

4.2.19 void

4.2.20 EF_{CBMID} (Cell Broadcast Message Identifier for Data Download)

This EF contains the message identifier parameters which specify the type of content of the cell broadcast messages which are to be passed to the USIM.

Any number of CB message identifier parameters may be stored in the USIM. No order of priority is applicable.

Identifier: '6F48'	Structure: transparent	Optional
SFI: '0E'		
File size: 2n bytes	Update activity: low	
Access Conditions: READ PIN UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to 2	CB Message Identifier 1	O	2 bytes
3 to 4	CB Message Identifier 2	O	2 bytes
2n-1 to 2n	CB Message Identifier n	O	2 bytes

- Cell Broadcast Message Identifier.
  Coding:
  - as in 3G TS 23.041 [16]. Values listed show the identifiers of messages which shall be accepted by the UE to be passed to the USIM.
    Unused entries shall be set to 'FF FF'.

4.2.21 EF_{ECC} (Emergency Call Codes)

This EF contains emergency call codes.

Identifier: '6FB7'	Structure: linear fixed	Mandatory
SFI: '01'		
Record size: X+4 bytes	Update activity: low	

Access Conditions:

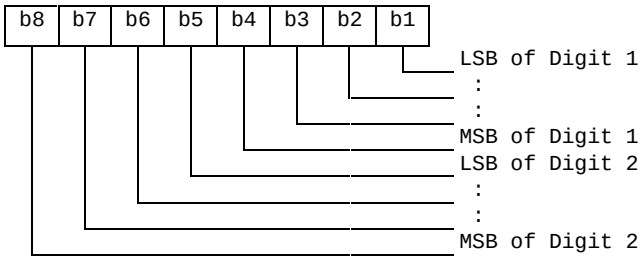
READ	ALW
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 3	Emergency Call Code	M	3 bytes
4 to X+3	Emergency Call Code Alpha Identifier	O	X bytes
X+4	Emergency Service Category	M	1 byte

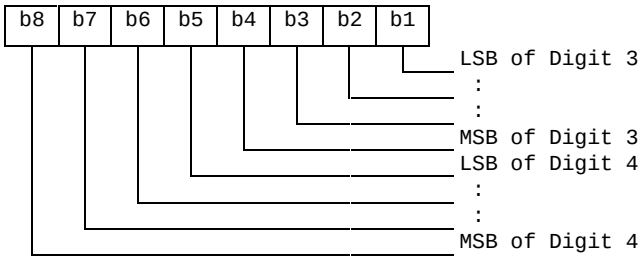
- Emergency Call Code.
  Contents:
  - Emergency Call Code.

  Coding:
  - the emergency call code is of a variable length with a maximum length of 6 digits. Each emergency call code is coded on three bytes, with each digit within the code being coded on four bits as shown below. If a code of less than 6 digits is chosen, then the unused nibbles shall be set to 'F'. If EF_{ECC} does not contain any valid number, the UE shall use the emergency numbers it stores for use in setting up an emergency call without a USIM.

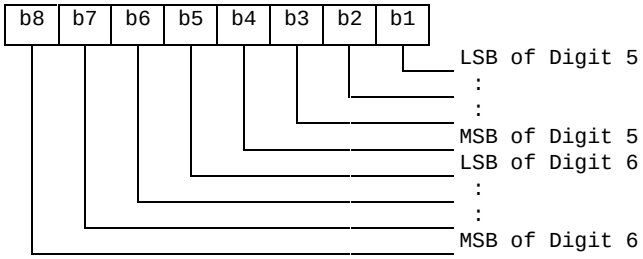
Byte 1:



Byte 2:



Byte 3:



- Emergency Call Code Alpha Identifier.
  Contents:
  Information about the dialled emergency number to be displayed to the user.
  Coding:
  this alpha-tagging shall use
  either:
  - the SMS default 7-bit coded alphabet as defined in 3G 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 3G TS 31.101 [11].
- Emergency Service Category.
  Contents:
  Information to be sent to the network indicating the category of the emergency call.
  Coding:
  Coding according to 24.008 [9].

4.2.22 EF_{CBMIR} (Cell Broadcast Message Identifier Range selection)

This EF contains ranges of cell broadcast message identifiers that the subscriber wishes the UE to accept.

Any number of CB Message Identifier Parameter ranges may be stored in the USIM. No order of priority is applicable.

Identifier: '6F50'	Structure: transparent	Optional
File size: 4n bytes	Update activity: low	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to 4	CB Message Identifier Range 1	O	4 bytes
5 to 8	CB Message Identifier Range 2	O	4 bytes
(4n-3) to 4n	CB Message Identifier Range n	O	4 bytes

- Cell Broadcast Message Identifier Ranges.
  Contents:
  - CB Message Identifier ranges:

  Coding:
  - bytes one and two of each range identifier equal the lower value of a cell broadcast range, bytes three and four equal the upper value of a cell broadcast range, both values are coded as in 3G TS 23.041 [16] "Message Format on BTS-MS Interface - Message Identifier". Values listed show the ranges of messages which shall be accepted by the UE.
    Unused entries shall be set to 'FF FF FF FF'.

4.2.23 EF_{PSLOCI} (Packet Switched location information)

This EF contains the following Location Information:

- Packet Temporary Mobile Subscriber Identity (P-TMSI);

- Packet Temporary Mobile Subscriber Identity signature value (P-TMSI signature value);
- Routing Area Information (RAI);
- Routing Area update status.

Identifier: '6F73'	Structure: transparent	Mandatory
SFI: '0C'		
File size: 14 bytes	Update activity: high	

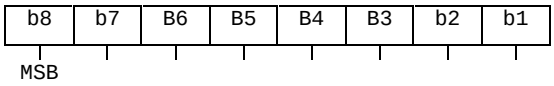
Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 4	P-TMSI	M	4 bytes
5 to 7	P-TMSI signature value	M	3 bytes
8 to13	RAI	M	6 bytes
14	Routing Area update status	M	1 byte

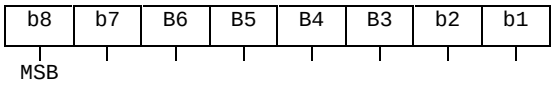
- P-TMSI.
  Contents:
  Packet Temporary Mobile Subscriber Identity.
  Coding:
  according to 3G TS 24.008 [9].

Byte 1: first byte of P-TMSI



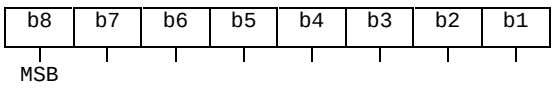
- P-TMSI signature value.
  Contents:
  Packet Temporary Mobile Subscriber Identity signature value.
  Coding:
  according to 3G TS 24.008 [9].

  Byte 5: first byte of P-TMSI signature value.



- RAI
  Contents:
  Routing Area Information.
  Coding:
  according to 3G TS 24.008 [9].

Byte 8: first byte of RAI



- Routing Area update status.
  Contents:
  status of routing area update according to 3G TS 24.008 [9].

Coding:
byte 14:

Bits:	b3	b2	b1.	
	0	0	0	: updated.
	0	0	1	: not updated.
	0	1	0	: PLMN not allowed.
	0	1	1	: Routing Area not allowed.
	1	1	1	: reserved.

Bits b4 to b8 are RFU (see 3G TS 31.101 [11]).

4.2.24 EF_{FDN} (Fixed Dialling Numbers)

This EF contains Fixed Dialling Numbers (FDN) and/or Supplementary Service Control strings (SSC). In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records at the USIM ADF level. It may also contain an associated alpha-tagging. If this file is present in the USIM, the Enabled Services Table (EF_{EST}) shall also be present.

Identifier: '6F3B'	Structure: linear fixed	Optional
Record length: X+14 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN2
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	Alpha Identifier	O	X bytes
X+1	Length of BCD number/SSC contents	M	1 byte
X+2	TON and NPI	M	1 byte
X+3 to X+12	Dialling Number/SSC String	M	10 bytes
X+13	Capability/Configuration2 Identifier	M	1 byte
X+14	Extension2 Record Identifier	M	1 byte

For contents and coding of all data items see the respective data items of the EF_{ADN} (subclause 4.4.2.3), with the exception that extension records are stored in the EF_{EXT2}.

By default, destination addresses which are not in EF_{FDN} shall not be allowed on any CS bearer service/teleservice or SMS when FDN is enabled.

For the FDN procedures related to SMS see TS 22.101 [24] and TS 31.111 [12].

NOTE: The value of X (the number of bytes in the alpha-identifier) may be different to the length denoted X in EF_{ADN}.

4.2.25 EF_{SMS} (Short messages)

This EF contains information in accordance with 3G TS 23.040 [6] comprising short messages (and associated parameters) which have either been received by the UE from the network, or are to be used as an UE originated message.

Identifier: '6F3C'	Structure: linear fixed	Optional
Record length: 176 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Status	M	1 byte
2 to 176	Remainder	M	175 bytes

- Status.

  Contents:

  Status byte of the record which can be used as a pattern in the SEARCH RECORD command. For UE originating messages sent to the network, the status shall be updated when the UE receives a status report, or sends a successful SMS Command relating to the status report.

  Coding:

b8	b7	b6	b5	b4	b3	b2	b1	
					X	X	0	free space
					X	X	1	used space
					0	0	1	message received by UE from network; message read
					0	1	1	message received by UE from network; message to be read
					1	1	1	UE originating message; message to be sent
								RFU (see 3G TS 31.101 [11])

b8	b7	b6	b5	b4	b3	b2	b1	
			X	X	1	0	1	UE originating message; message sent to the network:
			0	0	1	0	1	Status report not requested
			0	1	1	0	1	Status report requested but not (yet) received;
			1	0	1	0	1	Status report requested, received but not stored in EF-SMSR;
			1	1	1	0	1	Status report requested, received and stored in EF-SMSR;
								RFU (see 3G TS 31.101 [11])

- Remainder.

  Contents:

  This data item commences with the TS-Service-Centre-Address as specified in 3G TS 24.011 [10]. The bytes immediately following the TS-Service-Centre-Address contain an appropriate short message TPDU as specified in 3G TS 23.040 [6], with identical coding and ordering of parameters.

  Coding:

  according to 3G TS 23.040 [6] and 3G TS 24.011 [10]. Any TP-message reference contained in an UE originated message stored in the USIM, shall have a value as follows:

	Value of the TP-message-reference:
message to be sent:	'FF'.
message sent to the network:	the value of TP-Message-Reference used in the message sent to the network.

  Any bytes in the record following the TPDU shall be filled with 'FF'.

  It is possible for a TS-Service-Centre-Address of maximum permitted length, e.g. containing more than 18 address digits, to be associated with a maximum length TPDU such that their combined length is 176 bytes. In this case the ME shall store in the USIM the TS-Service-Centre-Address and the TPDU in bytes 2-176 without modification, except for the last byte of the TPDU, which shall not be stored.

4.2.26 EF_{MSISDN} (MSISDN)

This EF contains MSISDN(s) related to the subscriber. In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records at the USIM ADF level. It may also contain an associated alpha-tagging.

Identifier: '6F40'	Structure: linear fixed	Optional
Record length: X+14 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN/ADM (fixed during administrative management)
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	Alpha Identifier	O	X bytes
X+1	Length of BCD number/SSC contents	M	1 byte
X+2	TON and NPI	M	1 byte
X+3 to X+12	Dialling Number/SSC String	M	10 bytes
X+13	Capability/Configuration2 Identifier	M	1 byte
X+14	Extension5 Record Identifier	M	1 byte

For contents and coding of all data items see the respective data items of EF_{ADN}.

If the USIM stores more than one MSISDN number and the ME displays the MSISDN number(s) within the initialisation procedure then the one stored in the first record shall be displayed with priority.

NOTE: The value of X (the number of bytes in the alpha-identifier) may be different to the length denoted X in EF_{ADN}.

4.2.27 EF_{SMSP} (Short message service parameters)

This EF contains values for Short Message Service header Parameters (SMSP), which can be used by the ME for user assistance in preparation of mobile originated short messages. For example, a service centre address will often be common to many short messages sent by the subscriber.

The EF consists of one or more records, with each record able to hold a set of SMS parameters. The first (or only) record in the EF shall be used as a default set of parameters, if no other record is selected.

To distinguish between records, an alpha-identifier may be included within each record, coded on Y bytes.

The SMS parameters stored within a record may be present or absent independently. When a short message is to be sent from the UE, the parameter in the USIM record, if present, shall be used when a value is not supplied by the user.

Identifier: '6F42'	Structure: linear fixed	Optional
Record length: 28+Y bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to Y	Alpha-Identifier	O	Y bytes
Y+1	Parameter Indicators	M	1 byte
Y+2 to Y+13	TP-Destination Address	M	12 bytes
Y+14 to Y+25	TS-Service Centre Address	M	12 bytes
Y+26	TP-Protocol Identifier	M	1 byte
Y+27	TP-Data Coding Scheme	M	1 byte
Y+28	TP-Validity Period	M	1 byte

Storage is allocated for all of the possible SMS parameters, regardless of whether they are present or absent. Any bytes unused, due to parameters not requiring all of the bytes, or due to absent parameters, shall be set to 'FF'.

- Alpha-Identifier.
  Contents:
  Alpha Tag of the associated SMS-parameter.
  Coding:
  see subclause 4.4.2.3 (EF_{ADN}).

NOTE: The value of Y may be zero, i.e. the alpha-identifier facility is not used. By using the command GET RESPONSE the ME can determine the value of Y.

- Parameter Indicators.
  Contents:
  each of the default SMS parameters which can be stored in the remainder of the record are marked absent or present by individual bits within this byte.
  Coding:
  allocation of bits:

bit number	Parameter indicated.
1	TP-Destination Address.
2	TS-Service Centre Address.
3	TP-Protocol Identifier.
4	TP-Data Coding Scheme.
5	TP-Validity Period.
6	reserved, set to 1.
7	reserved, set to 1.
8	reserved, set to 1.

Bit value	Meaning.
0	Parameter present.
1	Parameter absent.

- TP-Destination Address.
  Contents and Coding:
  as defined for SM-TL address fields in 3G TS 23.040 [6].

- TP-Service Centre Address.
  Contents and Coding:
  as defined for RP-Destination address Centre Address in 3G TS 24.011 [10].

- TP-Protocol Identifier.
  Contents and Coding:
  as defined in 3G TS 23.040 [6].

- TP-Data Coding Scheme.
  Contents and Coding:
  as defined in 3G TS 23.038 [5].

- TP-Validity Period.
  Contents and Coding:
  as defined in 3G TS 23.040 [6] for the relative time format.

4.2.28 EF_{SMSS} (SMS status)

This EF contains status information relating to the short message service.

The provision of this EF is associated with EF_{SMS}. Both files shall be present together, or both absent from the USIM.

Identifier: '6F43'	Structure: transparent	Optional
File size: 2+X bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Last Used TP-MR	M	1 byte
2	SMS "Memory Cap. Exceeded" Not. Flag	M	1 byte
3 to 2+X	RFU	O	X bytes

- Last Used TP-MR.
  Contents:
  - the value of the TP-Message-Reference parameter in the last mobile originated short message, as defined in 3G TS 23.040 [6].

  Coding:
  - as defined in 3G TS 23.040 [6].

- SMS "Memory Capacity Exceeded" Notification Flag.
  Contents:
  - this flag is required to allow a process of flow control, so that as memory capacity in the UE becomes available, the Network can be informed. The process for this is described in 3G TS 23.040 [6].

  Coding:
  b1=1 means flag unset; memory capacity available;
  b1=0 means flag set;
  b2 to b8 are reserved and set to 1.

4.2.29 EF_{SDN} (Service Dialling Numbers)

This EF contains special service numbers (SDN) and/or the respective supplementary service control strings (SSC). In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records at the USIM ADF level. It may also contain associated alpha-tagging.

Identifier: '6F49'	Structure: linear fixed	Optional
Record length: X+14 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1-X	Alpha identifier	O	X bytes
X+1	Length of BCD number/SSC contents	M	1 bytes
X+2	TON and NPI	M	1 byte
X+3 to X+12	Dialling Number/SSC String	M	10 bytes
X+13	Capability/Configuration Identifier	M	1 byte
X+14	Extension3 Record Identifier	M	1 byte

For contents and coding of all data items see the respective data items of the EF_{ADN} (subclause 4.4.2.3), with the exception that extension records are stored in the EF_{EXT3}.

NOTE: The value of X (the number of bytes in the alpha-identifier) may be different to the length denoted X in EF_{ADN}.

4.2.30 EF_{EXT2} (Extension2)

This EF contains extension data of an FDN (see FDN in 4.2.24).

Identifier: '6F4B'	Structure: linear fixed	Optional
Record length: 13 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN2
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Record type	M	1 byte
2 to 12	Extension data	M	11 bytes
13	Identifier	M	1 byte

For contents and coding see subclause 4.4.2.4 (EF_{EXT1}).

4.2.31 EF_{EXT3} (Extension3)

This EF contains extension data of an SDN (see SDN in 4.2.29).

Identifier: '6F4C'	Structure: linear fixed	Optional
Record length: 13 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Record type	M	1 byte
2 to 12	Extension data	M	11 bytes
13	Identifier	M	1 byte

For contents and coding see subclause 4.4.2.4 (EF_{EXT1}).

4.2.32 EF_{SMSR} (Short message status reports)

This EF contains information in accordance with 3G TS 23.040 [6] comprising short message status reports which have been received by the UE from the network.

Each record is used to store the status report of a short message in a record of EF_{SMS}. The first byte of each record is the link between the status report and the corresponding short message in EF_{SMS}.

Identifier: '6F47'	Structure: linear fixed	Optional
Record length: 30 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	SMS record identifier	M	1
2 to 30	SMS status report	M	29 bytes

- SMS record identifier.
  Contents:
  - this data item identifies the corresponding SMS record in EF_{SMS}, e.g. if this byte is coded '05' then this status report corresponds to the short message in record #5 of EF_{SMS}.
  Coding:
  - '00' - empty record;
  - '01' - 'FF' - record number of the corresponding SMS in EF_{SMS}.

- SMS status report:
  Contents:
  - this data item contains the SMS-STATUS-REPORT TPDU as specified in 3G TS 23.040 [6], with identical coding and ordering of parameters.
  Coding:
  - according to 3G TS 23.040 [6]. Any bytes in the record following the TPDU shall be filled with 'FF'.

4.2.33 EF_{ICI} (Incoming Call Information)

This EF is located within the USIM application. The incoming call information can be linked to the phone book stored under $DF_{TELECOM}$ or to the local phone book within the USIM. The EF_{ICI} contains the information related to incoming calls.

The time of the call and duration of the call are stored in this EF. This EF can also contain associated alpha identifier that may be supplied with the incoming call. In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records at the USIM ADF level. The structure of this EF is cyclic, so the contents shall be updated only after a call is disconnected.

If CLI is supported and the incoming phone number matches a number stored in the phone book the incoming call information is linked to the corresponding information in the phone book. If the incoming call matches an entry but is indicated as hidden in the phone book the link is established but the information is not displayed by the ME if the code for the secret entry has not been verified. The ME shall not ask for the secret code to be entered at this point.

Optionally the ME may store the link to phone book entry in the file, so that it does not need to look again for a match in the phone book when it reuses the entry. But the ME will have to check that the incoming call number still exits in the linked phone book entry, as the link might be broken (entry modified). When not used by the ME or no link to the phone book has been found, this field shall be set to 'FFFFFF'.

The first byte of this link is used to identify clearly the phone book location either global (i.e. under $DF_{TELECOM}$) or local (i.e. USIM specific). To allow the reuse of the referring mechanism in further implementation of the phonebook under discussion, this byte can be used to indicate those.

For the current version of the phone book, the phone book entry is identified as follows:

- the record number in the EF_{PBR} which indicates the EF_{ADN} containing the entry;
- the record number inside the indicated EF_{ADN}.

The structure of EF_{ICI} is shown below. Coding scheme is according to EF_{ADN}

Structure of EF_{ICI}

Identifier: '6F80'	Structure: Cyclic	Optional
SFI: '14'		
Record length: X+28 bytes	Update activity: high	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to X	Alpha Identifier	O	X bytes
X+1	Length of BCD number contents	M	1 byte
X+2	TON and NPI	M	1 byte
X+3 to X+12	Incoming Call Number	M	10 bytes
X+13	Capability/Configuration2 Identifier	M	1 byte
X+14	Extension5 Record Identifier	M	1 byte
X+15 to X+21	Incoming call date and time (see detail 1)	M	7 bytes
X+22 to X+24	Incoming call duration (see detail 2)	M	3 bytes
X+25	Incoming call status (see detail 3)	M	1 byte
X+26 to X+28	Link to phone book entry (see detail 4)	M	3 bytes

NOTE: When the contents except incoming call status are invalid, they are filled with 'FF'.

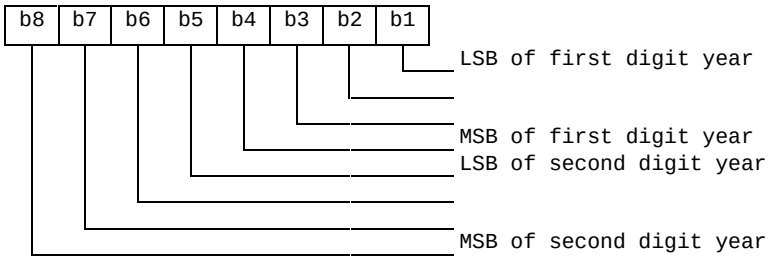
Detail 1 Coding of date and time.

Content:

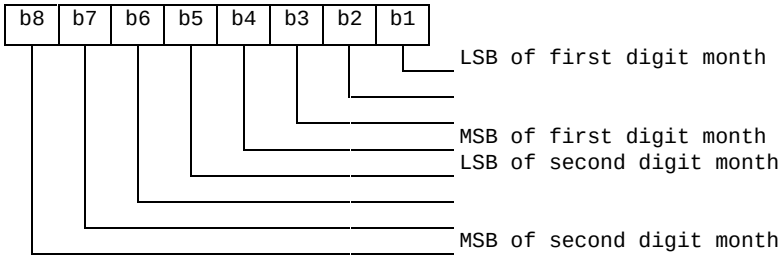
the date and time are defined by the ME.

Coding:

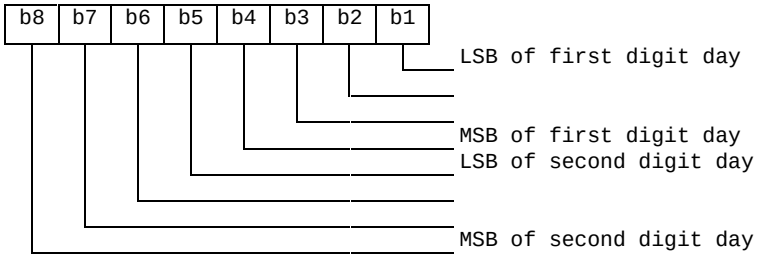
it is according to the extended BCD coding from Byte1 to Byte 7. The first 3 bytes show year, month and day (yy.mm.dd). The next 3 bytes show hour, minute and second (hh.mm.ss). The last Byte 7 is Time Zone. The Time Zone indicates the difference, expressed in quarters of an hour, between the local time and GMT. Bit 4 in Byte 7 represents the algebraic sign of this difference (0: positive, 1: negative). If the terminal does not support the Time Zone, Byte 7 shall be "FF". Byte X+15: Year.



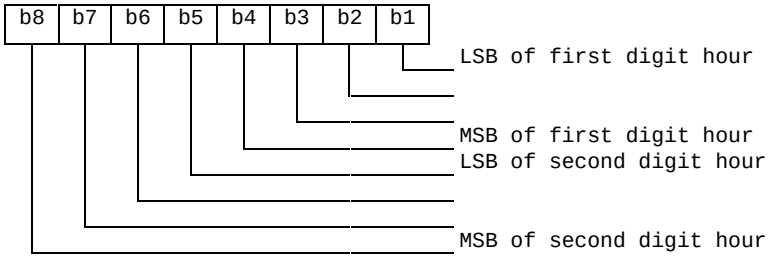
Byte X+16: Month



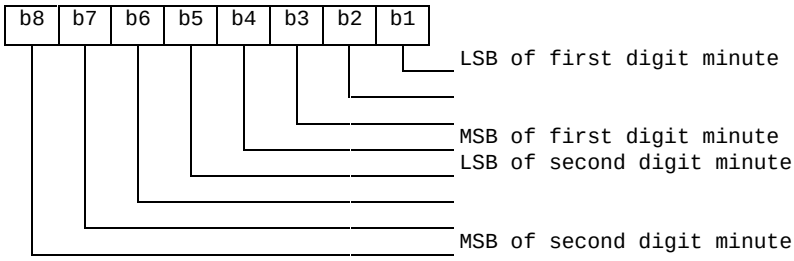
Byte X+17: Day



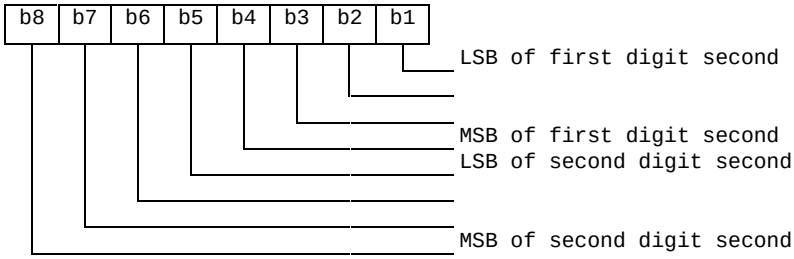
Byte X+18: Hour



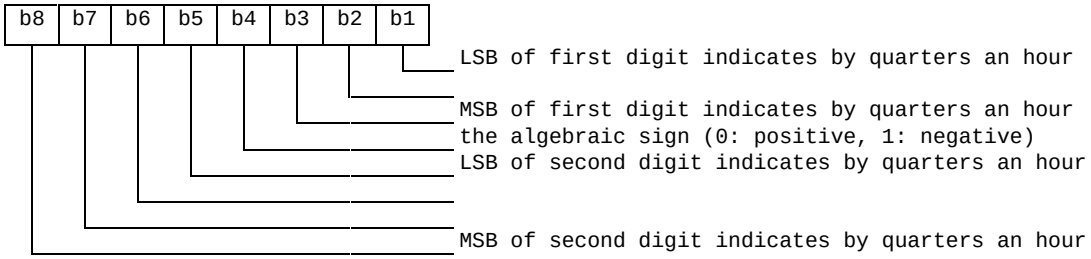
Byte X+19: Minute



Byte X+20: Second



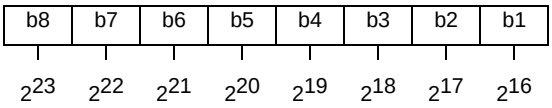
Byte X+21: Time Zone



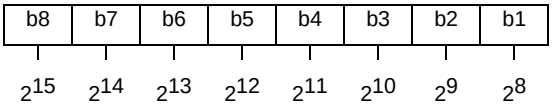
Detail 2 Coding of call duration.

Call duration is indicated by second.

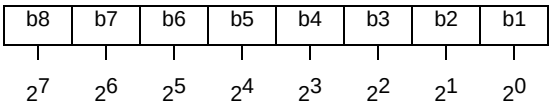
Byte X+22:



Byte X+23:



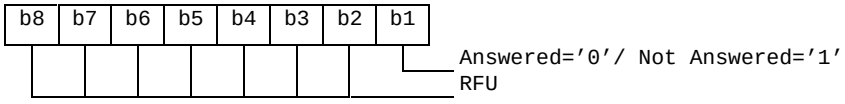
Byte X+24:



For instance, '00' '00' '30' represents 2^5+2^4.

Detail 3 Coding of Call status.

Byte X+25:

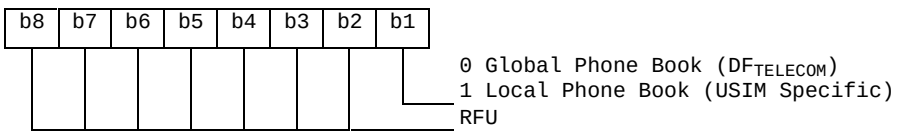


Detail 4 Link to phone book entry

For the current implementation of the phone book the following coding applies:

Phone book reference.

Byte X+26:



EF_{PBR} record number:

- Byte X+27: Hexadecimal value.

- EF_{ADN} record number:
  - Byte X+28: Hexadecimal value.

4.2.34 EF_{OCI} (Outgoing Call Information)

This EF is located within the USIM application. The outgoing call information can be linked to the phone book stored under $DF_{TELECOM}$ or to the local phone book within the USIM. The EF_{OCI} contains the information related to outgoing calls.

The time of the call and duration of the call are stored in this EF. It may also contain associated alpha identifier. In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records at the USIM ADF level. The structure of this file is cyclic, so the contents shall be updated only after a call is disconnected.

If the dialled phone number matches a number stored in the phone book the outgoing call information might be linked to the corresponding information in the phone book. The dialled number may match with a hidden entry in the phone book. If the dialled number matches a hidden entry in the phone book the link is established but the information related to the phone book entry is not displayed by the ME, if the hidden code has not been verified. The ME shall not perform hidden code verification at this point.

Optionally, the ME may store the link to phone book entry in the file, so that it does not need to look again for a match in the phone book when it reuses the entry. But the ME will have to check that the outgoing call number still exists in the linked phone book entry, as the link might be broken (entry modified). When not used by the ME or no link to the phone book has been found, this field shall be set to 'FFFFFF'.

Coding scheme is according to EF_{ICI}.

Structure of EF_{OCI}

Identifier: '6F81'	Structure: Cyclic	Optional
SFI: '15'		
Record length: X+27 bytes	Update activity: high	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	Alpha Identifier	O	X bytes
X+1	Length of BCD number/SSC contents	M	1 byte
X+2	TON and NPI	M	1 byte
X+3 to X+12	Outgoing Call Number/SSC String	M	10 bytes
X+13	Capability/Configuration2 Identifier	M	1 byte
X+14	Extension5 Record Identifier	M	1 byte
X+15 to X+21	Outgoing call date and time	M	7 bytes
X+22 to X+24	Outgoing call duration	M	3 bytes
X+25 to X+27	Link to Phone Book Entry	M	3 bytes

NOTE: When the contents are invalid, they are filled with 'FF'.

4.2.35 EF_{ICT} (Incoming Call Timer)

This EF contains the accumulated incoming call timer duration value for the current call and previous calls. The EF is USIM specific and resides within the USIM application.

Structure of EF_{ICT}

Identifier: '6F82'	Structure: cyclic	Optional
Record length: 3 bytes	Update activity: high	

Access Conditions:

READ	PIN
UPDATE	PIN/PIN2 (fixed during administrative management)
INCREASE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 3	Accumulated call timer value	M	3 bytes

Coding:

Accumulated call timer value is indicated by second.

Byte 1:

b8	b7	b6	b5	b4	b3	b2	b1
2^{23}	2^{22}	2^{21}	2^{20}	2^{19}	2^{18}	2^{17}	2^{16}

Byte 2:

b8	b7	b6	b5	b4	b3	b2	b1
2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^{9}	2^{8}

Byte 3:

b8	b7	b6	b5	b4	b3	b2	b1
2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}

For example, '00' '00' '30' represents 2^5+2^4.

4.2.36 EF_{OCT} (Outgoing Call Timer)

This EF contains the accumulated outgoing call timer duration value for the current call and previous calls. The EF is USIM specific and resides within the USIM application. The contents of this EF shall be updated only after a call is disconnected. The coding of this EF is the same as EF_{ICT}.

Structure of EF_{OCT}

Identifier: '6F83'	Structure: cyclic	Optional
Record length: 3 bytes	Update activity: high	

Access Conditions:

READ	PIN
UPDATE	PIN/PIN2 (fixed during administrative management)
INCREASE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 3	Accumulated call timer value	M	3 bytes

4.2.37 EF_{EXT5} (Extension5)

This EF contains extension data of EF_{ICI}, EF_{OCI} and EF_{MSISDN} of the USIM application.

Identifier: '6F4E'	Structure: linear fixed	Optional
Record length: 13 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Record type	M	1 byte
2 to 12	Extension data	M	11 bytes
13	Identifier	M	1 byte

For contents and coding see EF_{EXT1}.

4.2.38 EF_{CCP2} (Capability Configuration Parameters 2)

This EF contains parameters of required network and bearer capabilities and terminal configurations associated with a call established using a fixed dialling number, an MSISDN, a service dialling number, an incoming call or an outgoing call. It is referred by EF_{FDN}, EF_{MSISDN}, EF_{SDN}, EF_{ICI} and EF_{OCI} at USIM ADF level.

Identifier: '6F4F'	Structure: linear fixed	Optional
SFI: '16'		
Record length: X bytes, X≥15	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	Bearer capability information element	M	X bytes

- Bearer capability information elements.
  - Contents and Coding:
    - see 3G TS 24.008 [9]. The Information Element Identity (IEI) shall be excluded, i.e. the first byte of the EF_{CCP2} record shall be Length of the bearer capability contents.

- unused bytes are filled with 'FF'.

4.2.39 EF_{eMLPP} (enhanced Multi Level Precedence and Pre-emption)

This EF contains information about priority levels and fast call set-up conditions for the enhanced Multi Level Precedence and Pre-emption service that can be used by the subscriber.

Identifier: '6FB5'	Structure: transparent	Optional
File size: 2 bytes	Update activity: low	

Access Conditions:

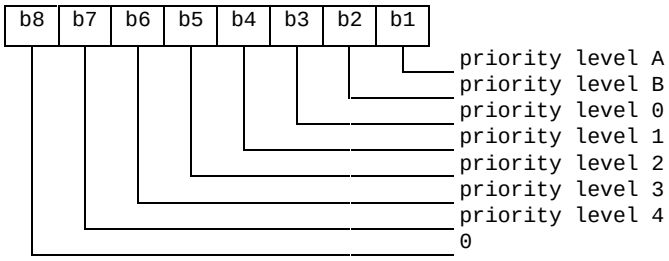
READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Priority levels	M	1 byte
2	Fast call set-up conditions	M	1 byte

- Priority levels.
  Contents:
  - the eMLPP priority levels subscribed to.

  Coding:
  - each eMLPP priority level is coded on one bit. Priority levels subscribed to have their corresponding bits set to 1. Priority levels not subscribed to have their corresponding bits set to 0. Bit b8 is reserved and set to 0.

Byte 1:



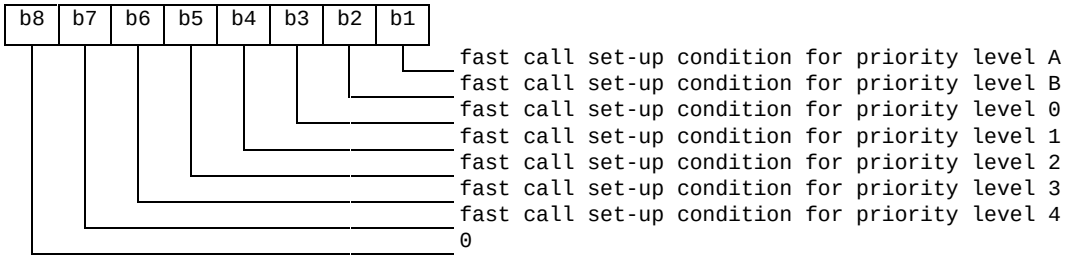
NOTE: Priority levels A and B can not be subscribed to (see 3G TS 22.067 [5] for details).

EXAMPLE 1: If priority levels 0, 1 and 2 are subscribed to, EF_{eMLPP} shall be coded '1C'.

- Fast call set-up conditions.
  Contents:
  for each eMLPP priority level, the capability to use a fast call set-up procedure.
  Coding:
  each eMLPP priority level is coded on one bit. Priority levels for which fast call set-up is allowed have their corresponding bits set to 1. Priority levels for which fast call set-up is not allowed have their corresponding bits set to 0. Bit b8 is reserved and set to 0.

Byte 2: fast call set-up condition for:

‘



EXAMPLE 2: If fast call set-up is allowed for priority levels 0, and 1, then byte 2 of EF_{eMLPP} is coded '0C'.

4.2.40 EF_{AAeM} (Automatic Answer for eMLPP Service)

This EF contains those priority levels (of the Multi Level Precedence and Pre-emption service) for which the ME shall answer automatically to incoming calls.

Identifier: '6FB6'	Structure: transparent	Optional
File size: 1 byte	Update activity: low	

Access Conditions:

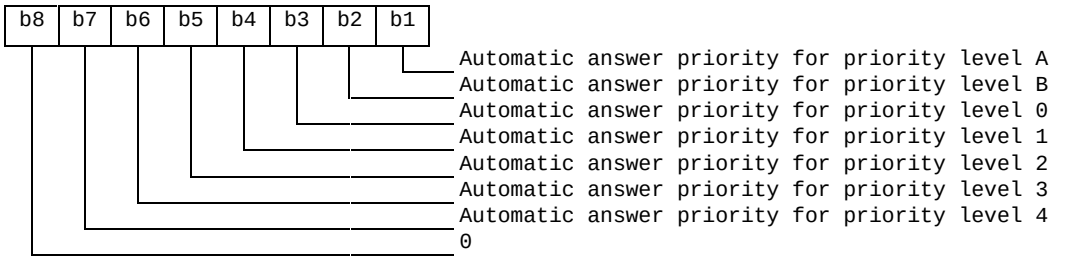
READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Automatic answer priority levels	M	1 byte

- Automatic answer priority levels.
  Contents:
  - for each eMLPP priority level, the capability for the mobile station to answer automatically to incoming calls (with the corresponding eMLPP priority level).

  Coding:
  - each eMLPP priority level is coded on one bit. Priority levels allowing an automatic answer from the mobile station have their corresponding bits set to 1. Priority levels not allowing an automatic answer from the mobile station have their corresponding bits set to 0. Bit b8 is reserved and set to 0.

Byte 1:



EXAMPLE: If automatic answer is allowed for incoming calls with priority levels A, 0 and 1, then EF_{AAeM} is coded '0D'.

4.2.41 EF_{GMSI} (Group Identity)

This subclause is expected to be defined in the release 2000 version of the present document.

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

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

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

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

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

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

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

4.2.43 void

4.2.44 EF_{BDN} (Barred Dialling Numbers)

This EF contains Barred Dialling Numbers (BDN) and/or Supplementary Service Control strings (SSC). In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records. It may also contain an associated alpha-tagging. As the BDN service relies on the Call Control feature, BDN shall only be available if Call Control is available. If this file is present in the USIM, the Enabled Services Table (EF_{EST}) shall also be present.

Identifier: '6F4D'	Structure: linear fixed	Optional
Record length: X+15 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN2
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	Alpha Identifier	O	X bytes
X+1	Length of BCD number/SSC contents	M	1 byte
X+2	TON and NPI	M	1 byte
X+3 to X+12	Dialling Number/SSC String	M	10 bytes
X+13	Capability/Configuration Identifier	M	1 byte
X+14	Extension4 Record Identifier	M	1 byte
X+15	Comparison Method Pointer	M	1 byte

For contents and coding of all data items, except for the Comparison Method Pointer, see the respective data items of EF_{ADN}, with the exception that extension records are stored in the EF_{EXT4}. The Comparison Method Pointer refers to a record number in EF_{CMI}.

NOTE: The value of X (the number of bytes in the alpha-identifier) may be different to the length denoted X in EF_{ADN}.

4.2.45 EF_{EXT4} (Extension4)

This EF contains extension data of a BDN/SSC.

Identifier: '6F55'	Structure: linear fixed	Optional
Record length: 13 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN2
DEACTIVE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Record type	M	1 byte
2 to 12	Extension data	M	11 bytes
13	Identifier	M	1 byte

For contents and coding see subclause 4.4.2.4 EF_{EXT1}.

4.2.46 EF_{CMI} (Comparison Method Information)

This EF contains the list of Comparison Method Identifiers and alpha-tagging associated with BDN entries (see EF_{BDN}). This EF shall be present if EF_{BDN} is present.

Identifier: '6F58'	Structure: linear fixed	Optional
Record length: X+1 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Comparison Method Identifier	M	1 byte
2 to X+1	Alpha Identifier	M	X bytes

- Alpha Identifier.
  Contents:
  Alpha-tagging of the associated Comparison Method Identifier.
  Coding:
  Same as the alpha identifier in EF_{ADN}.
- Comparison Method Identifier.
  Contents:
  - this byte describes the comparison method which is associated with a BDN record. Its interpretation is not specified but it shall be defined by the card issuers implementing the BDN feature on their USIMs.

  Coding:
  - binary; values from 0 to 255 are allowed.
    The default coding 255 is reserved for empty field.

4.2.47 EF_{EST} (Enabled Services Table)

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

Identifier: '6F56'	Structure: transparent	Optional
SFI: '05'		
File size: X bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN2
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Services n°1 to n°8	M	1 byte
2	Services n°9 to n°16	O	1 byte
etc.			
X	Services n°(8X-7) to n°(8X)	O	1 byte

-Services

Contents:

Service n°1 : Fixed Dialling Numbers (FDN)

Service n°2 : Barred Dialling Numbers (BDN)

Service n°3 : APN Control List (ACL)

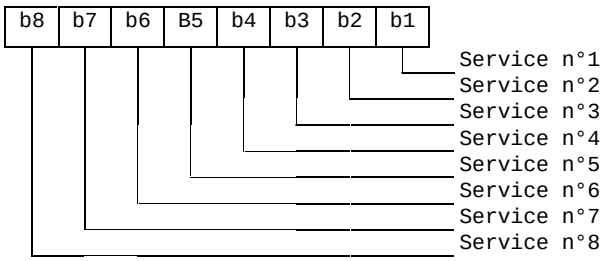
The EF shall contain at least one byte. Further bytes may be included, but if the EF includes an optional byte, then the EF shall also contain all bytes before that byte. Other services are possible in the future. The coding falls under the responsibility of the 3GPP.

Coding:

- 1 bit is used to code each service:
  - bit = 1: service activated;
  - bit = 0: service deactivated.
- Unused bits shall be set to '0'.

A service which is listed in this table is enabled if it is indicated as available in the USIM Service Table (UST) and indicated as activated in the Enabled Services Tables (EST) otherwise this service is, either not available or disabled.

First byte:



etc.

4.2.48 EF_{ACL} (Access Point Name Control List)

This EF contains the list of allowed APNs (Access Point Names). If this file is present in the USIM, the Enabled Services Table (EF_{EST}) shall also be present.

Identifier: '6F57'	Structure: transparent	Optional
File size: X bytes (X>1)	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN2
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Number of APNs	M	1 byte
2 to X	APN TLVs	M	X-1 byte

For contents and coding of APN-TLV values see TS 23.003 [25]. The tag value of the APN-TLV shall be 'DD'. "Network provided APN" is coded with a TLV object of length zero.

4.2.49 EF_{DCK} (Depersonalisation Control Keys)

This EF provides storage for the de-personalization control keys associated with the OTA de-personalization cycle of TS 22.022 [27].

Identifier: '6F2C'	Structure: transparent	Optional
File Size: 16 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 4	8 digits of network de-personalization control key	M	4 bytes
5 to 8	8 digits of network subset de-personalization control key	M	4 bytes
9 to 12	8 digits of service provider de-personalization control key	M	4 bytes
13 to 16	8 digits of corporate de-personalization control key	M	4 bytes

Empty control key bytes shall be coded 'FFFFFFFF'.

4.2.50 EF_{CNL} (Co-operative Network List)

This EF contains the Co-operative Network List for the multiple network personalization services defined in TS 22.022 [27].

Identifier: '6F32'	Structure: transparent	Optional
File size: 6n bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 6	Element 1 of co-operative net list	M	6 bytes
6n-5 to 6n	Element n of co-operative net list	O	6 bytes

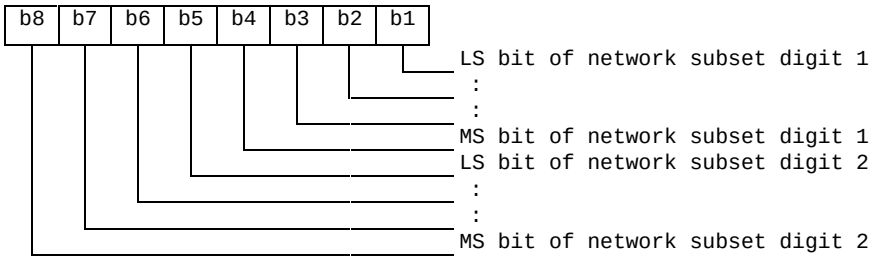
- Co-operative Network List.

  Contents:
  - PLMN network subset, service provider ID and corporate ID of co-operative networks.

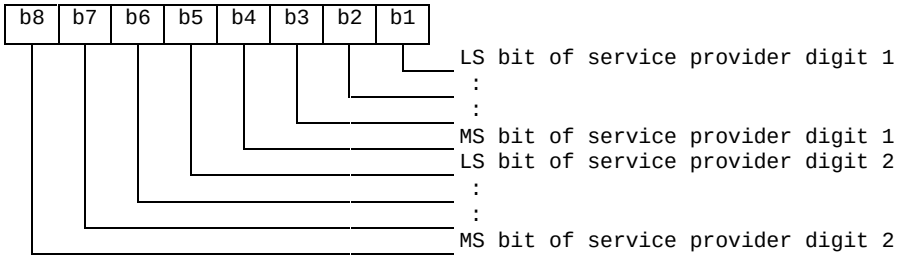
  Coding:
  - For each 6 byte list element.

Bytes 1 to 3 : PLMN (MCC + MNC): according to 3G TS 24.008 [9].

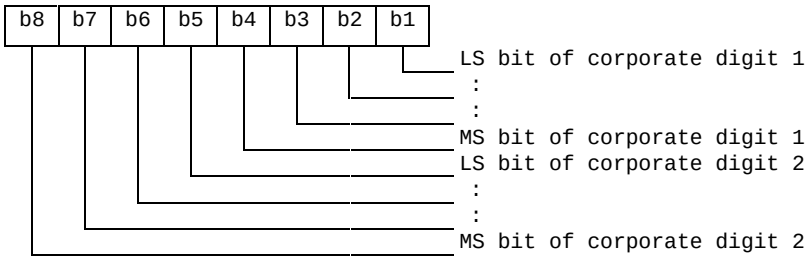
Byte 4:



Byte 5:



Byte 6:



- Empty fields shall be coded with 'FF'.
- The end of the list is delimited by the first MCC field coded 'FFF'.

4.2.51 $EF_{START-HFN}$ (Initialisation values for Hyperframe number)

This EF contains the values of $START_{CS}$ and $START_{PS}$ of the bearers that were protected by the keys in EF_{KEYS} or EF_{KEYSPS} at release of the last CS or PS RRC connection. These values are used to control the lifetime of the keys (see 3G TS 33.102 [13]).

Identifier: '6F5B'	Structure: transparent	Mandatory
SFI: '0F'		
File size: 6 bytes	Update activity: high	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to 3	$START_{CS}$	M	3 bytes
4 to 6	$START_{PS}$	M	3 bytes

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

- $START_{PS}$
  Contents: Initialisation value for Hyperframe number – PS domain.
  Coding: As for $EF_{START-CS}$.

4.2.52 $EF_{THRESHOLD}$ (Maximum value of START)

This EF contains the maximum value of $START_{CS}$ or $START_{PS}$. This value is used to control the lifetime of the keys (see 3G TS 33.102 [13]).

Identifier: '6F5C'	Structure: transparent	Mandatory
SFI: '10'		
File size: 3 bytes	Update activity: low	
Access Conditions: READ PIN UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to 3	Maximum value of $START_{CS}$ or $START_{PS}$.	M	3 bytes

- Maximum value of $START_{CS}$ or $START_{PS}$.
  Coding: As for $EF_{START-CS}$.

4.2.53 $EF_{OPLMNwACT}$ (Operator controlled PLMN selector with Access Technology)

This EF contains the coding for n PLMNs where n is determined by the operator. This information is determined by the operator and defines the preferred PLMNs in priority order. The first record indicates the highest priority and the n^{th} record indicates the lowest. The EF also contains the Access Technologies for each PLMN in this list. (see TS 23.122 [31])

Identifier: '6F61'	Structure: transparent	Optional
SFI: '11'		
File size: 5n (where n ≥8 bytes)	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 3	1st PLMN (highest priority)	M	3 bytes
4 to 5	1st PLMN Access Technology Identifier	M	2 bytes
6 to 8	2nd PLMN	O	3 bytes
9 to 10	2nd PLMN Access Technology Identifier	O	2 bytes
(5n-4) to (5n-2)	Nth PLMN (lowest priority)	O	3 bytes
(5n-1) to 5n	Nth PLMN Access Technology Identifier	O	2 bytes

- PLMN.
  Contents:
  - Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).
  Coding:
  - according to 3G TS 24.008 [9].
- Access Technology Identifier:
  Coding:
  - See $EF_{PLMNwACT}$ for coding.

4.2.54 $EF_{HPLMNwAcT}$ (HPLMN selector with Access Technology)

The HPLMN Selector with access technology data field shall contain the HPLMN code, or codes together with the respected access technology in priority order (see TS 23.122 [31]).

Identifier: '6F62'	Structure: Transparent	Optional
SFI: '13'		
File size: 5n bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 3	1st PLMN (highest priority)	M	3 bytes
4 to 5	1st PLMN Access Technology Identifier	M	2 bytes
6 to 8	2nd PLMN	O	3 bytes
9 to 10	2nd PLMN Access Technology Identifier	O	2 bytes
:	:		
(5n-4) to (5n-2)	nth PLMN (lowest priority)	O	3 bytes
(5n-1) to 5n	nth PLMN Access Technology Identifier	O	2 bytes

- PLMN
  Contents:
  Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).
  Coding:
  according to TS 24.008 [47].

- Access Technology:
  Contents: The Access Technology of the HPLMN that the ME will assume when searching for the HPLMN, in priority order. The first Access Technology in the list has the highest priority.

  Coding:
  - See $EF_{PLMNwACT}$ for coding.

4.2.55 EF_{ARR} (Access Rule Reference)

This EF contains the access rules for files located under the USIM ADF in the UICC. If the security attribute tag '8B' is indicated in the FCP it contains a reference to a record in this file.

Structure of EF_{ARR} at ADF-level

Identifier: '6F06'	Structure: Linear fixed		Mandatory
SFI: '17'			
Record Length: X bytes		Update activity: low	
Access Conditions: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM			
Bytes	Description	M/O	Length
1 to X	Access Rule TLV data objects	M	X bytes

This EF contains one or more records containing access rule information according to the reference to expanded format as defined in ISO/IEC 7816-9 [26]. Each record represents an access rule. Unused bytes in the record are set to 'FF'.

If the card cannot access EF_{ARR} , any attempt to access a file with access rules indicated in this EF_{ARR} shall not be granted.

4.2.56 $EF_{RPLMNACT}$ (RPLMN Last used Access Technology)

This EF contains the last used access technology for the Registered PLMN, RPLMN. (see TS 23.122 [31]). This EF shall contain only one access technology.

NOTE: One access technology means that only one bit is set in the entire field.

Identifier: '6F65'	Structure: transparent		Mandatory
SFI: '18'			
File size: 2+X bytes		Update activity: High	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM			
Bytes	Description	M/O	Length
1 to 2	Access Technology of RPLMN	M	2 bytes
3 to 2+X	RFU	O	X bytes

- Access Technology

  Coding:

  - See $EF_{PLMNselwACT}$ for coding.

4.2.57 EF_{NETPAR} (Network Parameters)

This EF contains information concerning the cell frequencies

Network Parameter storage may reduce the extent of the terminal search of FDD, TDD or GSM carriers when selecting a cell. The network parameters stored in the USIM shall be in accordance with the procedures specified in this paragraph.

The RF carrier frequency information is stored on 2 bytes and coded on 16 bits starting from 0,0 MHz. Each increment of the 16 bit value is an increment of 200 kHz in frequency. This allows the exact channel frequency to be stored in this data field making it independent of any band information. It is up to the terminal to associate the indicated frequency with a particular band, e.g. GSM 900, GSM 1800 etc. This means that a range from 0 to 13,1 GHz can be covered, with the resolution of 200 kHz. The frequency indicated is always the terminal receiver carrier frequency.

The EF provides a minimum storage capacity of 46 bytes in order to provide the capability of storing at least two cell information TLV objects, e.g. GSM/FDD or FDD/TDD in its minimum configuration, i.e. the terminal can rely on the required memory space for storing at least two cell information lists offering 8 GSM neighbour carrier frequencies and 8 Intra/Inter frequencies, respectively. In what configuration the available memory actually is being used is up to the terminal.

A terminal shall ignore a TLV object or the value of a carrier frequency which is beyond its capabilities, i.e an FDD only terminal shall ignore the GSM related frequency information. When updating this file, the terminal shall update it with the current values available in the terminal. Updating of this file shall start from the beginning of the file. The terminal need not respect the structure of any information previously stored, i.e. an FDD only terminal may overwrite the GSM parameters stored in this file by another terminal.

The GSM cell information constructed TLV object contains the information of the BCCH channel frequency that the terminal is currently camped on, indicated by tag '80'. The constructed TLV object also contains an indication of up to 32 neighbour BCCH carrier frequencies indicated by tag '81'. In order to store a complete set of GSM network parameters, a total of 72 bytes is required. The terminal shall convert the BCCH channel information, as specified in GSM 04.18 [28], received from the network into the corresponding frequency before storing it in the USIM.

The FDD cell information constructed TLV object contains the scrambling code information for the intra frequency carrier, tag '80', and the inter frequency scrambling codes, tag '81'. The intra frequency carrier information may contain up to 32 scrambling codes (m) while there is a limitation of the number of inter frequency scrambling codes (n1, n2, n3). The number of inter frequencies that can be indicated is limited to three and the total amount of scrambling codes for the inter frequencies is limited to 32 (n1+n2+n3 <= 32), i.e. if only one inter frequency carrier is indicated, it can contain up to 32 scrambling codes. If two or more inter frequency carriers are indicated, a total of 32 scrambling codes can be provided. How the information is split between the inter frequency carriers is determined by the terminal. In order to store a complete set of FDD cell information a total of 146 bytes is required. The terminal shall convert the UARFCN information, as specified in 25.101 [33], received from the network into the corresponding frequency before storing it in the USIM.

The TDD cell information constructed TLV object has the same structure as the FDD cell information TLV object.

NOTE: Currently there is no inter frequency cell information required for the TDD case.

Identifier: '6FC4'	Structure: transparent	Mandatory
File size: X >= 46 bytes	Update activity: high	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 - X	TLV object(s) containing GSM/FDD/TDD cell information	O	

- EF_{NETPAR} Cell Information tags

Description	Value	Information Element size bytes
GSM Cell Information Tag	'A0'	1
Camping Frequency Tag	'80'	1
Camping Frequency Information		2
Neighbour Frequency Tag	'81'	1
Neighbour Frequency Information		2*m (8 <= m <= 32)
FDD Cell Information Tag	'A1'	1
Intra Frequency Information Tag	'80'	1
Scrambling code Information		2*m (8 <= m <= 32)
Inter Frequency Information Tag	'81'	1
Scrambling code information		2*(n1+n2+n3) (8 <= n1+n2+n3 <= 32)
TDD Frequency information Tag	'A2'	1
Intra Frequency Information Tag	'80'	1
Cell parameters ID		2*m (8 <= m <= 32)
Inter Frequency Information Tag	'81'	1
Cell parameters ID		2*(n1+n2+n3) (8 <= n1+n2+n3 <= 32)

- GSM Cell Information, if tag 'A0' is present in this EF the content of this TLV is as follows:

Description	Value	M/O	Length
GSM Cell Information Tag	'A0''	M	1
Length	'4+ (2+2*m) (<=70) '	M	1
Current camped cell BCCH frequency information tag	'80'	M	1
Length	'02'	M	1
Current camped BCCH frequency		M	2
Neighbour Cell BCCH Frequency information tag	'81'	O	1
Length	2*m (=< 32)	O	1
Neighbour BCCH carrier frequencies		O	2*m (8 <= m <= 32)

- - FDD Cell Information. If tag 'A1' is present in this EF the content of this TLV is as follows:

Description	Value	M/O	Length
FDD Cell Information Tag	'A1'	M	1
Length	4+(2*m)+(4+2*n 1)+(4+2*n2)+(4+ 2*n3) (<=144)	M	1
FDD Intra Frequency information tag	'80'	M	1
Length	2+2*m	M	1
Intra Frequency carrier frequency		M	2
Intra Frequency scrambling codes		M	2*m (8 <= m <= 32)
FDD Inter Frequency information tag (see NOTE 1)	'81'	O	1
Length	2+2*n (NOTE 2)	O	1
Inter Frequency carrier frequencies		O	2
Inter Frequency scrambling codes		O	2*n (NOTE 2)
NOTE 1: This TLV object may occur up to 3 times within the constructed TLV object depending how many inter frequencies are indicated NOTE 2: n is in this case n1, n2 or n3, 8 <= (n1+n2+n2)<=32			

- TDD Cell Information: If tag 'A2' is present in this EF the content of this TLV is as follows:

Description	Value	M/O	Length
TDD Cell Information Tag	'A2'	M	1
Length	4+(2*m)+(4+2*n 1)+(4+2*n2)+(4+ 2*n3) (<=144)	M	1
TDD Intra Frequency information tag	'80'	M	1
Length	2+2*m	M	1
Intra Frequency carrier frequency		M	2
Intra Frequency scrambling codes		M	2*m (8 <= m <= 32)
TDD Inter Frequency information tag (see NOTE 1)	'81'	O	1
Length	2+2*n (NOTE 2)	O	1
Inter Frequency carrier frequencies		O	2
Inter Frequency scrambling codes		O	2*n (NOTE 2)
NOTE 1: This TLV object may occur up to 3 times within the constructed TLV object depending how many inter frequencies are indicated NOTE 2: n is in this case n1, n2 or n3, 8 <= (n1+n2+n2)<=32			

4.3 DFs at the USIM ADF (Application DF) Level

DFs may be present as child directories of USIM ADF. The following DFs are defined:

- $DF_{PHONEBOOK}$ '5F3A'.
- DF_{GSM} '5F3B'.
- DF_{MExE} '5F3C'.

(DF for application specific phonebook. This DF has the same structure as the $DF_{PHONEBOOK}$ under $DF_{TELECOM}$).

'5F70' is reserved for DF_{SoLSA} and is expected to be defined in the release 2000 version of the present document.

4.4 Contents of DFs at the USIM ADF (Application DF) level

4.4.1 Contents of files at the DF SoLSA level

This subclause is expected to be defined in the release 2000 version of the present document.

4.4.1.1 EF_{SAI} (SoLSA Access Indicator)

This subclause is expected to be defined in the release 2000 version of the present document.

4.4.1.2 EF_{SLL} (SoLSA LSA List)

This subclause is expected to be defined in the release 2000 version of the present document.

4.4.1.3 LSA Descriptor files

This subclause is expected to be defined in the release 2000 version of the present document.

4.4.2 Contents of files at the DF PHONEBOOK level

The UICC may contain a global phonebook, or application specific phonebooks, or both in parallel. When both phonebook types co-exist, they are independent and no data is shared. In this case, it shall be possible for the user to select which phonebook the user would like to access.

The global phonebook is located in $DF_{PHONEBOOK}$ under $DF_{TELECOM.}$. Each specific USIM application phonebook is located in $DF_{PHONEBOOK}$ of its respective Application DF_{USIM}. The organisation of files in $DF_{PHONEBOOK}$ under DF_{USIM} and under DF $_{TELECOM}$ follows the same rules. Yet $DF_{PHONEBOOK}$ under DF_{USIM} may contain a different set of files than $DF_{PHONEBOOK}$ under $DF_{TELECOM}$. All phonebook related EFs are located under their respective $DF_{PHONEBOOK}$. USIM specific phonebooks are dedicated to application specific entries. Each application specific phonebook is protected by the application PIN.

If a GSM application resides on the UICC, the EFs ADN and EXT1 from one $DF_{PHONEBOOK}$ (defined at GSM application installation) are mapped to $DF_{TELECOM}$. Their file IDs are specified in GSM 11.11 [18], i.e. EF_{ADN} = '6F3A' and EF_{EXT1} = '6F4A', respectively. EF_{ADN} and EF_{PBR} shall always be present if the $DF_{Phonebook}$ is present. If any phonebook file other than EF_{ADN} or $EF_{EXT1,}$ is used, then EF_{PBC} shall be present.

If the UICC is inserted into a GSM terminal and a record in the phonebook has been updated, a flag in the entry control information in the EF_{PBC} is set from 0 to 1 by the card. If the UICC is later inserted into a 3G terminal again, the terminal shall check the flag in EF_{PBC} and if this flag is set, shall update the EF_{CC}, and then reset the flag. A set flag in EF_{PBC} results in a full synchronisation of the phonebook between an external entity and the UICC (if synchronisation is requested).

The EF structure related to the public phonebook is located under $DF_{PHONEBOOK}$ in $DF_{TELECOM}$. A USIM specific phonebook may exist for application specific entries. The application specific phonebook is protected by the application PIN. The organisation of files in the application specific phonebook follows the same rules as the one specified for the public phone book under $DF_{TELECOM}$. The application specific phonebook may contain a different set of files than the one in the public area under $DF_{TELECOM}$.

4.4.2.1 EF_{PBR} (Phone Book Reference file)

This file describes the structure of the phonebook. All EFs representing the phonebook are specified here, together with their file identifiers (FID) and their short file identifiers (SFI), if applicable.

Some types of EFs can occur more than once in the phonebook, e.g. there may be two entities of Abbreviated Dialling Numbers, EF_{ADN} and EF_{ADN1}. For these kinds of EFs, no fixed FID values are specified. Instead, the value '4FXX' indicates that the value is to be assigned by the card issuer. These assigned values are then indicated in the associated TLV object in EF_{PBR}.

EFs stating an SFI value ('XX') in the description of their structure shall provide an SFI. The value shall be assigned by the card issuer and is indicated in the associated TLV object in EF_{PBR}.

The reference file is a file that contains information how the information in the different files is to be combined together to form a phone book entry. The reference file contains records. Each record specifies the structure of up to 254 entries in the phone book. Each phone book entry consists of data stored in files indicated in the reference file record. The entry structure shall be the same over all the records in the EF $_{PBR}$. If more than 254 entries are to be stored, a second record is needed in the reference file. The structure of a phone book entry is defined by different TLV objects that are

stored in a reference file record. The reference file record structure describes the way a record in a file that is part of the phonebook is used to create a complete entry. Three different types of file linking exist.

- Type 1 files: Files that contain as many records as the reference/master file (EF_{ADN}, EF_{ADN1}) and are linked on record number bases (Rec1 -> Rec1). The master file record number is the reference.

- Type 2 files: Files that contain less entries than the master file and are linked via pointers in the index administration file (EF_{IAP}).

- Type 3 files are files that are linked by a record identifier within a record.

Table 4.1: Phone Book Reference file Constructed Tags

Tag Value	Constructed TAG Description
'A8'	Indicating files where the amount of records equal to master EF, type 1
'A9'	Indicating files that are linked using the index administration file, type 2. Order of pointer appearance in index administration EF is the same as the order of file IDs following this tag
'AA'	Indicating files that are addressed inside a TLV object, type 3. (The file pointed to is defined by the TLV object.)

The first file ID indicated using constructed Tag 'A8' is called the master EF. Access conditions for all other files in the index structure is set to the same as for the master EF unless otherwise specified.

File IDs indicated using constructed Tag 'A8' is a type 1 file and contains the same number of records as the first file that is indicated in the data part of this TLV object. All files following this Tag are mapped one to one using the record numbers/IDs of the first file indicated in this TLV object.

File IDs indicated using constructed Tag 'A9' are mapped to the master EF (the file ID indicated as the first data object in the TLV object using Tag 'A8') using the pointers in the index administration file. The order of the pointers in the index administration file is the same as the order of the file IDs presented after Tag 'A9'. If this Tag is not present in the reference file record the index administration file is not present in the structure. In case the index administration file is not present in the structure it is not indicated in the data following tag 'A8'.

File IDs indicated using constructed Tag 'AA' indicate files that are part of the reference structure but they are addressed using TLV objects in one or more of the files that are part of the reference structure. The length of the tag indicates whether the file to be addressed resides in the same directory or if a path to the file is provided in the TLV object.

Type 2 and type 3 files contain records that may be shared between several phonebook entries (except when otherwise indicated). The terminal shall ensure that a shared record is emptied when the last phonebook entry referencing it is modified in such a way that it doesn't reference the record anymore.

NOTE: in the current version of the specification, only type 3 files contain records that may be shared.

Each constructed Tag contains a list of primitive Tags indicating the order and the type of data (e.g. ADN, IAP,…) of the reference structure.

The primitive tag identifies clearly the type of data, its value field indicates the file identifier and, if applicable, the SFI value of the specified EF. That is, the length value of a primitive tag indicates if an SFI value is available for the EF or not:

- Length = '02' Value: 'FID (2 bytes)'

- Length = '03' Value: 'FID (2 bytes)', 'SFI (1 byte)'

Table 4.2: Tag definitions for the phone book type of file

Tag Value	TAG Description
'C0'	EF_{ADN} data object
'C1'	EF_{IAP} data object
'C2'	EF_{EXT1} data object
'C3'	EF_{SNE} data object
'C4'	EF_{ANR} data object
'C5'	EF_{PBC} data object
'C6'	EF_{GRP} data object
'C7'	EF_{AAS} data object
'C8'	EF_{GAS} data object
'C9'	EF_{UID} data object
'CA'	EF_{EMAIL} data object
'CB'	EF_{CCP1} data object

Table 4.3 (below) lists the allowed types for each file

Table 4.3: Presence of files as type

File name	Type 1	Type 2	Type 3
EF_{AAS}			X
EF_{ADN}	X		
EF_{ANR}	X	X	
EF_{EMAIL}	X	X	
EF_{EXT1}			X
EF_{GAS}			X
EF_{GRP}	X		
EF_{IAP}	X		
EF_{PBC}	X		
EF_{SNE}	X	X	
EF_{UID}	X		
EF_{CCP1}			X

Phone Book Reference file EF_{PBR} structure

Identifier: '4F30'	Structure: linear fixed		Conditional (see Note)
Record Length: X bytes		Update activity: low	
Access Conditions: READ PIN UPDATE ADM DEACTIVATE ADM ACTIVATE ADM			
Bytes	Description	M/O	Length
1 to X	TLV object(s) for indicating EFs that are part of the phone book structure	M	X bytes
NOTE: This file is mandatory if and only if $DF_{Phonebook}$ is present.			

At the end of each record, unused bytes, if any, shall be filled with 'FF'.

4.4.2.2 EF_{IAP} (Index Administration Phone book)

This file is present if Tag 'A9' is indicated in the reference file.

The EF contains pointers to the different records in the files that are part of the phone book. The index administration file record number/ID is mapped one to one with the corresponding EF_{ADN} (shall be record to record). The index administration file contains the same amount of records as EF_{ADN}. The order of the pointers in an EF_{IAP} shall be the same as the order of file IDs that appear in the TLV object indicated by Tag 'A9' in the reference file record. The amount of bytes in a record is equal to the number of files indicated the EF_{PBR} following tag 'A9'.

The value 'FF' is an invalid record number/ID and is used in any location in to indicate that no corresponding record in the indicated file is available.

The content of EF_{IAP} is set to 'FF' at the personalisation stage.

Index administration file EF_{IAP} structure

Identifier: '4FXX'	Structure: linear fixed	Conditional (see Note)
SFI: 'XX'		
Record Length: X bytes	Update activity: high	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Record number of the first object indicated after Tag 'D9'	M	1 byte
2	Record number of the second object indicated after Tag 'D9'	M	1 byte
X	Record number of the x^{th} object indicated after Tag 'D9'	M	1 byte

NOTE: This file is mandatory if and only if type 2 files are present.

4.4.2.3 EF_{ADN} (Abbreviated dialling numbers)

This EF contains Abbreviated Dialling Numbers (ADN) and/or Supplementary Service Control strings (SSC). In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records. It may also contain an associated alpha-tagging.

Identifier: '4FXX'	Structure: linear fixed	Conditional (see Note)
SFI: 'XX'		
Record length: X+14 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	Alpha Identifier	O	X bytes
X+1	Length of BCD number/SSC contents	M	1 byte
X+2	TON and NPI	M	1 byte
X+3 to X+12	Dialling Number/SSC String	M	10 bytes
X+13	Capability/Configuration1 Identifier	M	1 byte
X+14	Extension1 Record Identifier	M	1 byte

NOTE: This file is mandatory if and only if $DF_{PHONEBOOK}$ is present.

- Alpha Identifier.
  Contents:
  - Alpha-tagging of the associated dialling number.

  Coding:
  - this alpha-tagging shall use
    either:
    - the SMS default 7-bit coded alphabet as defined in 3G TS 23.038 [5] with bit 8 set to 0. The alpha identifier shall be left justified. Unused bytes shall be set to 'FF'.

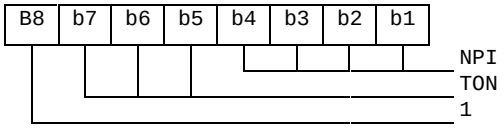
or:
- one of the UCS2 coded options as defined in the annex of 3G TS 31.101 [11].

NOTE 1: The value of X may be from zero to 241. Using the command GET RESPONSE the ME can determine the value of X.

- Length of BCD number/SSC contents.
  Contents:
  - this byte gives the number of bytes of the following two data items containing actual BCD number/SSC information. This means that the maximum value is 11, even when the actual ADN/SSC information length is greater than 11. When an ADN/SSC has extension, it is indicated by the extension1 identifier being unequal to 'FF'. The remainder is stored in the EF_{EXT1} with the remaining length of the additional data being coded in the appropriate additional record itself (see subclause 4.4.2.4).
  Coding:
  - according to 3G TS 24.008 [9].

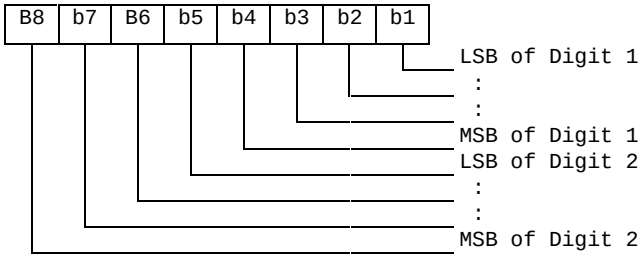
- TON and NPI.
  Contents:
  - Type of number (TON) and numbering plan identification (NPI).
  Coding:
  - according to 3G TS 24.008 [9]. If the Dialling Number/SSC String does not contain a dialling number, e.g. a control string deactivating a service, the TON/NPI byte shall be set to 'FF' by the ME (see note 2).

NOTE 2: If a dialling number is absent, no TON/NPI byte is transmitted over the radio interface (see 3G TS 24.008 [9]). Accordingly, the ME should not interpret the value 'FF' and not send it over the radio interface.

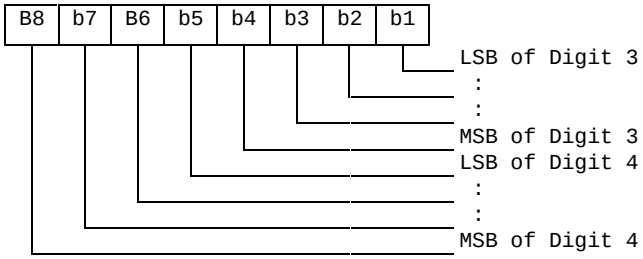


- Dialling Number/SSC String
  Contents:
  - up to 20 digits of the telephone number and/or SSC information.
  Coding:
  - according to 3G TS 24.008 [9] , 3G TS 22.030 [4] and the extended BCD-coding (see table 4.4). If the telephone number or SSC is longer than 20 digits, the first 20 digits are stored in this data item and the remainder is stored in an associated record in the EF_{EXT1}. The record is identified by the Extension1 Record Identifier. If ADN/SSC require less than 20 digits, excess nibbles at the end of the data item shall be set to 'F'. Where individual dialled numbers, in one or more records, of less than 20 digits share a common appended digit string the first digits are stored in this data item and the common digits stored in an associated record in the EF_{EXT1}. The record is identified by the Extension 1 Record Identifier. Excess nibbles at the end of the data item shall be set to 'F'.

Byte X+3



Byte X+4:



etc.

- Capability/Configuration1 Identifier.
  Contents:
  - capability/configuration identification byte. This byte identifies the number of a record in the EF_{CCP1} containing associated capability/configuration parameters required for the call. The use of this byte is optional. If it is not used it shall be set to 'FF'.

  Coding:
  - binary.

- Extension1 Record Identifier.
  Contents:
  - extension1 record identification byte. This byte identifies the number of a record in the EF_{EXT1} containing an associated called party subaddress or additional data. The use of this byte is optional. If it is not used it shall be set to 'FF'.
  - if the ADN/SSC requires both additional data and called party subaddress, this byte identifies the additional record. A chaining mechanism inside EF_{EXT1} identifies the record of the appropriate called party subaddress (see subclause 4.4.2.4).

  Coding:
  - binary.

NOTE 3: EF_{ADN} in the public phone book under $DF_{TELECOM}$ may be used by USIM, GSM and also other applications in a multi-application card. If the non-GSM application does not recognise the use of Type of Number (TON) and Number Plan Identification (NPI), then the information relating to the national dialling plan shall be held within the data item dialling number/SSC and the TON and NPI fields set to UNKNOWN. This format would be acceptable for 3G operation and also for the non-GSM application where the TON and NPI fields shall be ignored.

EXAMPLE: SIM storage of an International Number using E.164 [22] numbering plan.

	TON	NPI	Digit field.
USIM application	001	0001	abc...
Other application compatible with 3G	000	0000	xxx...abc...

where "abc..." denotes the subscriber number digits (including its country code), and "xxx..." denotes escape digits or a national prefix replacing TON and NPI.

NOTE 4: When the ME acts upon the EF_{ADN} with a SEARCH RECORD command in order to identify a character string in the alpha-identifier, it is the responsibility of the ME to ensure that the number of characters used as SEARCH RECORD parameters are less than or equal to the value of X if the MMI allows the user to offer a greater number.

Table 4.4: Extended BCD coding

BCD Value	Character/Meaning
'0'	"0"
:	:
'9'	"9"
'A'	"*"
'B'	"#"
'C'	DTMF Control digit separator (GSM 02.07 [17]).
'D'	"Wild" value. This will cause the MMI to prompt the user for a single digit (see GSM 02.07 [17]).
'E'	RFU.
'F'	Endmark e.g. in case of an odd number of digits.

BCD values 'C', 'D' and 'E' are never sent across the radio interface.

NOTE 5: A second or subsequent 'C' BCD value will be interpreted as a 3 second PAUSE (see GSM 02.07 [17]).

4.4.2.4 EF_{EXT1} (Extension1)

This EF contains extension data of an ADN/SSC. . This EF shall always be present if the $DF_{Phonebook}$ is present.

Extension data is caused by:

- an ADN/SSC which is greater than the 20 digit capacity of the ADN/SSC Elementary File or where common digits are required to follow an ADN/SSC string of less than 20 digits. The remainder is stored in this EF as a record, which is identified by a specified identification byte inside the ADN/SSC Elementary File. The EXT1 record in this case is specified as additional data;
- an associated called party subaddress. The EXT1 record in this case is specified as subaddress data.

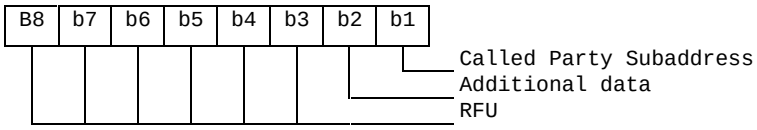
Identifier: '4FXX'	Structure: linear fixed	Optional
SFI: 'XX'		
Record length: 13 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Record type	M	1 byte
2 to 12	Extension data	M	11 bytes
13	Identifier	M	1 byte

- Record type.
  Contents:
  - type of the record.
  Coding:



- b3-b8 are reserved and set to 0;
- a bit set to 1 identifies the type of record;
- only one type can be set;

- '00' indicates the type "unknown".

The following example of coding means that the type of extension data is "additional data":

B8	b7	b6	b5	b4	b3	b2	b1
0	0	0	0	0	0	1	0

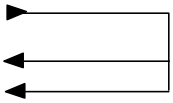
- Extension data.
  Contents:
  additional data or Called Party Subaddress depending on record type.
  Coding:
  Case 1, Extension1 record is additional data:
  - The first byte of the extension data gives the number of bytes of the remainder of ADN/SSC. The coding of remaining bytes is BCD, according to the coding of ADN/SSC. Unused nibbles at the end shall be set to 'F'. It is possible if the number of additional digits exceeds the capacity of the additional record to chain another record inside the EXT1 Elementary File by the identifier in byte 13.

  Case 2, Extension1 record is Called Party Subaddress:
  - The subaddress data contains information as defined for this purpose in 3G TS 24.008 [9]. All information defined in 3G TS 24.008, except the information element identifier, shall be stored in the USIM. The length of this subaddress data can be up to 22 bytes. In those cases where two extension records are needed, these records are chained by the identifier field. The extension record containing the first part of the called party subaddress points to the record which contains the second part of the subaddress.

- Identifier.
  Contents:
  identifier of the next extension record to enable storage of information longer than 11 bytes.
  Coding:
  record number of next record. 'FF' identifies the end of the chain.

- Example of a chain of extension records being associated to an ADN/SSC. The extension1 record identifier (Byte 14+X) of ADN/SSC is set to 3.

No of Record	Type	Extension Data	Next
:	:	:	:
:	:	:	:
Record 3	'02'	xx xx	'06'
Record 4	'xx'	xx xx	'xx'
Record 5	'01'	xx xx	'FF'
Record 6	'01'	xx xx	'05'
:	:	:	:
:	:	:	:



In this example ADN/SSC is associated to additional data (record 3) and a called party subaddress whose length is more than 11 bytes (records 6 and 5).

4.4.2.5 EF_{PBC} (Phone Book Control)

This EF contains control information related to each entry in the phone book. This EF contains as many records as the EF_{ADN} associated with it (shall be record to record). Each record in EF_{PBC} points to a record in its EF_{ADN}. This file indicates the control information and the hidden information of each phone book entry.

The content of EF_{PBC} is linked to the associated EF_{ADN} record by means of the ADN record number/ID (there is a one to one mapping of record number/identifiers between EF_{PBC} and EF_{ADN}).

Structure of control file EF_{PBC}

Identifier: '4FXX'	Structure: linear fixed	Conditional (see Note)
SFI: 'XX'		
Record length: 2 bytes	Update activity: low	

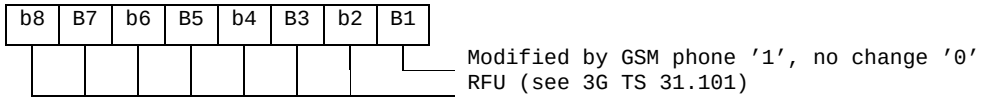
Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Entry Control Information	M	1 byte
2	Hidden Information	M	1 byte

NOTE: This file is mandatory if and only if one or both of the following is true:
- hidden entries are supported
- a GSM SIM application is supported in the UICC.

- Entry Control Information.
  Contents:
  - provides some characteristics about the phone book entry (eg modification by a GSM mobile).
  Coding:



- Hidden Information.
  Contents:
  indicates to which USIM application of the UICC this phone book entry belongs, so that the corresponding secret code can be verified to display the phone book entry. If the secret code is not verified, then the phone book entry is hidden.
  Coding:
  '00' – the phone book entry is not hidden;
  'xx' – the phone book entry is hidden. 'xx' is the record number in EF_{DIR} of the associated USIM application.

4.4.2.6 EF_{GRP} (Grouping file)

This EF contains the grouping information for each phone book entry. This file contains as many records as the associated EF_{ADN}. Each record contains a list of group identifiers, where each identifier can reference a group to which the entry belongs.

Structure of grouping file EF_{GRP}

Identifier: '4FXX'	Structure: linear fixed		Conditional (see Note)
SFI: 'XX'			
Record Length: X bytes (1 ≤ X ≤10)		Update activity: high	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM			
Bytes	Description	M/O	Length
1	Group Name Identifier 1	M	1 byte
2	Group Name Identifier 2	O	1 byte
X	Group Name Identifier X	O	1 byte
NOTE: This file is mandatory if and only if EF_{GAS} is present.			

- Group Name Identifier x.

  Content:

  - indicates if the associated entry is part of a group, in that case it contains the record number of the group name in EF_{GAS}.
  - One entry can be assigned to a maximum of 10 groups.

  Coding:

  - '00' – no group indicated;
    'XX' – record number in EF_{GAS} containing the alpha string naming the group of which the phone book entry is a member.

4.4.2.7 EF_{AAS} (Additional number Alpha String)

This file contains the alpha strings that are associated with the user defined naming tags for additional numbers referenced in EF_{ANR}.

Structure of EF_{AAS}

Identifier: '4FXX'	Structure: linear fixed		Optional
SFI: -			
Record length: X bytes		Update activity: low	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM			
Bytes	Description	M/O	Length
1 to X	Alpha text string	M	X bytes

- Alpha text string.

  Content:

  - user defined text for additional number.

  Coding:

  - same as the alpha identifier in EF_{ADN}.

4.4.2.8 EF_{GAS} (Grouping information Alpha String)

This file contains the alpha strings that are associated with the group name referenced in EF_{GRP}.

Structure of EF_{GAS}

Identifier: '4FXX'		Structure: linear fixed		Conditional (see Note)
SFI: -				
Record length: X bytes		Update activity: low		
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM				
Bytes	Description		M/O	Length
1 to X	Alpha text string		M	X bytes
NOTE: This file is mandatory if and only if EF_{GRP} is present.				

- Alpha text string

  Content:

  - group names.

  Coding:

  - same as the alpha identifier in EF_{ADN}.

4.4.2.9 EF_{ANR} (Additional Number)

Several phone numbers and/or Supplementary Service Control strings (SSC) can be attached to one EF_{ADN} record, using one or several EF_{ANR}. The amount of additional number entries may be less than or equal to the amount of records in EF_{ADN}. The EF structure is linear fixed. Each record contains an additional phone number or Supplementary Service Control strings (SSC). This record cannot be shared between several phonebook entries. The first byte indicates whether the record is free or the type of additional number referring to the record number in EF_{AAS}, containing the text to be displayed. The following part indicates the additional number and the reference to the associated record in the EF_{ADN} file. In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records.

Structure of EF_{ANR}

Identifier: '4FXX'	Structure: linear fixed	Optional
SFI: 'XX'		
Record length: 15 or 17 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Additional Number identifier	M	1 byte
2	Length of BCD number/SSC contents	M	1 byte
3	TON and NPI	M	1 byte
4 to 13	Additional number/SSC String	M	10 bytes
14	Capability/Configuration1 Identifier	M	1 byte
15	Extension1 Record Identifier	M	1 byte
16	ADN file SFI	C	1 byte
17	ADN file Record Identifier	C	1 byte

NOTE: The fields marked C above are mandatory if and only if the file is not type 1 (as specified in EF_{PBR})

- Additional Number Identifier

  Content:

  - describes the type of the additional number defined in the file EF_{AAS}.

  Coding:

  - '00' – no additional number description;
    'xx' – record number in EF_{AAS} describing the type of number (e.g. "FAX");
    'FF' – free record.

- Length of BCD number/SSC contents

  Contents:

  - this byte gives the number of bytes of the following two data items containing actual BCD number/SSC information. This means that the maximum value is 11, even when the actual additional number/SSC information length is greater than 11. When the additional number/SSC has extension, it is indicated by the extension1 identifier being unequal to 'FF'. The remainder is stored in the EF_{EXT1} with the remaining length of the additional data being coded in the appropriate additional record itself (see subclause 4.4.2.4).

  Coding:

  - same as the length of BCD number/SSC string byte in $EF_{ADN.}$

- TON and NPI.

  Contents:

  - Type of number (TON) and numbering plan identification (NPI).

  Coding:

  - same as the TON and NPI byte in $EF_{ADN.}$

- Additional number/SSC string

  Content:

  - up to 20 digits of the additional phone number and/or SSC information linked to the phone book entry.

Coding:

- same as the dialling number /SSC string in $EF_{ADN.}$

- Capability/Configuration1 Identifier.

  Contents:

  - This byte identifies the number of a record in the EF_{CCP1} containing associated capability/configuration parameters required for the call. The use of this byte is optional. If it is not used it shall be set to 'FF'.

  Coding:

  - binary.

- Extension1 Record Identifier.

  Contents:

  - extension1 record identification byte. This byte identifies the number of a record in the EF_{EXT1} containing an associated called party subaddress or additional data. The use of this byte is optional. If it is not used it shall be set to 'FF'.

    if the number requires both additional data and called party subaddress, this byte identifies the additional record. A chaining mechanism inside EF_{EXT1} identifies the record of the appropriate called party subaddress (see subclause 4.4.2.4).

  Coding:

  - binary.

- ADN file SFI.

  Content:

  - Short File identifier of the associated EF_{ADN} file.

  Coding:

  - as defined in the UICC specification.

- ADN file Record Identifier

  Content:

  - record identifier of the associated phone book entry.

  Coding:

  - 'xx' – record identifier of the corresponding ADN record.

4.4.2.10 EF_{SNE} (Second Name Entry)

The phone book also contains the option of a second name entry. The amount of second name entries may be less than or equal to the amount of records in EF_{ADN}. Each record contains a second name entry. This record cannot be shared between several phonebook entries.

Structure of EF_{SNE}

Identifier: '4FXX'	Structure: linear fixed	Optional
SFI: 'XX'		
Record length: X or X+2 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	Alpha Identifier of Second Name	M	X bytes
X+1	ADN file SFI	C	1 byte
X+2	ADN file Record Identifier	C	1 byte

NOTE: The fields marked C above are mandatory if and only if the file is not type 1 (as specified in EF_{PBR})

- Alpha Identifier of Second Name.

  Content:

  - string defining the second name of the phone book entry.

  Coding:

  - as the alpha identifier for EF_{ADN}.

- ADN file SFI.

  Content:

  - Short File identifier of the associated EF_{ADN} file.

  Coding:

  - as defined in the UICC specification.

- ADN file Record Identifier

  Content:

  record identifier of the associated phone book entry.

  Coding:

  'xx' – record identifier of the corresponding ADN record.

4.4.2.11 EF_{CCP1} (Capability Configuration Parameters 1)

This EF contains parameters of required network and bearer capabilities and ME configurations associated with a call established using a phone book entry.

Structure of EF_{CCP1}

Identifier: '"4FXX'	Structure: linear fixed	Optional
SFI: 'XX'		
Record length: X bytes, X ≥ 15	Update activity: low	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to X	Bearer capability information element	M	X bytes

- Bearer capability information element.

  Contents and Coding:

  - see 3G TS 24.008 [9]. The Information Element Identity (IEI) shall be excluded; i.e. the first byte of the EF_{CCP1} record shall be Length of the bearer capability contents.

"- unused bytes are filled with 'FF'

4.4.2.12 Phone Book Synchronisation

To support synchronisation of phone book data with other devices, the USIM may provide the following files to be used by the synchronisation method: a phone book synchronisation counter (PSC), a unique identifier (UID) and change counter (CC) to indicate recent changes.

If synchronisation is supported in the phonebook, then EF_{PSC}, EF_{UID}, EF_{PUID} and EF_{CC} are all mandatory.

4.4.2.12.1 EF_{UID} (Unique Identifier)

The EF_{UID} is used to uniquely identify a record and to be able to keep track of the entry in the phone book. The terminal assigns the (UID) when a new entry is created. The value of the UID does not change as long as the value of the PBID remains the same. The UID shall remain on the UICC, in EF_{UID}, until the PBID is regenerated. This means that when a phone book entry is deleted, the content of the linked information (eg ADN, E-MAIL,..) shall be set to the personalization value 'FF…FF'. But the UID-value of the deleted record shall not be used when a new entry is added to the phonebook until the PBID is regenerated, but it shall be set to a new value.

If/when the PBID is regenerated, all UIDs for the entry in the phone book shall be assigned new values starting from 1. The new value of the UID for each entry shall then be kept until the PBID is regenerated again.

Structure of EF_{UID}

Identifier: '4FXX'	Structure: linear fixed	Conditional (see Note)
SFI: 'XX'		
Record length: 2 bytes	Update activity: low	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to 2	Unique Identifier (UID) of Phone Book Entry	M	2 bytes
NOTE: This file is mandatory if and only if synchronisation is supported in the phonebook.			

- Unique Identifier of Phone Book Entry.

  Content:

  - number to unambiguously identify the phone book entry for synchronisation purposes.

  Coding:

  - hexadecimal value. At initialisation all UIDs are personalised to "00 00" (i.e. empty).

4.4.2.12.2 EF_{PSC} (Phone book Synchronisation Counter)

The phone book synchronisation counter (PSC) is used by the ME to construct the phone book identifier (PBID) and to determine whether the accessed phone book is the same as the previously accessed phone book or if it is a new unknown phone book (might be the case that there is one phonebook under DF-telecom and one phone book residing in a USIM-application). If the PSC is unknown, a full synchronisation of the phone book will follow.

The PSC is also used to regenerate the UIDs and reset the CC to prevent them from running out of range. When the UIDs or the CC has reached its maximum value, a new PSC is generated. This leads to a scenario where neither the CC nor the UIDs will run out of range.

The PSC shall be regenerated by the terminal if one of the following situation applies:
- the values of the UIDs have run out of range;
- the whole phone book has been reset/deleted;
- the value of the CC has run out of range.

Structure of EF_{PSC}

Identifier: '4F22'	Structure: transparent	Conditional (see Note)
SFI: 'XX'		
File size: 4 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 4	Phone book synchronisation counter (PSC)	M	4 bytes

NOTE: This file is mandatory if and only if synchronisation is supported in the phonebook.

- PSC: Unique synchronisation counter of Phone Book.

  Content:

  number to unambiguously identify the status of the phone book for synchronisation purposes.

  Coding:

  hexadecimal value.

  The phone book identifier (PBID) coding based on the EF_{PSC} is described hereafter:

- For a phone book residing in DF-telecom:
  - PBID = ICCid (10bytes) "fixed part" + 4 bytes (in EF_{PSC}) "variable part".
- For a phone book residing in an USIM application:
  - PBID = 10 last bytes of (ICCid XOR AID) "fixed part" + 4 bytes (in EF_{PSC}) "variable part".

To be able to detect if the PSC needs to be regenerated (i.e. the variable part) the following test shall be made by the terminal before for each update of either the CC or the assignment of a new UID:

- Each time the terminal has to increment the value of the UID the following test is needed:
  - If UID = 'FF FF' then.

    {Increment **PSC** mod 'FF FF FF FF'; all the UIDs shall be regenerated}.
- Each time the terminal has to increment the value of CC the following test is needed:

  If CC = 'FF FF' then.

  {Increment **PSC** mod 'FF FF FF FF'; CC=0001}.

NOTE: If the phonebook is deleted then the terminal will change the **PSC** according to:

Incrementing **PSC** modulus 'FFFFFFFF'.

4.4.2.12.3 EF_{CC} (Change Counter)

The change counter (CC) shall be used to detect changes made to the phone book.

Every update/deletion of an existing phone book entry or the addition of a new phone book entry causes the terminal to increment the EF_{CC}. The concept of having a CC makes it possible to update the phone book in different terminals, which still are able to detect the changes (e.g. changes between different handset and/or 2nd and 3rd generation of terminals).

Structure of EF_{CC}

Identifier: '4F23'	Structure: transparent		Conditional (see Note)
SFI: 'XX'			
File size: 2 bytes		Update activity: high	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM			
Bytes	Description	M/O	Length
1 to 2	Change Counter (CC) of Phone Book	M	2 bytes
NOTE: This file is mandatory if and only if synchronisation is supported in the phonebook.			

- Change Counter of Phone Book.

  Content:

  - indicates recent change(s) to phone book entries for synchronisation purposes.

  Coding:

  - hexadecimal value. At initialisation, CC shall be personalised to '00 00' (i.e. empty).

4.4.2.12.4 EF_{PUID} (Previous Unique Identifier)

The PUID is used to store the previously used unique identifier (UID). The purpose of this file is to allow the terminal to quickly generate a new UID, which shall then be stored in the EF_{UID}.

Structure of EF_{PUID}

Identifier: '4F24'	Structure: transparent	Conditional (see Note)
SFI: 'XX'		
File size: 2 bytes	Update activity: high	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to 2	Previous Unique Identifier (PUID) of Phone Book Entry	M	2 bytes

NOTE: This file is mandatory if and only if synchronisation is supported in the phonebook.

- Previous unique Identifier of Phone Book Entry.

  Content:

  - Previous number that was used to unambiguously identify the phone book entry for synchronisation purposes.

4.4.2.13 EF_{EMAIL} (e-mail address)

This EF contains the e-mail addresses that may be linked to a phone book entry. Several e-mail addresses can be attached to one EF_{ADN} record, using one or several EF_{EMAIL}. The number of email addresses may be equal to or less than the amount of records in EF_{ADN}. Each record contains an e-mail address. The first part indicates the e-mail address, and the second part indicates the reference to the associated record in the EF_{ADN} file. This record cannot be shared between several phonebook entries.

Structure of EF_{EMAIL}

Identifier: '4FXX'	Structure: linear fixed	Optional
SFI: 'XX'		
Record length: X or X+2 bytes	Update activity: low	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to X	E-mail Address	M	X bytes
:			
:			
X+1	ADN file SFI	C	1 byte
X+2	ADN file Record Identifier	C	1 byte

NOTE: The fields marked C above are mandatory if and only if the file is not type 1 (as specified in EF_{PBR})

- E-mail Address.
  Content:

  - string defining the e-mail address

  Coding:

- the SMS default 7-bit coded alphabet as defined in 3G TS 23.038 [5] with bit 8 set to 0. The alpha identifier shall be left justified. Unused bytes shall be set to 'FF'.

- ADN file SFI.

  Content:

  - short File identifier of the associated EF_{ADN} file.

  Coding:

  - as defined in 3G TS 31.101.

- ADN file Record Identifier.

  Content:

  - record identifier of the associated phone book entry.

  Coding:

  - binary.

4.4.2.14 Phonebook restrictions

This subclause lists some general restrictions that apply to the phonebook:

- if an EF_{PBR} file contains more than one record, then they shall all be formatted identically on a type-by-type basis, e.g. if EF_{PBR} record #1 contains one type 1 e-mail then all EF_{PBR} records shall have one type 1 email;

- if an EF_{PBR} record contains more than one reference to one type of file , such as two EF_{EMAIL} files, then they shall all be formatted identically on a type-by-type basis, e.g. if an EF_{PBR} record has 2 email addresses, then they shall have the same record size and the same number of records in each EF_{PBR} entry;

- an EF_{PBR} record may contain TLV entries indicating that the file exist as a type 1 and 2 file, e.g. a phonebook entry may have two emails, one with a one-to-one mapping (type 1) and one with a indirect mapping (type 2). Regardless of the type, files in all entries shall have the same record configuration.

Editor's note: this list is currently not complete.

4.4.3 Contents of files at the DF GSM-ACCESS level (Files required for GSM Access)

The EFs described in this subclause are required for the USIM application to be able to access service through a GSM network.

The presence of these files and thus the support of a GSM access is indicated in the 'USIM Service Table' as service no. '27' being available. If the GSM access service is available on the USIM, then all these files are mandatory.

4.4.3.1 EF_{Kc} (GSM Ciphering key Kc)

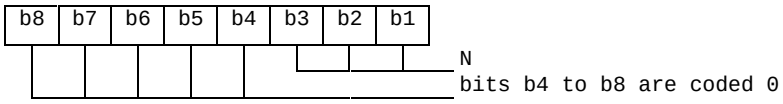
This EF contains the ciphering key Kc and the ciphering key sequence number n for enciphering in a GSM access network.

Identifier: '4F20'	Structure: transparent	Optional
SFI: '01'		
File size: 9 bytes	Update activity: high	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to 8	Ciphering key Kc	M	8 bytes
9	Ciphering key sequence number n	M	1 byte

- Ciphering key Kc.
  Coding:
  - the least significant bit of Kc is the least significant bit of the eighth byte. The most significant bit of Kc is the most significant bit of the first byte.

- Ciphering key sequence number n
  Coding:



NOTE: 3G TS 24.008 [9] defines the value of n=111 as "key not available". Therefore the value '07' and not 'FF' should be present following the administrative phase.

4.4.3.2 EF_{KcGPRS} (GPRS Ciphering key KcGPRS)

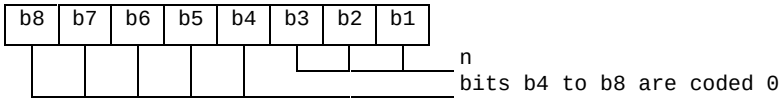
This EF contains the ciphering key KcGPRS and the ciphering key sequence number n for GPRS (see 3G TS 23.060 [7]).

Identifier: '4F52'	Structure: transparent	Optional
SFI: '02		
File size: 9 bytes	Update activity: high	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to 8	Ciphering key KcGPRS	M	8 bytes
9	Ciphering key sequence number n for GPRS	M	1 byte

- Ciphering key KcGPRS.
  Coding:
  the least significant bit of KcGPRS is the least significant bit of the eighth byte. The most significant bit of KcGPRS is the most significant bit of the first byte.

- Ciphering key sequence number n for GPRS.
  Coding:



NOTE: TS 24.008 [9] defines the value of n=111 as "key not available". Therefore the value '07' and not 'FF' should be present following the administrative phase.

4.4.3.3 Void

4.4.3.4 EF_{CPBCCH} (CPBCCH Information)

This EF contains information concerning the CPBCCH according to GSM 04.18 [28].

CPBCCH storage may reduce the extent of a Mobile Station's search of CPBCCH carriers when selecting a cell. The CPBCCH carrier lists shall be in accordance with the procedures specified TS 23.022 [29]. The MS stores CPBCCH information (from the System Information 19 message, Packet System Information 3, and Packet System Information 3 bis) on the USIM. The same CPBCCH carrier shall never occur twice in the list.

Identifier: '4F63'	Structure: transparent	Optional
File size: 2n bytes	Update activity: high	

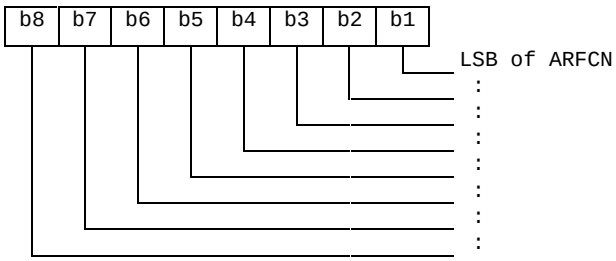
Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

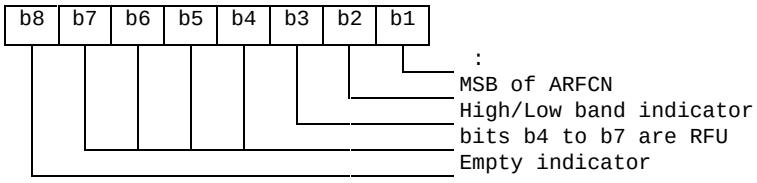
Bytes	Description	M/O	Length
1 to 2	Element 1 of CPBCCH carrier list	M	2 bytes
2n-1 to 2n	Element n of CPBCCH carrier list	M	2 bytes

- Element in CPBCCH carrier list
  Coding:

  Byte 1: first byte of CPBCCH carrier list element



  Byte 2: second byte of CPBCCH carrier list element



  - ARFCN (10 bits) as defined in TS 05.05 [34].

  - High/Low band indicator: If the ARFCN indicates possibly a channel in the DCS 1800 or a channel in the PCS 1900 band, if the bit is set to '1' the channel is in the higher band (GSM 1900). If the bit is set to '0', the lower band (GSM 1800) is indicated. If ARFCN indicates a unique channel, this indicator shall be set to '0'.

- Empty indicator: If this bit is set to '1', no valid CPBCCH carrier is stored in this position. If the Empty Indicator is set to '1', the content of the CPBCCH carrier field shall be ignored. The empty indicator shall also be used, and set to '1', if storage of fewer than maximum number n, of CPBCCH carrier fields is required.

4.4.3.5 $EF_{InvScan}$ (Investigation Scan)

This EF contains two flags used to control the investigation scan for higher prioritized PLMNs not offering voice services.

Identifier: '4F64'	Structure: transparent	Optional
File size: 1 byte	Update activity: low	

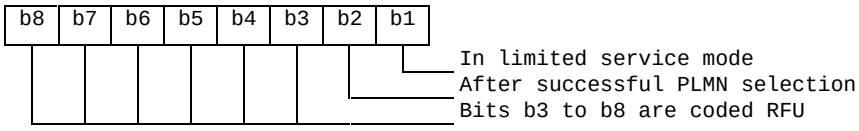
Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Investigation scan flags	M	1 byte

- Investigation scan flags

  Coding:



  A '1' in a bit position indicates that the investigation scan shall be performed for the condition corresponding to that bit position and a '0' that it shall not be performed.

If this elementary file is not present, no investigation scan shall be performed.

4.4.4 Contents of files at the MExE level

This subclause specifies the EFs in the dedicated file DF_{MExE}. It only applies if the USIM supports MExE (see TS 23.057 [30]).

The EFs in the Dedicated File DF_{MExE} contain execution environment related information.

4.4.4.1 $EF_{MExE-ST}$ (MExE Service table)

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

Identifier: '4F40'	Structure: transparent	Optional
File size: X bytes, X ≥ 1	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Services n°1 to n°8	M	1 byte
2	Services n°9 to n°16	O	1 byte
etc.			
X	Services (8X-7) to (8X)	O	1 byte

-Services

Contents: Service n°1 : Operator Root Public Key
Service n°2 : Administrator Root Public Key
Service n°3 : Third Party Root Public Key
Service n°4 : RFU

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

4.4.4.2 EF_{ORPK} (Operator Root Public Key)

This EF contains the descriptor(s) of certificates containing the Operator Root Public Key. This EF shall only be allocated if the operator wishes to verify applications and certificates in the MExE operator domain using a root public key held in the USIM. Each record of this EF contains one certificate descriptor.

For example, an operator may provide a second key for recover disaster procedure in order to limit OTA data to load.

Identifier: '4F41'	Structure: linear fixed	Optional
Record length : X + 10 bytes	Update activity: low	

Access Conditions:

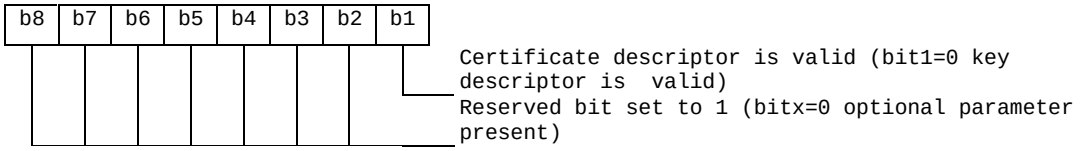
READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Parameters indicator	M	1 byte
2	Flags	M	1 byte
3	Type of certificate	M	1 byte
4 to 5	Key/certificate file identifier	M	2 bytes
6 to 7	Offset into key/certificate file	M	2 bytes
8 to 9	Length of key/certificate data	M	2 bytes
10	Key identifier length (X)	M	1 byte
11 to 10+X	Key identifier	M	X bytes

- Parameter indicator

Contents:
The parameter indicator indicates if record is full and which optional parameters are present

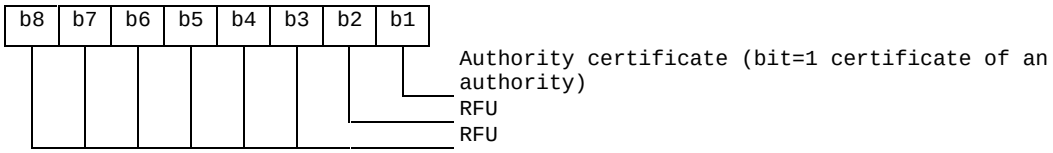
Coding: bit string



- Flags

Contents:
The authority flag indicates whether the certificate identify an authority (i.e. CA or AA) or not.

Coding: bit string



- Type of certificate

Contents:
This field indicates the type of certificate containing the key.
Coding: binary :
0 : WTLS
1 : X509
2 : X9.68
Other values are reserved for further use

- Key/certificate File Identifier
Contents:
these bytes identify an EF which is the key/certificate data file (see subclause 4.4.4.5), holding the actual key/certificate data for this record.
Coding:
byte 4: high byte of Key/certificate File Identifier;
byte 5: low byte of Key/certificate File Identifier.

- Offset into Key/certificate File
Contents:
these bytes specify an offset into the transparent key/certificate data File identified in bytes 4 and 5.
Coding:
byte 6: high byte of offset into Key/certificate Data File;
byte 7: low byte of offset into Key/certificate Data File

- Length of Key/certificate Data
Contents:
these bytes yield the length of the key/certificate data, starting at the offset identified in "Offset into Key/certificate File" field.
Coding:
byte 8: high byte of Key/certificate Data length;
byte 9: low byte of Key/certificate Data length.

- Key identifier length
Contents:
This field gives length of key identifier
Coding:
binary

- Key identifier
Contents:
This field provides a means of identifying certificates that contain a particular public key (chain building) and linking the public key to its corresponding private key. For more information about value and using see TS 23.057 [30].
Coding:
octet string

Note: transparent key/certificate data longer than 256 bytes may be read using successive READ BINARY commands.

4.4.4.3 EF_{ARPK} (Administrator Root Public Key)

This EF contains the descriptor(s) of certificates containing the Administrator Root Public Key. This EF shall only be allocated if the SIM issuer wishes to control the Third Party certificates on the terminal using an Administrator root public key held in the USIM. Each record of this EF contents one certificate descriptor.

This file shall contain only one record.

Identifier: '4F42'	Structure: linear fixed	Optional
Record length: X + 10 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Parameters indicator	M	1 byte
2	Flags	M	1 byte
3	Type of certificate	M	1 byte
4 to 5	Key/certificate file identifier	M	2 bytes
6 to 7	Offset into key/certificate file	M	2 bytes
8 to 9	Length of key/certificate data	M	2 bytes
10	Key identifier length (X)	M	1 byte
11 to 10+X	Key identifier	M	X bytes

For contents and coding of all data items see the respective data items of the EF_{ORPK} (sub-clause 4.4.4.2).

4.4.4.4 EF_{TPRPK} (Third Party Root Public Key)

This EF contains descriptor(s) of certificates containing the Third Party root public key (s). This EF shall only be allocated if the USIM issuer wishes to verify applications and certificates in the MExE Third Party domain using root public key(s) held in the USIM. This EF can contain one or more root public keys. Each record of this EF contains one certificate descriptor.

For example, an operator may provide several Third Party Root Public Keys.

Identifier:'4F43'	Structure: linear fixed	Optional
Record length : X + Y + 11 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Parameters indicator	M	1 byte
2	Flags	M	1 byte
3	Type of certificate	M	1 byte
4 to 5	Key/certificate file identifier	M	2 bytes
6 to 7	Offset into key/certificate file	M	2 bytes
8 to 9	Length of key/certificate data	M	2 bytes
10	Key identifier length (X)	M	1 byte
11 to 10+X	Key identifier	M	X bytes
11+X to 11+Y	Certificate identifier length (Y)	M	1 byte
12+X to 11+X+Y	Certificate identifier	M	Y bytes

- Certificate identifier length
  Contents:
  This field gives the length of the certificate identifier
  Coding:
  binary

- Certificate identifier
  Contents:
  This field identifies the issuer and provides an easy way to find a certificate. For more information about the value and usage see TS 23.057 [30].
  Coding:
  Octet string

For contents and coding of all other data items see the respective data items of the EF_{ORPK} (sub-clause 4.4.4.2).

4.4.4.5 EF_{TKCDF} (Trusted Key/Certificates Data Files)

Residing under DF_{MExE}, there may be several key/certificates data files. These EFs containing key/certificates data shall have the following attributes:

Identifier: '4FXX'	Structure: transparent	Optional
File size: Y bytes	Update activity: low	
Access Conditions: READ PIN UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to Y	Key/Certificate Data	M	Y bytes

Contents and coding:

Key/certificate data are accessed using the key/certificates descriptors provided by EF_{TPRPK} (see sub-clause 4.4.4.4).

The identifier '4FXX' shall be different from one key/certificate data file to another. For the range of 'XX', see TS 31.101 [11]. The length Y may be different from one key/certificate data file to another.

4.5 Contents of EFs at the TELECOM level

The EFs in the Dedicated File $DF_{TELECOM}$ contain service related information.

4.5.1 EF_{ADN} (Abbreviated dialling numbers)

In case of a present GSM application on the UICC the first EF_{ADN} (i.e. reflected by the first record in EF_{PBR}) of the $DF_{PHONEBOOK}$ is mapped (with an identifier equal to '6F3A') to $DF_{TELECOM}$ to ensure backwards compatibility.

A 3G ME shall not access this file. The information is accessible for a 3G ME in EF_{ADN} under $DF_{PHONEBOOK}$.

4.5.2 EF_{EXT1} (Extension1)

In case of a present GSM application on the UICC the first EF_{EXT1} (i.e. reflected by the first record in EF_{PBR}) of the $DF_{PHONEBOOK}$ is mapped (with an identifier equal to '6F4A') to $DF_{TELECOM}$ to ensure backwards compatibility.

4.5.3 EF_{ECCP} (Extended Capability Configuration Parameter)

In case of a present GSM application on the UICC the first EF_{CCP1} (i.e. reflected by the first record in EF_{PBR}) of the $DF_{PHONEBOOK}$ is mapped (with an identifier equal to '6F4F') to $DF_{TELECOM}$ to ensure backwards compatibility. There

shall not be any EF_{CCP} (with a file-id of '6F3D') under $DF_{TELECOM}$ because otherwise a GSM terminal could create inconsistencies within the phonebook.

4.5.4 EF_{SUME} (SetUpMenu Elements)

This EF contains Simple TLVs related to the menu title to be used by a UICC when issuing a SET UP MENU proactive command.

Identifier: '6F54'	Structure: transparent	Optional
File size: X+Y bytes	Update activity: low	

Access Conditions:

READ	ADM
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	Title Alpha Identifier	M	X bytes
1+X to X+Y	Title Icon Identifier	O	Y bytes

- Title Alpha Identifier.

  Contents:

  - this field contains the Alpha Identifier Simple TLV defining the menu title text.

  Coding:

  - according to TS 31.111 [12].

- Title Icon Identifier

  Contents:

  - this field contains the Icon Identifier Simple TLV defining the menu title icon.

  Coding:

  - according to TS 31.111 [12]. If not present the field shall be set to 'FF'.
  - Unused bytes of this file shall be set to 'FF'.

4.5.5 EF_{ARR} (Access Rule Reference)

This EF contains the access rules for files located under the $DF_{TELECOM}$ in the UICC. If the security attribute tag '8B' is indicated in the FCP it contains a reference to a record in this file.

Structure of EF_{ARR} at $DF_{Telecom}$-level

Identifier: '6F06'	Structure: Linear fixed	Mandatory
Record length: X bytes	Update activity: low	

Access Conditions:

READ	ALW
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	Access Rule TLV data objects	M	X bytes

This EF contains one or more records containing access rule information according to the reference to expanded format as defined in ISO/IEC 7816-9 [26]. Each record represents an access rule. Unused bytes in the record are set to 'FF'.

If the card cannot access EF_{ARR} , any attempt to access a file with access rules indicated in this EF_{ARR} shall not be granted.

4.6 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).

4.6.1 Contents of files at the $DF_{GRAPHICS}$ level

The EFs in the Dedicated File $DF_{GRAPHICS}$ contain graphical information.

4.6.1.1 EF_{IMG} (Image)

Each record of this EF identifies instances of one particular graphical image, which graphical image is identified by this EF's record number.

Image instances may differ as to their size, having different resolutions, and the way they are coded, using one of several image coding schemes.

As an example, image k may represent a company logo, of which there are i instances in the UICC, of various resolutions and perhaps encoded in several image coding schemes. Then, the i instances of the company's logo are described in record k of this EF.

Identifier: '4F20'	Structure: linear fixed	Optional
Record length: 9n+2 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Number of Actual Image Instances	M	1 byte
2 to 10	Descriptor of Image Instance 1	M	9 bytes
11 to 19	Descriptor of Image Instance 2	O	9 bytes
9(n-1)+2 to 9n+1	Descriptor of Image Instance n	O	9 bytes
9n + 2	RFU (see 3G TS 31.101)	O	1 byte

- Number of Actual Image Instances.

  Contents:

  - this byte gives the number of actual image instances described in the following data items (i.e. unused descriptors are not counted).

  Coding:

  - binary.

- Image Instance Descriptor

Contents:

- a description of an image instance.

Coding:

- Byte 1: Image Instance Width

  Contents:

  - this byte specifies the image instance width, expressed in raster image points.

  Coding:

  - binary.

Byte 2: Image Instance Height.

Contents:

- this byte specifies the image instance height, expressed in raster image points.

Coding:

- binary.

Byte 3: Image Coding Scheme.

Contents:

- this byte identifies the image coding scheme that has been used in encoding the image instance.

Coding:

- '11' - basic image coding scheme as defined in annex B;
- '21' - colour image coding scheme as defined in annex B;

other values are reserved for future use.

Bytes 4 and 5: Image Instance File Identifier.

Contents:

- these bytes identify an EF which is the image instance data file (see subclause 4.6.1.2), holding the actual image data for this particular instance.

Coding:

- byte 4: high byte of Image Instance File Identifier;
- byte 5: low byte of Image Instance File Identifier.

Bytes 6 and 7: Offset into Image Instance File.

Contents:

- these bytes specify an offset into the transparent Image Instance File identified in bytes 4 and 5.

Coding:

- byte 6: high byte of offset into Image Instance File;

byte 7: low byte of offset into Image Instance File.

Bytes 8 and 9: Length of Image Instance Data.

Contents:

- these bytes yield the length of the image instance data, starting at the offset identified in bytes 6 and 7.

Coding:

- byte 8: high byte of Image Instance Data length;
- byte 9: low byte of Image Instance Data length.

NOTE: Transparent image instance data longer than 256 bytes may be read using successive READ BINARY commands.

4.6.1.2 Image Instance Data Files

Residing under $DF_{GRAPHICS}$, there may be several image instance data files. These EFs containing image instance data shall have the following attributes:

Identifier: '4FXX'	Structure: transparent	Optional
Record length: Y bytes	Update activity: low	
Access Conditions: READ PIN UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to Y	Image Instance Data	M	Y bytes

Contents and coding:

- Image instance data are accessed using the image instance descriptors provided by EF_{IMG} (see subclause 4.6.1.1).

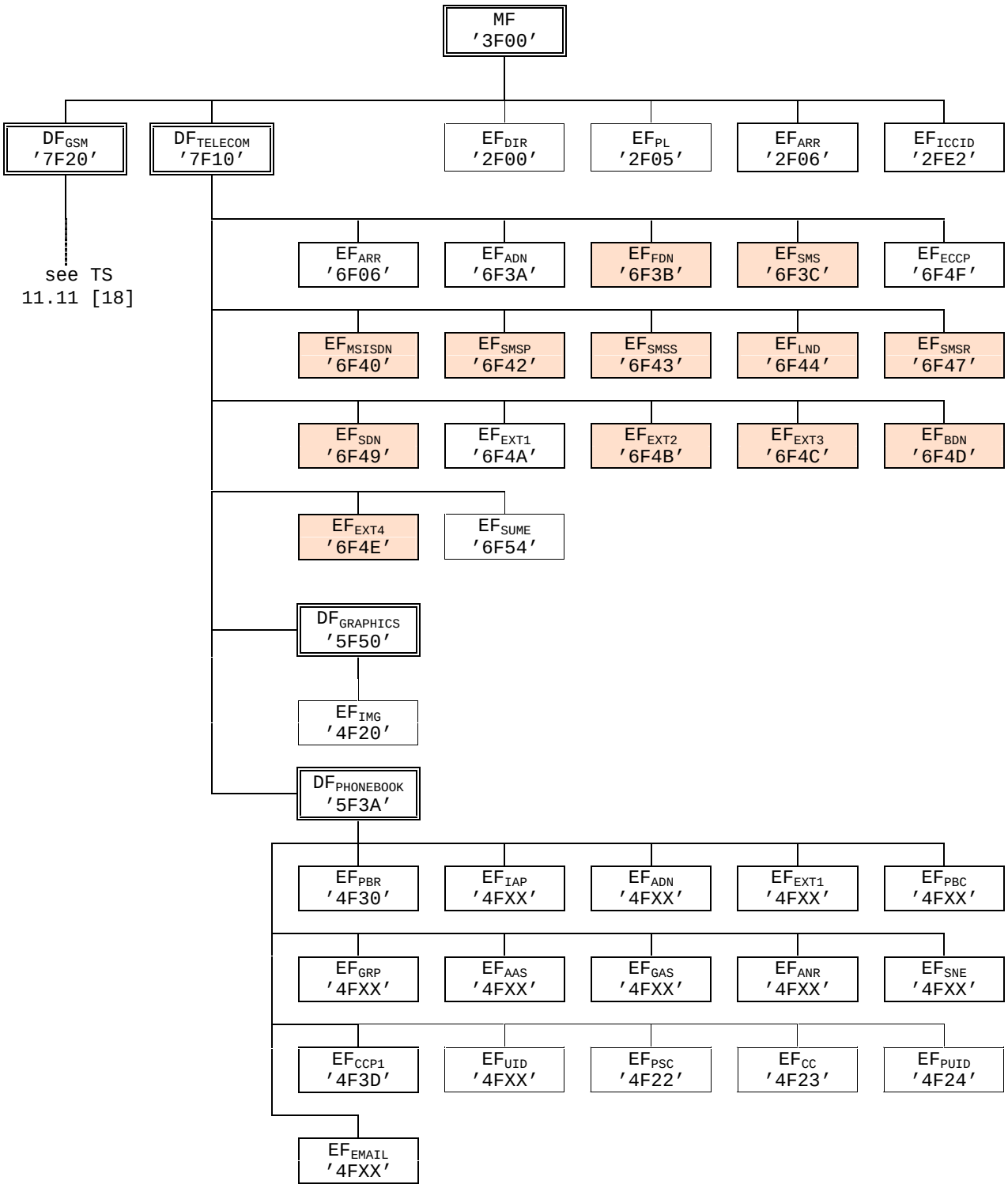
The identifier '4FXX' shall be different from one image instance data file to the other. For the range of 'XX', TS 31.101 [11]. The length Y may be different from one image instance data file to the other.

4.6.2 Contents of files at the $DF_{PHONEBOOK}$ under the $DF_{TELECOM}$

This DF has the same structure as $DF_{PHONEBOOK}$ under the DF_{USIM}.

4.7 Files of USIM

This subclause 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: Files under $DF_{TELECOM}$ with shaded background are defined in TS 11.11 [18].

Figure 4.1: File identifiers and directory structures of UICC

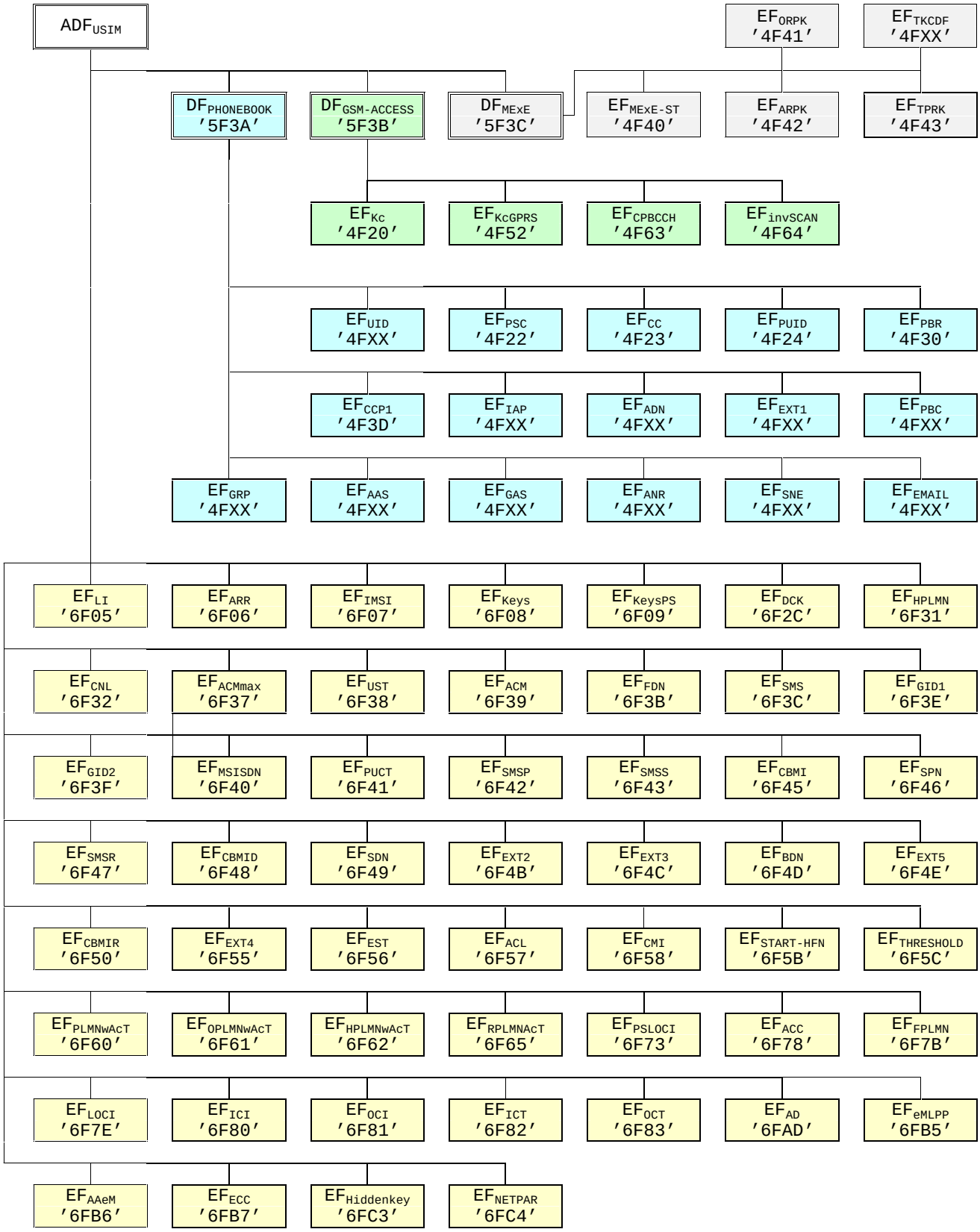


Figure 4.2: File identifiers and directory structures of USIM

DF '5F70' is reserved for SoLSA. EF '4F30' (EF_{SAL}) and EF '4F31' (EF_{SLL}) are reserved under DF '5F70' (SoLSA).

5 Application protocol

When involved in 3G administrative management operations, the USIM interfaces with appropriate equipment. These operations are outside the scope of this standard.

When involved in 3G network operations the USIM interfaces with an ME with which messages are exchanged. A message can be a command or a response.

- A USIM Application command/response pair is a sequence consisting of a command and the associated response.
- A USIM Application procedure consists of one or more USIM Application command/response pairs which are used to perform all or part of an application-oriented task. A procedure shall be considered as a whole, that is to say that the corresponding task is achieved if and only if the procedure is completed. The ME shall ensure that, when operated according to the manufacturer's manual, any unspecified interruption of the sequence of command/response pairs which realise the procedure, leads to the abortion of the procedure itself.
- A 3G session of the USIM in the 3G application is the interval of time starting at the completion of the USIM initialisation procedure and ending either with the start of the 3G session termination procedure, or at the first instant the link between the UICC and the ME is interrupted.

During the 3G network operation phase, the ME plays the role of the master and the USIM plays the role of the slave.

The USIM shall execute all 3G and USIM Application Toolkit commands or procedures in such a way as not to jeopardise, or cause suspension, of service provisioning to the user. This could occur if, for example, execution of the AUTHENTICATE is delayed in such a way which would result in the network denying or suspending service to the user.

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

If a procedure is related to a specific service indicated in the USIM Service Table, it shall only be executed if the corresponding bits denote this service as "service available" (see subclause "EF_{UST}"). In all other cases the procedure shall not start.

5.1 USIM management procedures

5.1.1 Initialisation

5.1.1.1 USIM application selection

After UICC activation (see 3G TS 31.101 [11]), the ME selects a USIM application. If no EF_{DIR} file is found or no USIM applications are listed in the EF_{DIR} file, the ME then tries to select the GSM application as specified in GSM 11.11 [18].

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

If a USIM application is selected using partial DF name, the partial DF name supplied in the command shall uniquely identify a USIM application. Furthermore if a USIM application is selected using a partial DF name as specified in 3G TS 31.101 [11] indicating in the SELECT command the last occurrence the UICC shall select the USIM application stored as the last application. If, in the SELECT command, the options first, next/previous are indicated, they have no meaning if an application has not been previously selected in the same session and shall return an appropriate error code.

5.1.1.2 USIM initialisation

The ME requests the emergency call codes. For service requirements, see 3G TS 22.101 [24].

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

- if the EF_{LI} has the value 'FFFF' in its highest priority position, then the preferred language selection shall be the language preference in the EF_{PL} at the MF level according the procedure defined in 3G TS 31.101[11];
- if the ME does not support any of the language codes indicated in EF_{LI}, or if EF_{LI} is not present, then the language selection shall be as defined in EF_{PL} at the MF level according the procedure defined in 3G TS 31.101[11];
- if neither the languages of EF_{LI} nor EF_{PL} are supported by the terminal, then the terminal shall use its own internal default selection.

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

The ME performs the administrative information request.

The ME performs the USIM Service Table request.

The ME performs the Enabled Services Table Request.

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

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

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

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

Afterwards, the ME runs the following procedures if the ME supports the related feature:

- IMSI request.
- Access control information request.
- HPLMN search period request.
- HPLMN selector with Access Technology request;
- User controlled PLMN selector with Access Technology request;
- Operator controlled PLMN selector with Access Technology request;
- RPLMN last used Access Technology
- GSM initialisation requests.
- Location Information request for CS-and/or PS-mode.
- Cipher key and integrity key request for CS- and/or PS-mode.
- Forbidden PLMN request.
- Initialisation value for hyperframe number request.
- Maximum value of START request.
- CBMID request.

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

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

5.1.1.3 GSM related initialisation procedures

If GSM access is enabled the following procedures shall be performed if the applicable service is enabled.

- Investigation Scan request.
- CPBCCH information request.

5.1.2 Session termination

5.1.2.1 3G session termination

NOTE 1: This procedure is not to be confused with the deactivation procedure in 3G TS 31.101 [11].

The 3G session is terminated by the ME as follows.

The ME shall indicate to the USIM by sending a particular STATUS command that the termination procedure is starting.

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

- Location Information update.
- Cipher Key and Integrity Key update.
- Advice of Charge increase.
- Forbidden PLMN update.
- GSM Termination procedures.
- RPLMN last used Access Technology update.

Finally, the ME deletes all these subscriber related information elements from its memory.

NOTE 2: If the ME has already updated any of the subscriber related information during the 3G session, and the value has not changed until 3G session termination, the ME may omit the respective update procedure.

To actually terminate the session, the ME shall then use one of the mechanisms described in 3G TS 31.101 [11].

5.1.2.2 GSM termination procedures

If GSM access is enabled the following termination procedures shall be performed if the applicable service is enabled.

- CPBCCH information update.

5.1.3 USIM application closure

After termination of the 3G session as defined in 5.1.2 the USIM application may be closed by closing the logical channels that are used to communicate with this particular USIM application.

5.1.4 Emergency call codes

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

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

NOTE: The update procedure is only applicable when access conditions of ADM for update is set to ALW, PIN or PIN2.

5.1.5 Language indication

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

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

5.1.6 Administrative information request

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

5.1.7 USIM service table request

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

5.1.8 Spare

5.1.9 UICC presence detection

The ME checks for the presence of the UICC according to 3G TS 31.101 [11].

5.2 USIM security related procedures

5.2.1 Authentication algorithms computation

The ME selects a USIM application and uses the AUTHENTICATE command (see 7.1.1). The response is sent to the ME (in case of the T=0 protocol when requested by a subsequent GET RESPONSE command).

5.2.2 IMSI request

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

5.2.3 Access control information request

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

5.2.4 HPLMN search period request

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

5.2.5 Location information

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

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

In the case when updating EF_{LOCI} with data containing the TMSI value and the card reports the error '6581' (Memory Problem), the ME shall terminate 3G operation.

5.2.6 Cipher and Integrity key

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

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

5.2.7 Forbidden PLMN

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

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

5.2.8 LSA information

This subclause is expected to be defined in the release 2000 version of the present document.

5.2.9 User Identity Request

The ME selects a USIM and performs the reading procedure with EF_{IMSI}.

5.2.10 GSM Cipher key

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

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

5.2.11 GPRS Cipher key

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

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

5.2.12 Initialisation value for Hyperframe number

Request: The ME performs the reading procedure with $EF_{START-HFN}$.

Update: The ME performs the updating procedure with $EF_{START-HFN}$.

5.2.13 Maximum value of START

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

5.2.14 HPLMN selector with Access Technology request

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

5.3 Subscription related procedures

5.3.1 Phone book procedures

5.3.1.1 Initialisation

The ME first reads the content of EF_{PBR} to determine the configuration phonebook. If the EF_{IAP} file is indicated in EF_{PBR} following tag 'A8' the ME reads the content of EF_{IAP} in order to establish the relation ship between the content in the files indicated using tag 'A9' and files indicated by tag 'A8'. The ME may read the contents of the phone book related files in any order.

5.3.1.2 Creation/Deletion of information

In order to avoid unlinked data to introduce fragmentation of the files containing phone book data the following procedures shall be followed when creating a new entry in the phone book. The data related to EF_{ADN} is first stored in the relevant record. As the record number is used as a pointer the reference pointer is now defined for the entry. The

rule for storing additional information for an entry is that the reference pointer shall be created before the actual data is written to the location.

In case of deletion of a complete or part of an entry the data shall be deleted first followed by the reference pointer for that data element. In case of deletion of a complete entry the contents of EF_{ADN} is the last to be deleted.

5.3.1.3 Hidden phone book entries

If a phone book entry is marked as hidden by means of EF_{PBC} the ME first prompts the user to enter the 'Hidden Key'. The key presented by the user is compared against the value that is stored in the corresponding $EF_{Hiddenkey}$. Only if the presented and stored hidden key are identical the ME displays the data stored in this phone book entry. Otherwise the content of this phone book entry is not displayed by the ME.

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

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

5.3.2 Dialling numbers

The following procedures may not only be applied to EF_{ADN} and its associated extension files EF_{CCP1} and EF_{EXT1} as described in the procedures below, but also to EF_{FDN}, EF_{MSISDN}, EF_{LND}, EF_{BDN}, $EF_{SDN,}$ $EF_{OCI,}$ $EF_{ICI,}$ EF_{OCT} and EF_{ICT} and their associated extension files. If these files are not allocated and activated, as denoted in the USIM service table, the current procedure shall be aborted and the appropriate EFs shall remain unchanged.

As an example, the following procedures are described as applied to ADN.

Requirement: Service n°1 "available".

- Service n°2 for FDN.
- Service n°21 for MSISDN.
- Service n°4 for SDN.
- Service n°6 for BDN.

Update: The ME analyses and assembles the information to be stored as follows (the byte identifiers used below correspond to those in the definition of the relevant EFs in the present document):

i) The ME identifies the Alpha-tagging, Capability/Configuration Identifier and Extension1 Record Identifier.

ii) The dialling number/SSC string shall be analysed and allocated to the bytes of the EF as follows:

- if a "+" is found, the TON identifier is set to "International";
- if 20 or less "digits" remain, they shall form the dialling number/SSC string;
- if more than 20 "digits" remain, the procedure shall be as follows:

  Requirement:

  - Service n°1 "available".
  - Service n°2 for FDN.
  - Service n°4 for SDN.
  - Service n°6 for BDN.

- The ME seeks for a free record in EF_{EXT1}. If an Extension1 record is not marked as "free", the ME runs the Purge procedure. If an Extension1 record is still unavailable, the procedure is aborted.
- The first 20 "digits" are stored in the dialling number/SSC string. The value of the length of BCD number/SSC contents is set to the maximum value, which is 11. The Extension1 record identifier is coded with the associated record number in the EF_{EXT1}. The remaining digits are stored in the selected Extension1 record where the type of the record is set to "additional data". The first byte of the Extension1 record is set

with the number of bytes of the remaining additional data. The number of bytes containing digit information is the sum of the length of BCD number/SSC contents of EF_{ADN} and byte 2 of all associated chained Extension1 records containing additional data.

iii) If a called party subaddress is associated to the ADN/SSC the procedure shall proceed as follows:

- Requirement:
  - Service n°1 "available".
  - Service n°2 for FDN.
  - Service n°4 for SDN.
  - Service n°6 for BDN.
- If the length of the called party subaddress is less than or equal to 11 bytes (see 3G TS 24.008 [9] for coding):
  - The ME seeks for a free record in EF_{EXT1}. If an Extension1 record is not marked as "free", the ME runs the Purge procedure. If an Extension1 record is still unavailable, the procedure is aborted.
  - The ME stores the called party subaddress in the Extension1 record, and sets the Extension1 record type to "called party subaddress".
  - If the length of the called party subaddress is greater than 11 bytes (see 3G TS 24.008 [9] for coding):
    - The ME seeks for two free records in EF_{EXT1}. If no such two records are found, the ME runs the Purge procedure. If two Extension1 records are still unavailable, the procedure is aborted.
    - The ME stores the called party subaddress in the two Extension1 records. The identifier field in the Extension1 record containing the first part of the subaddress data is coded with the associated EF_{EXT1} record number containing the second part of the subaddress data. Both Extension1 record types are set to "called party subaddress".

Once i), ii), and iii) have been considered the ME performs the updating procedure with EF_{ADN}. If the USIM has no available empty space to store the received ADN/SSC, or if the procedure has been aborted, the ME advises the user.

For reasons of memory efficiency, the ME may analyse all Extension1 records to recognise if the additional or subaddress data to be stored is already existing in EF_{EXT1}. In this case, the ME may use the existing chain or the last part of the existing chain from more than one ADN. The ME is only allowed to store extension data in unused records. If existing records are used for multiple access, the ME shall not change any data in those records to prevent corruption of existing chains.

Erasure: The ME sends the identification of the information to be erased. The content of the identified record in EF_{ADN} is marked as "free".

Request: The ME sends the identification of the information to be read. The ME shall analyse the data of EF_{ADN} to ascertain, whether additional data is associated in EF_{EXT1} or EF_{CCP}. If necessary, then the ME performs the reading procedure on these EFs to assemble the complete ADN/SSC.

Purge: The ME shall access each EF which references EF_{EXT1} (EF_{EXT2}) for storage and shall identify records in these files using extension data (additional data or called party subaddress). Note that existing chains have to be followed to the end. All referred Extension1 (Extension2) records are noted by the ME. All Extension1 (Extension2) records not noted are then marked by the ME as "free" by setting the whole record to 'FF'.

NOTE: Dependent upon the implementation of the ME, and in particular the possibility of erasure of ADN/SSC records by Phase 1 MEs, which have no knowledge of the EF_{EXT1}, it is possible for Extension1 records to be marked as "used space" (not equal to 'FF'), although in fact they are no longer associated with an ADN/SSC record.

The following three procedures are only applicable to service n°2 (FDN).

FDN capability request. The ME shall check the state of service n°2, i.e. if FDN is "enabled" or "disabled". If FDN is enabled, the ME shall only allow outgoing calls as defined in the fixed number dialling description in TS 22.101 [24].

To ascertain the state of FDN, the ME shall check in EF_{UST} and EF_{EST} if FDN is enabled (service activated and available). In all other cases service n°2 is disabled.

FDN enabling is done by activating the FDN service in EF_{EST}.

FDN disabling is done by deactivating the FDN service in EF_{EST}.

The following three procedures are only applicable to service n°6 (BDN).

- BDN capability request. The ME shall check the state of service n°6, i.e. if BDN is "enabled" or "disabled". To ascertain the state of BDN, the ME shall check in EF_{UST} and EF_{EST} if BDN is "enabled" (service available and activated). In all other cases, the BDN service is "disabled".
- BDN enabling is done by activating the BDN service in EF_{EST}.
- BDN disabling is done by deactivating the BDN service in EF_{EST}.

5.3.3 Short messages

- Requirement: Service n°10 "available".
- Request: The USIM seeks for the identified short message. If this message is found, the ME performs the reading procedure with EF_{SMS}.
- If service n°10 is "available" and the status of the SMS is '1D' (status report requested, received and stored in EF_{SMSR}), the ME performs the reading procedure with the corresponding record in EF_{SMSR}. If the ME does not find a corresponding record in EF_{SMSR}, then the ME shall update the status of the SMS with '19' (status report requested, received but not stored in EF_{SMSR}).
- If the short message is not found within the USIM memory, the USIM indicates that to the ME.
- Update: The ME looks for the next available area to store the short message. If such an area is available, it performs the updating procedure with EF_{SMS}.
- If there is no available empty space in the USIM to store the received short message, a specific MMI will have to take place in order not to loose the message.
- Erasure: The ME will select in the USIM the message area to be erased. Depending on the MMI, the message may be read before the area is marked as "free". After performing the updating procedure with EF_{SMS}, the memory allocated to this short message in the USIM is made available for a new incoming message. The memory of the USIM may still contain the old message until a new message is stored in this area.
- If service n°11 is "available" and the status of the SMS is '1D' (status report requested, received and stored in EF_{SMSR}), the ME performs the erasure procedure for EF_{SMSR} with the corresponding record in EF_{SMSR}.

5.3.4 Advice of charge

- Requirement: Service n°13 "available".
- Accumulated Call Meter.
- Request: The ME performs the reading procedure with EF_{ACM}. The USIM returns the last updated value of the ACM.
- Initialisation: The ME performs the updating procedure with EF_{ACM} using the new initial value.
- Increasing: The ME performs the increasing procedure with EF_{ACM} sending the value which has to be added.

Accumulated Call Meter Maximum Value.

- Request: The ME performs the reading procedure with EF_{ACMmax}.
- Initialisation: The ME performs the updating procedure with EF_{ACMmax} using the new initial maximum value.

Price per Unit and Currency Table (PUCT).

- Request: The ME performs the reading procedure with EF_{PUCT}.
- Update: The ME performs the updating procedure with EF_{PUCT}.

5.3.5 Capability configuration parameters

- Requirement: Service n°14 "available".
- Request: The ME performs the reading procedure with EF_{CCP}.
- Update: The ME performs the updating procedure with EF_{CCP}.
- Erasure: The ME sends the identification of the requested information to be erased. The content of the identified record in EF_{CCP} is marked as "free".

5.3.6 User controlled PLMN selector with Access Technology

- Requirement: Service n°20 "available".
- Request: The ME performs the reading procedure with $EF_{PLMNwACT}$.
- Update: The ME performs the updating procedure with $EF_{PLMNwACT}$.

5.3.7 Cell broadcast message identifier

- Requirement: Service n°15 "available".
- Request: The ME performs the reading procedure with EF_{CBMI}.
- Update: The ME performs the updating procedure with EF_{CBMI}.

5.3.8 Group identifier level 1

- Requirement: Service n°17 "available".
- Request: The ME performs the reading procedure with EF_{GID1}.

5.3.9 Group identifier level 2

Requirement: Service n°18 "available".

Request: The ME performs the reading procedure with EF_{GID2}.

5.3.10 Service provider name

Requirement: Service n°19 "available".

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

5.3.11 Enhanced multi level precedence and pre-emption service

Requirement: Service n°24 "available".

Enhanced Multi Level Precedence and Pre-amption.

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

Automatic Answer on eMLPP service.

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

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

5.3.12 Cell broadcast message identifier ranges

Requirement: Service n°16 "available".

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

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

5.3.13 Short message status report

- Requirement: Service n°11 "available".
- Request: If the status of a stored short message indicates that there is a corresponding status report, the ME performs the search record function with EF_{SMSR} to identify the record containing the appropriate status report. The ME performs the reading procedure with EF_{SMSR}.
- Update: If a status report is received, the ME first seeks within the SMS record identifiers of EF_{SMSR} for the same record number it used for the short message in EF_{SMS}. If such a record identifier is found in EF_{SMSR}, it is used for storage. If such a record identifier is not found, then the ME seeks for a free entry in EF_{SMSR} for storage. If no free entry is found the ME runs the Purge procedure with EF_{SMSR}. If there is still no free entry, the status report is not stored.
- If the ME found an appropriate record in EF_{SMSR} for storage, it updates the record with the status report setting the record identifier in EF_{SMSR} to the appropriate record number of the short message in EF_{SMS}.
- The status in EF_{SMS} is updated accordingly by performing the update procedure with EF_{SMS}.
- Erasure: The ME runs the update procedure with EF_{SMSR} by at least storing '00' in the first byte of the record. The ME may optionally update the following bytes with 'FF'.

Purge: The ME shall read the SMS record identifier (byte 1) of each record of EF_{SMSR}. With each record the ME checks the corresponding short messages in EF_{SMS}. If the status (byte 1) of the corresponding SMS is not equal '1D' (status report requested, received and stored in EF_{SMSR}), the ME shall perform the erasure procedure with the appropriate record in EF_{SMSR}.

5.3.14 APN Control List

Requirement: Service n°35 "available".

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

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

Enabling: The ME activates service n°3 in EF_{EST} (bit n°3 set to "1").

Disabling: The ME deactivates service n°3 in EF_{EST} (bit n°3 set to "0").

When the APN Control List service is enabled, the ME shall check that the entire APN of any PDP context is listed in EF_{ACL} before requesting this PDP context activation from the network. If the APN is not present in EF_{ACL}, the ME shall not request the corresponding PDP context activation from the network.

In the case that the APN Control List is enabled and no APN is indicated in the PDP context request, indicating that a network provided APN is to be used, then the ME shall only request the PDP context activation if "network provided APN" is contained within EF_{ACL}.

5.3.15 Depersonalisation Control Keys

Requirement: Service n°36 "available".

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

5.3.16 Co-operative Network List

Requirement: Service n°37 "available".

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

5.3.17 CPBCCH information

Requirement: Service n°39 "available".

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

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

5.3.18 Investigation Scan

Requirement: Service n°40 "available".

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

5.3.19 Enabled Services Table Request

Requirement: Service n°34 "available".

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

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

5.3.20 Operator controlled PLMN selector with Access Technology

Requirement: Service n°42 "available".

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

5.3.21 HPLMN selector with Access Technology

Requirement: Service n°43 "available".

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

5.3.22 RPLMN last used Access Technology

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

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

5.3.23 Network Parameter information

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

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

5.4 USAT related procedures

5.4.1 Data Download via SMS-PP

Requirement: USIM Service n°28 "available".

The procedures and commands for Data Download via SMS-PP are defined in 3G TS 31.111 [12].

5.4.2 Image Request

The terminal sends the identification of the information to be read. The terminal shall analyse the data of EF_{IMG} to identify the files containing the instances of the image. If necessary, then the terminal performs READ BINARY commands on these files to assemble the complete image instance data.

5.4.3 Data Download via SMS-CB

Requirement: USIM Service n°29 "available".

The ME shall perform the reading procedure with EF_{CBMID}, and add the message identifiers to the Cell Broadcast search list. On receiving a cell broadcast message the procedure defined in 3G TS 31.111 [12] applies.

5.4.4 Call Control by USIM

Requirement: USIM Service n°30 "available".

The procedures and commands for Call Control by USIM are defined in 3G TS 31.111 [12]. It is mandatory for the ME to perform the procedures if it has indicated that it supports Call Control by USIM in the TERMINAL PROFILE command.

5.4.5 MO-SMS control by USIM

Requirement: USIM Service n°31 "available".

The procedures and commands for MO-SMS control by USIM are defined in 3G TS 31.111 [12]. It is mandatory for the ME to perform the procedures if it has indicated that it supports MO-SMS control by USIM in the TERMINAL PROFILE command.

5.5 MExE related procedures

MExE is an optional feature. The higher level procedures, and contents and coding of the commands are given in TS 23.057 [30]. Procedures relating to the transmission of commands and responses across the USIM/ME interface are given in this section. A USIM or ME supporting MExE shall conform to the requirements given in this section.

5.5.1 MExE ST

Requirement: Service n°41 (MExE) "allocated and activated".
Request: The ME performs the reading procedure with $EF_{MExE-ST}$

5.5.2 Operator root public key

Requirement: Service n°41 (MExE) "allocated and activated" and MExE ST service n°1 (EF_{ORPK})" allocated and activated".
Request: The ME performs the reading procedure with EF_{ORPK}. The ME shall analyse the data of EF_{ORPK} (sub-clause 4.4.1.4.2) to identify the files containing the certificate instances. If necessary, then the ME performs READ BINARY commands on these files to assemble the complete certificate instance data.

5.5.3 Administrator root public key

Requirement: Service n°41 (MExE) "allocated and activated" and MExE ST service n°2 (EF_{ARPK}) "allocated and activated".
Request: The ME performs the reading procedure with EF_{ARPK}. The ME shall analyse the data of EF_{ARPK} (sub-clause 4.4.1.4.3) to identify the file containing the certificate instance. If necessary, then the ME performs READ BINARY commands on this file to assemble the complete certificate instance data.

5.5.4 Third Party root public key(s)

Requirement: Service n°41 (MExE) "allocated and activated" and MExE ST service n°3 (EF_{TPRPK}) "allocated and activated".
Request: The ME performs the reading procedure with EF_{TPRPK}. The ME shall analyse the data of EF_{TPRPK} (sub-clause 4.4.1.4.4) to identify the files containing the certificate instances. If necessary, then the ME performs READ BINARY commands on these files to assemble the complete certificate instance data.

5.5.5 Trusted Key/Certificates Data Files

Requirement: Service n°41 (MExE) "allocated and activated.
Request: The ME performs the reading procedure with EF_{TKCDF}. The ME shall analyse the data of EF_{TKCDF} and, if necessary, perform READ BINARY commands on these files

6 Security features

The security aspects of 3G are specified in 3G TS 33.102 [13] and 3G TS 33.103 [14]. This clause gives information related to security features supported by the USIM to enable the following:

- authentication of the USIM to the network;
- authentication of the network to the USIM;
- authentication of the user to the USIM;
- data confidentiality over the radio interface;
- file access conditions;
- conversion functions to derive GSM parameters.

6.1 Authentication and key agreement procedure

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

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

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

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

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

6.2 Cryptographic Functions

The names and parameters of the cryptographic functions supported by the USIM are defined in 3G TS 33.102 [13]. These are:

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

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

6.3 GSM Conversion Functions

To gain GSM access, the USIM provides the conversion functions c2 and c3. These functions derive the required GSM parameters (SRES, cipher key Kc) from available 3G parameters.

6.4 User verification and file access conditions

The USIM application uses 2 PINs for user verification, PIN and PIN2. PIN2 is used only in the ADF. The PIN and PIN2 are mapped into key references as defined in 3G TS 31.101 [11]. Each key reference is associated with a usage qualifier as defined in ISO/IEC7816-9 [26]. The PIN status is indicated in the PS_DO, which is part of the FCP response when an ADF/DF is selected. The coding of the PS_DO is defined in 3G TS 31.101 [11].

PIN and PIN2 are coded on 8 bytes. Only (decimal) digits (0-9) shall be used, coded in CCITT T.50 [23] with bit 8 set to zero. The minimum number of digits is 4. If the number of digits presented by the user is less than 8 then the ME shall pad the presented PIN with 'FF' before sending it to the USIM.

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

The security architecture as defined in 3G TS 31.101 [11] applies to the USIM application with the following definitions and additions.

- The USIM application shall use key reference '01' as PIN and key reference '81' as PIN2. For access to DFTelecom the PIN shall be verified. Access with PIN2 is limited to the USIM application.
- The only valid usage qualifier is '08' which means user authentication knowledge based (PIN) as defined in ISO/IEC 7816-9 [26]. The terminal shall support the multi-application capabilities as defined in 31.101 [11].
- Every file in the USIM application shall have a reference to an access rule stored in EF_{ARR}.
- Every file under $DF_{Telecom}$ shall have a reference to an access rule stored in EF_{ARR} under $DF_{Telecom}$.
- A multi-application capability UICC (from the security context point of view) shall support the referenced format using SEID as defined in 3G TS 31.101 [11].
- A multi-application capability UICC (from the security context point of view) shall support the replacement of a USIM application PIN with the Universal PIN, key reference '01', as defined in 3G TS 31.101 [11]. Only the Universal PIN is allowed as a replacement.
- A terminal shall support the use of level 1 and level 2 user verification requirements as defined in 3G TS 31.101 [11].
- A terminal shall support the replacement of a USIM application PIN with the Universal PIN, key reference '01', as defined in 3G TS 31.101 [11].
- A terminal shall support the security attributes defined using tag's '8C', 'AB' and '8B' as defined in 3G TS 31.101 [11]. In addition both the referencing methods indicated by tag '8B' shall be supported as defined in 3G TS 31.101 [11].

The access rule is referenced in the FCP using tag '8B'. The TLV object contains the file ID (the file ID of EF_{ARR}) and record number, or file ID (the file ID of EF_{ARR}), SEID and record number, pointer to the record in EF_{ARR} where the access rule is stored. Each SEID refers to a record number in EF_{ARR}. EFs having the same access rule use the same record reference in EF_{ARR}. For a example EF_{ARR}, see 3G TS 31.101 [11].

7 USIM Commands

7.1 AUTHENTICATE

7.1.1 Command description

The function is used 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 related to a particular USIM and shall not be executable unless the USIM or any sub-directory has been selected as the Current Directory and a successful PIN verification procedure has been performed (see clause 5).

The function can be used in two different contexts:

- a 3G security context, when 3G authentication vectors (RAND, 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).

7.1.1.1 3G security context

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

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

Next the USIM verifies that the received sequence number SQN is previously unused. If it is unused and its value is lower than SQN_{MS}, it shall still be accepted if it is among the last 32 sequence numbers generated. A possible verification method is described in TS 33.102 [13].

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

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, where:
AUTS = Conc(SQN_{MS}) || MACS;
Conc(SQN_{MS}) = $SQN_{MS} \oplus f5^*_K$(RAND) is the concealed value of the counter *SQN_{MS}* in the USIM; and.
MACS = $f1^*_K$(SQN_{MS} || RAND || AMF) where:
RAND is the random value received in the current user authentication request;
the AMF assumes a dummy value of all zeroes so that it does not need to be transmitted in clear in the resynchronisation message.

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

The use of AMF is HE specific and while processing the command, the content of the AMF has to be interpreted in the appropriate manner. The AMF may e.g. be used for support of multiple algorithms or keys or for changing the size of lists, see 3G TS 33.102 [13].

If Service n°27 is "available", the USIM calculates the GSM response parameter K_C, using the conversion function defined in 3G TS 33.102 [13].

Input:

- RAND, AUTN (AUTN := SQN $\oplus$ AK || AMF || MAC).

Output:

- RES, CK, IK if Service n°27 is "not available".

or

- RES, CK, IK, K_C if Service n°27 is "available".

or

- AUTS.

7.1.1.2 GSM security context

USIM operation in an GSM security context is supported if Service n°38 is "available".

The USIM computes RES = $f2_K$ (RAND), the cipher key CK = $f3_K$ (RAND) and the integrity key IK = $f4_K$ (RAND). Next the USIM calculates the GSM response parameters SRES and K_C, using the conversion functions defined in 3G TS 33.102 [13].

Input:

- RAND.

Output:

- SRES; K_C.

7.1.2 Command parameters and data

Code	Value
CLA	As specified in 3G TS 31.101
INS	'88'
P1	'00'
P2	See table below
Lc	See below
Data	See below
Le	'00', or maximum length of data expected in response

Parameter P2 specifies the authentication context as follows:

Coding of the reference control P2

Coding b8-b1	Meaning
'1-------'	Specific reference data (e.g. DF specific/application dependant key)
'-XXXXXX-'	'000000'
'-------X'	Authentication context: 0 GSM context 1 3G context

All other codings are RFU.

Command parameters/data:

Byte(s)	Description	Length
1	Length of RAND (L1)	1
2 to (L1+1)	RAND	L1
(L1+2)	Length of AUTN (L2) (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 3G 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 3G 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.

7.2 Void

7.3 Status Conditions Returned by the UICC

Status of the card after processing of the command is coded in the status bytes SW1 and SW2. This subclause specifies coding of the status bytes in the following tables.

7.3.1 Security management

SW1	SW2	Error description
’98’	’62’	- Authentication error, incorrect MAC
’98’	’64	- Authentication error, GSM security context not supported

7.3.2 Status Words of the Commands

The following table shows for each command the possible status conditions returned (marked by an asterisk *). Status conditions of GSM and USIM applications are on the left and right sides of the table, respectively.

Commands and status words

AUTHENTICATE	
	90 00
	91 XX
*	9F XX
	61XX#
	93 00
	92 0X
*	65 81
	94 00
	94 02
	94 04
*	94 08
	98 02
*	69 82
	98 08
	98 10
	98 40
	98 50
*	98 62
*	98 64
*	67 XX
*	6B XX
	6D XX
*	6E XX
*	6F XX
	62 81
	62 83
	62 82
	62 84
	62 00
	63 CX
	69 81
*	69 84
*	69 85
	69 86
	6A 81
	6A 82
	6A 83
	6A 84
	6A 85
*	6A 86
	6A 87
*	6A 88
	6C XX

7.4 VERIFY command

The VERIFY command is used to verify the user as defined in 3G TS 31.101 [11]. For the USIM application during a 3G session the parameter P2 is restricted to the following values.

- '01' indicating verification of the PIN;
- '81' indicating verification of PIN2.

NOTE For administrative purposes any level 5 or level 6 value as specified in 3G TS 31.101 [11] may be used.

After 3 unsuccessful verification attempts, not necessarily in the same session the PINs blocked. The blocked status is indicated in the response to the VERIFY command (0 attempts left) see 3G TS 31.101 [11].

8 UICC Characteristics

8.1 Voltage classes

A UICC holding a USIM application shall support at least two consecutive voltage classes as defined in 3G TS 31.101 [11], e.g. AB or BC. If the UICC supports more than two classes, they shall all be consecutive, e.g. ABC.

8.2 File Control Parameters (FCP)

This subclause defines the contents of the data objects which are part of the FCP information where there is a difference compared to the values as specified in 3G TS 31.101 [11]. This section also specifies values for data objects in the FCP information where there is no exact value given in TS 31.101 [11] and there is a need for such from the USIM application point of view.

8.2.1 Minimum application clock frequency

This data object is indicated by tag '82' in the proprietary constructed data object in the FCP information, identified by tag 'A5', as defined in 3G TS 31.101 [11]. This data object specifies the minimum clock frequency to be provided by the terminal during the USIM session. The value indicated in this data object shall not exceed 3 MHz, corresponding to '1E'. The terminal shall use a clock frequency between the value specified by this data object and the maximum clock frequency for the UICC as defined in 3G TS 31.101 [11]. If this data object is not present in the FCP response or the value is 'FF' then the terminal shall assume that the minimum clock frequency is 1 MHz.

Annex A (informative): EF changes via Data Download or 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	
'2F05'	Preferred languages	Yes
'2F06'	Access rule reference	
'2FE2'	ICC identification	No
'4F20'	Image data	Yes
'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
'4F75'	CPBCCH Information	No
'4F76	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
'6F05'	Language indication	Yes
'6F07'	IMSI	Caution (Note 1)
'6F08'	Ciphering and integrity keys	No
'6F09'	Ciphering and integrity keys for packet switched domain	No
'6F20'	Ciphering key Kc	No
'6F2C'	De-personalization Control Keys	Caution
'6F31'	HPLMN 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
'6F4F'	Extended Capability configuration parameters	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
'6F44'	Last number dialled	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
'6F52'	GPRS Ciphering key KcGPRS	No
'6F54'	SetUp Menu Elements	Yes
'6F56'	Enabled services table	
'6F57'	Access point name control list	
'6F58'	Comparison method information	
'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
'6F63'	RPLMN last used 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
'6FB5'	Enhanced Multi Level Pre-emption and Priority	Yes
'6FB6'	Automatic Answer for eMLPP Service	Yes
'6FB7'	Emergency Call Codes	Caution
'6FC2'	Group identity	No
'6FC3'	Key for hidden phone book entries	
'6FC4'	Network Parameters	No

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

Annex B (normative): Image Coding Schemes

The following image coding schemes are applicable to rectangular raster images. Raster image points are assumed to be of square shape. They are numbered sequentially from 1 onwards, starting at the upper left corner, proceeding line by line downwards, each line in turn proceeding from left to right, and ending at the image's lower right corner.

The following example illustrates the numbering scheme for raster image points by showing how the corner points are numbered, assuming an image length of x points and an image height of y points.

B.1 Basic Image Coding Scheme

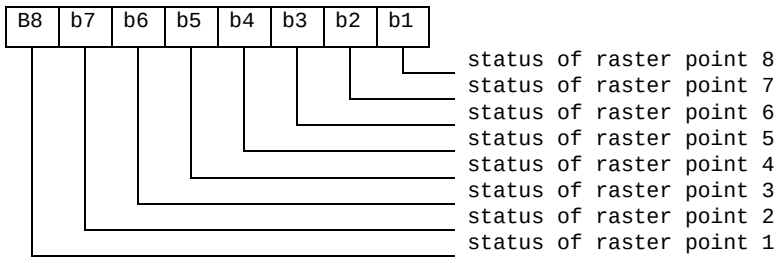
This coding scheme applies to rectangular raster images made up of raster points that are either set or not set. This coding scheme does not support any notion of colour. Image data are coded as follows:

Byte(s)	Description	Length
1	image width = X	1
2	image height = Y	1
3 to K+2	image body	K

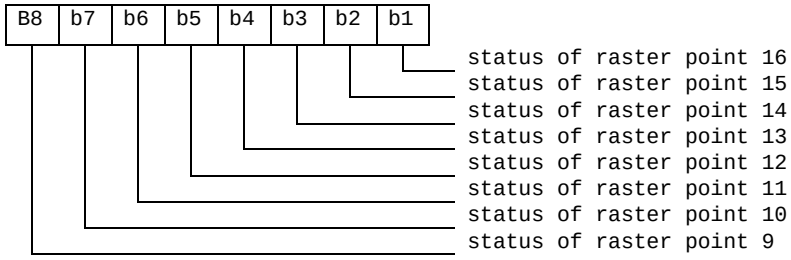
Coding of image body:

- The status of each raster image point is coded in one bit, to indicate whether the point is set (status = 1) or not set (status = 0).

Byte 1:



Byte 2:



etc.

Unused bits shall be set to 1.

B.2 Colour Image Coding Scheme

This coding scheme applies to coloured rectangular raster images. Raster image point colours are defined as references into a colour look-up table (CLUT), which contains a subset of the red-green-blue colour space. The CLUT in turn is located in the same transparent file as the image instance data themselves, at an offset defined within the image instance data.

Image data are coded as follows:

Byte(s)	Description	Length
1	Image width = X	1
2	Image height = Y	1
3	Bits per raster image point = B	1
4	Number of CLUT entries = C	1
5 to 6	Location of CLUT (Colour Look-up Table)	2
7 to K+6	Image body	K

Bits per raster image point:

Contents:

- the number B of bits used to encode references into the CLUT, thus defining a raster image point's colour. B shall have a value between 1 and 8.

Coding:

- binary.

Number of entries in CLUT:

Contents:

- the number C of entries in the CLUT which may be referenced from inside the image body. CLUT entries are numbered from 0 to C-1. C shall have a value between 1 and 2**B.

Coding:

- binary. The value 0 shall be interpreted as 256.

Location of CLUT:

Contents:

- this item specifies where the CLUT for this image instance may be found. The CLUT is always located in the same transparent file as the image instance data themselves, at an offset determined by these two bytes.

Coding:

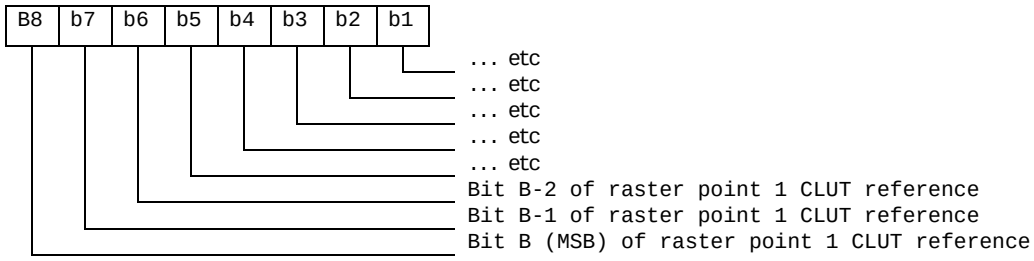
- Byte 1: high byte of offset into Image Instance File.
- Byte 2: low byte of offset into Image Instance File.

Image body:

Coding:

- each raster image point uses B bits to reference one of the C CLUT entries for this image instance. The CLUT entry being thus referenced yields the raster image point's colour.The image body is arrayed as for the Basic Colour Image Coding Scheme, that is, starting with the highest bit of the first raster image point's colour information.

Byte 1:



etc.

Unused bits shall be set to 1.

The CLUT (Colour Look-up Table) for an image instance with C colours is defined as follows:

Contents:

- C CLUT entries defining one colour each.

Coding:

- the C CLUT entries are arranged sequentially:

Byte(s) of CLUT	CLUT Entry
1-3	entry 0
...	...
3*(C-1) +1 to 3*C	Entry C-1

Each CLUT entry in turn comprises 3 bytes defining one colour in the red-green-blue colour space:

Byte(s) of CLUT enty	Intensity of Colour
1	Red
2	Green
3	Blue

A value of 'FF' means maximum intensity, so the definition 'FF' '00' 00' stands for fully saturated red.

NOTE 1: Two or more image instances located in the same file can share a single CLUT.

NOTE 2: Most MEs capable of displaying colour images are likely to support at least a basic palette of red, green, blue and white.

Annex C (informative): Structure of the Network parameters TLV objects

Structure of the GSM network parameter TLV object, 0<= m <=32

Tag	Length	Tag Currently Camped Frequency	Length	BCCH Frequency downlink		Tag Neighbour BCCH Frequency	Length	BCCH Neighbour Frequency 1		BCCH Neighbour Frequency 2		……		BCCH Neighbour Frequency m	
'A0'		'80'	'02'			'81'									

Structure of the FDD network parameter TLV object, 0 <= m <= 32

Tag	Length	Tag Intra frequency carrier	Length	Intra Frequency downlink carrier		Primary Scrambling code 1		Primary Scrambling code m		Tag Inter frequency carrier	Length	Inter Frequency downlink carrier		Primary Scrambling code n1	
'A1'		'80'								'81'					

Structure of the TDD network parameter TLV object, 0 <= m <= 32

Tag	Length	Tag Intra frequency carrier	Length	Intra Frequency downlink carrier		Primary Scrambling code 1		Primary Scrambling code m		Tag Inter frequency carrier	Length	Inter Frequency downlink carrier		Primary Scrambling code n1	
'A2'		'80'								'81'					

Annex D (informative): Tags defined in 31.102

Tag	Name of Data Element	Usage
'A0'	GSM cell information The following tags are encapsulated within 'A0': '80' GSM Camping Frequency data object '81' GSM Neighbour Frequency Information data object	Network Parameters (EF_{NETPAR})
'A1'	FDD cell information The following tags are encapsulated within 'A1': '80' FDD Intra Frequency data object '81' FDD Inter Frequency Information data object	Network Parameters (EF_{NETPAR})
'A2'	TDD cell information The following tags are encapsulated within 'A2': '80' TDD Intra Frequency data object '81' TDD Inter Frequency Information data object	Network Parameters (EF_{NETPAR})
'A8'	Indicator for type 1 EFs (amount of records equal to master EF) The following tags are encapsulated within 'A8': 'C0' EF_{ADN} data object 'C1' EF_{IAP} data object 'C3' EF_{SNE} data object 'C4' EF_{ANR} data object 'C5' EF_{PBC} data object 'C6' EF_{GRP} data object 'C9' EF_{UID} data object 'CA' EF_{EMAIL} data object	Phone Book Reference File (EF_{PBR})
'A9'	Indicator for type 2 EFs (EFs linked via the index administration file) The following tags are encapsulated within ' A9 ': 'C3' EF_{SNE} data object 'C4' EF_{ANR} data object 'CA' EF_{EMAIL} data object	Phone Book Reference File (EF_{PBR})
'AA'	Indicator for type 3 EFs (EFs addressed inside an object using a record identifier as a pointer) The following tags are encapsulated within 'AA': 'C2' EF_{EXT1} data object 'C7' EF_{AAS} data object 'C8' EF_{GAS} data object 'CB' EF_{CCP1} data object	Phone Book Reference File (EF_{PBR})
'DB'	Successful 3G authentication	Response to AUTHENTICATE
'DC'	Synchronisation failure	Response to AUTHENTICATE
'DD'	Access Point Name	APN Control List (EF_{ACL})

NOTE: the value 'FF' is an invalid tag value. For ASN.1 tag assignment rules see ISO/IEC 8825 [35]

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'
'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
'4FXX'	Capability configuration parameters 1	'FF…FF'
'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'
'6F05'	Language indication	'FF…FF'
'6F07'	IMSI	Operator dependant
'6F08'	Ciphering and integrity keys	'07FF…FF'
'6F09'	Ciphering and integrity keys for packet switched domain	'07FF…FF'
'6F20'	Ciphering key Kc	'FF...FF07'
'6F2C'	De-personalization control keys	'FF…FF'
'6F31'	HPLMN 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'
'6F52'	GPRS Ciphering key KcGPRS	'FF...FF07'
'6F54'	SetUp Menu Elements	Operator dependant
'6F55'	Extension 4	'FF...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	'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'
'6F65'	RPLMN last used Access Technology	'0000'
'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
'6FB5'	EMLPP	Operator dependant
'6FB6'	AaeM	'00'
'6FB7'	Emergency call codes	Operator dependant
'6FC2'	Group identity	'FFFFFFFF'
'6FC3'	Key for hidden phone book entries	'FF…FF'
'6FC4'	Network 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 3G TS 24.008 [9].

Annex F (informative): Examples of coding of LSA Descriptor files for SoLSA

This annex is expected to be defined in a later release of the present document.

Annex G (informative): Phonebook Example

This example phonebook has more than 254 entries. Additional number (3 additional numbers) information, second name and e-mail information can be added to each ADN entry. In addition each entry has a 2 byte Unique ID (UID) attached to it. The phonebook also contains three files that are shared EF_{EXT1}, EF_{AAS} and EF_{GAS}. These files are addressed from inside a file. EF_{EXT1} is addressed via $EF_{ADN,}$ EF_{ADN1}, EF_{AAS} is addressed via $EF_{ANRA1,}$ EF_{ANRA1} and EF_{GAS} is addressed via $EF_{GRP,}$ EF_{GRP1}. The phonebook supports two levels of grouping and hidden entries in $EF_{PBC.}$

Two records are needed in the phonebook reference file PBR '4F30' for supporting more than 254 entries. The content of the phonebook reference file PBR '4F30' records is as shown in table G.2. The structure of the $DF_{PHONEBOOK}$ is shown in table G.1.

The content of phonebook entries in the range from 1-508 is described in the tables G.3 and G.4.

Table G.1: Structure of EFs inside $DF_{PHONEBOOK}$

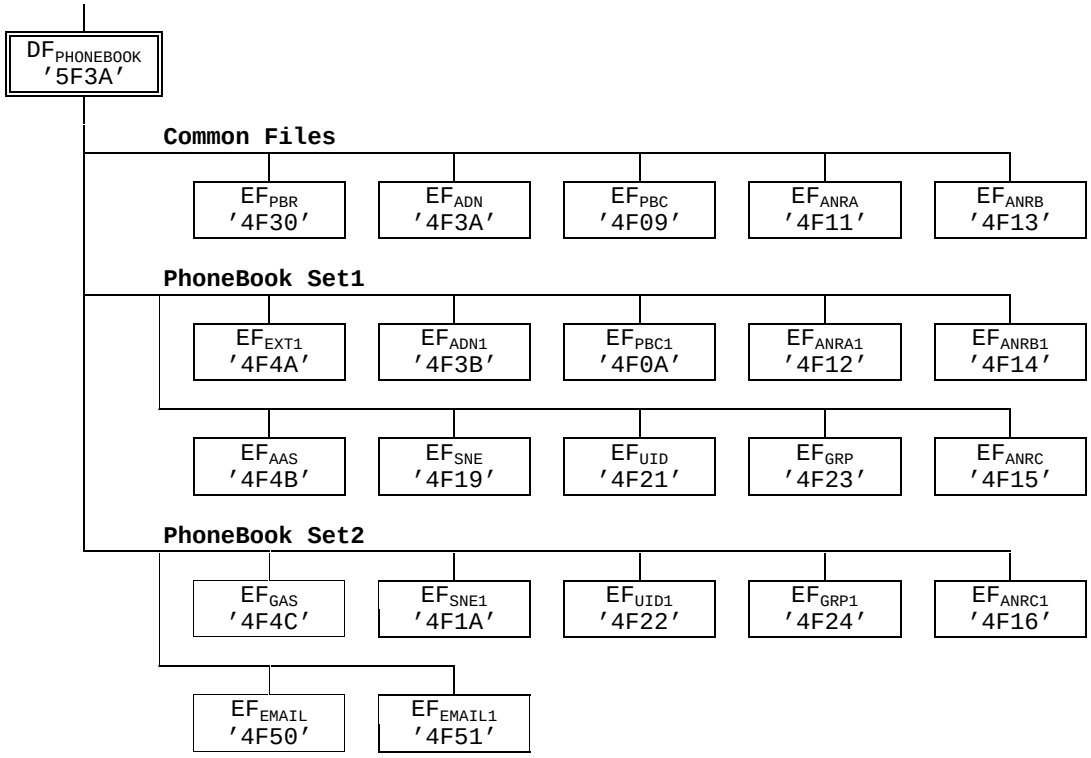


Table G.2: Contents of EF_{PBR}

Rec 1	Tag'A8'	L='26'	(for Phonebook Set1)										
	Tag'C0'	L='03'	'4F3A'	'01'	Tag'C5'	L='03'	'4F09'	'02'	Tag'C6'	L='02'	'4F23'	Tag'C4'	L='02'	'4F11'
	Tag'C4'	L='02'	'4F13'	Tag'C4'	L='02'	'4F15'	Tag'C3'	L='02'	'4F19'	Tag'C9'	L='02'	'4F21'		
	Tag'CA'	L='02'	'4F50'											
	Tag'AA'	L='0C'												
	Tag'C2'	L='02'	'4F4A'	Tag'C7'	L='02'	'4F4B'	Tag'C8'	L='02'	'4F4C'					

Rec 2 Tag'A8' L='24' (for Phonebook Set 2)

Tag'C0'	L='02'	'4F3B'	Tag'C5'	L='02'	'4F0A'	Tag'C6'	L='02'	'4F24'	Tag'C4'	L='02'	'4F12'	
Tag'C4'	L='02'	'4F14'	Tag'C4'	L='02'	'4F16'	Tag'C3'	L='02'	'4F1A'	Tag'C9'	L='02'	'4F22'	
Tag'CA'	L='02'	'4F51'										
Tag'AA'	L='0C'											
Tag'C2'	L='02'	'4F4A'	Tag'C7'	L='02'	'4F4B'	Tag'C8'	L='02'	'4F4C	'FF'	'FF'		

Table G.3: Structure of the 254 first entries in the phonebook

Phone book entry	ADN '4F3A' SFI '01'		PBC '4F09' SFI '02'	GRP '4F23'	ANRA '4F11'	ANRB '4F13'	ANRC '4F15'	SNE '4F19'	UID '4F21'	EXT1 '4F4A'	AAS '4F4B'	GAS '4F4C'	EMAIL '4F50'
# 1	ADN Content Bytes (1-(X+13))	EXT1 Ident. (Byte X+14): Rec '02'	Hidden (AID rec N° 3)	Rec n°1 Rec n°3 '00'	ANRA Rec n°1	ANRB Rec n°1	ANRC Rec n°1	Second Name Alpha String	UID	Rec '02'	Record numbers as defined in the ANRs	Record no.'s as defined in GRP	email address
# 2	ADN Content Bytes (1-(X+13))	EXT1 Ident. (Byte X+14): Rec '2A'	Not Hidden	Rec n°2 Rec n°1 Rec n°3	ANRA Rec n°2	ANRB Rec n°2	ANRC Rec n°2	Second Name Alpha String	UID	Rec '2A'	Record numbers as defined in the ANRs	Record no.'s as defined in GRP	email address
# 3													
:													
:													
:													
# 254													

Table G.4: Structure of phone book entries 255 to 508 (Rec 1-254)

Phone book entry	ADN1 '4F3B'		PBC1 '4F0A'	GRP1 '4F24'	ANRA1 '4F12'	ANRB1 '4F14'	ANRC1 '4F16'	SNE1 '4F1A'	UID1 '4F22'	EXT1 '4F4A'	AAS '4F4B'	GAS '4F4C'	EMAIL1 '4F51'
#255	ADN Content Bytes (1-(X+13))	EXT1 Ident. (Byte X+14): Rec '02'	Hidden (AID Rec n° 3)	Rec n°1 Rec n°3 '00'	ANRA1 Rec n°1	ANRB1 Rec n°1	ANRC1 Rec n°1	Second Name Alpha String	UID	Rec '02'	Record numbers as defined in the ANRs	Record no.'s as defined in GRP1	email address
#256	ADN Content Bytes (1-(X+13))	EXT1 Ident. (Byte X+14): Rec '2A'	Not Hidden	Rec n°2 Rec n°1 Rec n°3	ANRA1 Rec n°2	ANRB1 Rec n°2	ANRC1 Rec n°2	Second Name Alpha String	UID	Rec '2A'	Record numbers as defined in the ANRs	Record no.'s as defined in GRP1	email address
#257													
:													
:													
:													
#508													

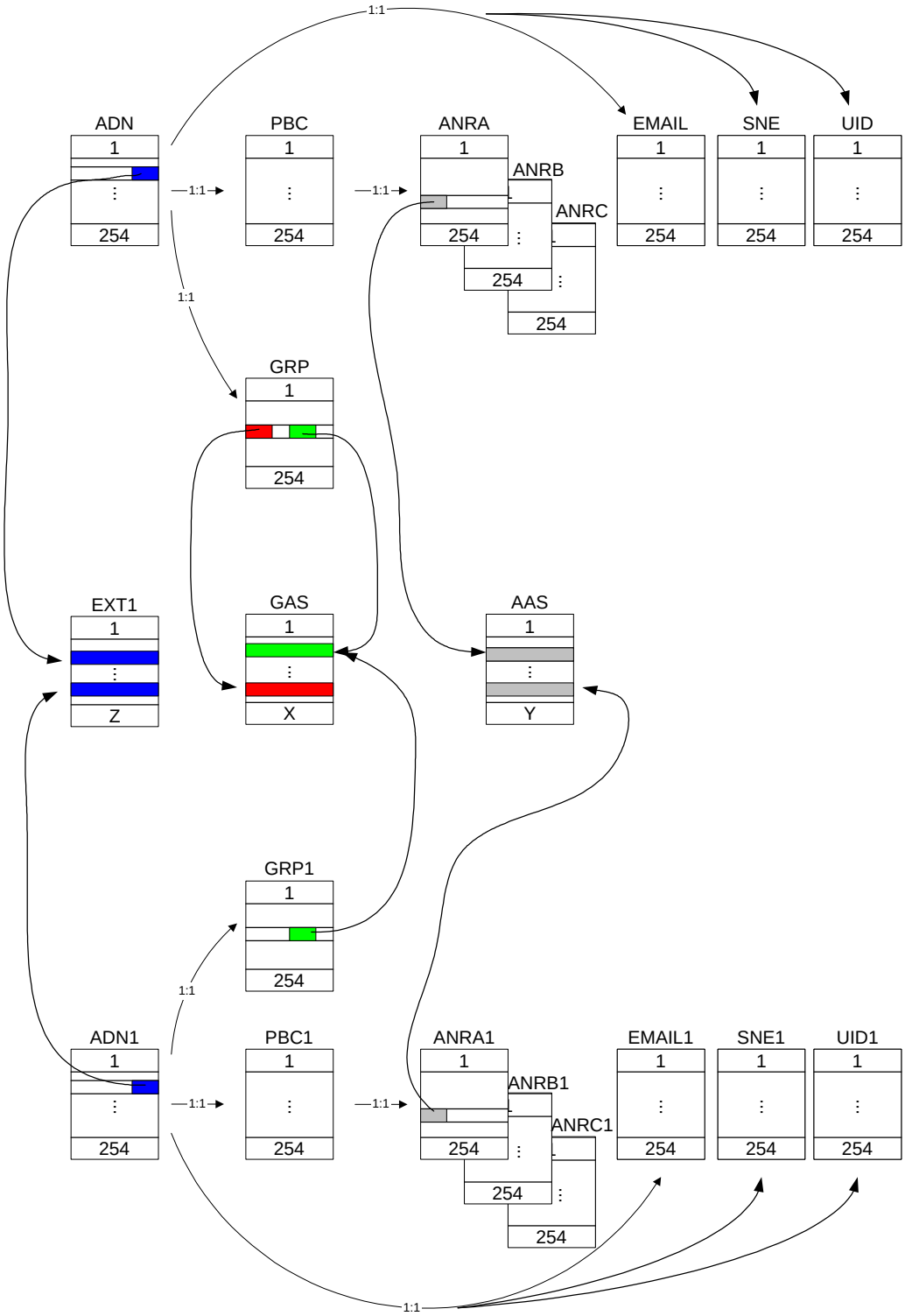


Figure G.1: Structure and Relations of the Example Phone Book

Annex H (normative): List of SFI Values

This annex lists SFI values assigned in this specification.

H.1 List of SFI Values at the USIM ADF Level

File Identification	SFI	Description
'6FB7'	'01'	Emergency call codes
'6F05'	'02'	Language indication
'6FAD'	'03'	Administrative data
'6F38'	'04'	USIM service table
'6F56'	'05'	Enabled services table
'6F78'	'06'	Access control class
'6F07'	'07'	IMSI
'6F08'	'08'	Ciphering and integrity keys
'6F09'	'09'	Ciphering and integrity keys for packet switched domain
'6F60'	'0A'	User PLMN selector
'6F7E	'0B'	Location information
'6F73'	'0C'	Packet switched location information
'6F7B'	'0D'	Forbidden PLMNs
'6F48'	'0E'	CBMID
'6F5B'	'0F'	Hyperframe number
'6F5C'	'10'	Maximum value of hyperframe number
'6F61'	'11'	Operator PLMN selector
'6F31'	'12'	HPLMN search period
'6F62'	'13'	Preferred HPLMN access technology
'6F80'	'14'	Incoming call information
'6F81'	'15'	Outgoing call information
'6F4F'	'16'	Capability configuration parameters 2
'6F06'	'17'	Access Rule Reference
'6F65'	'18'	RPLMN last used Access Technology

All other SFI values are reserved for future use.

H.2 List of SFI Values at the DF GSM-ACCESS Level

File Identification	SFI	Description
'4F20'	'01'	GSM Ciphering Key Kc
'4F52'	'02'	GPRS Ciphering Key KcGPRS

All other SFI values are reserved for future use.

Annex I (informative): USIM Application Session Activation / Termination

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

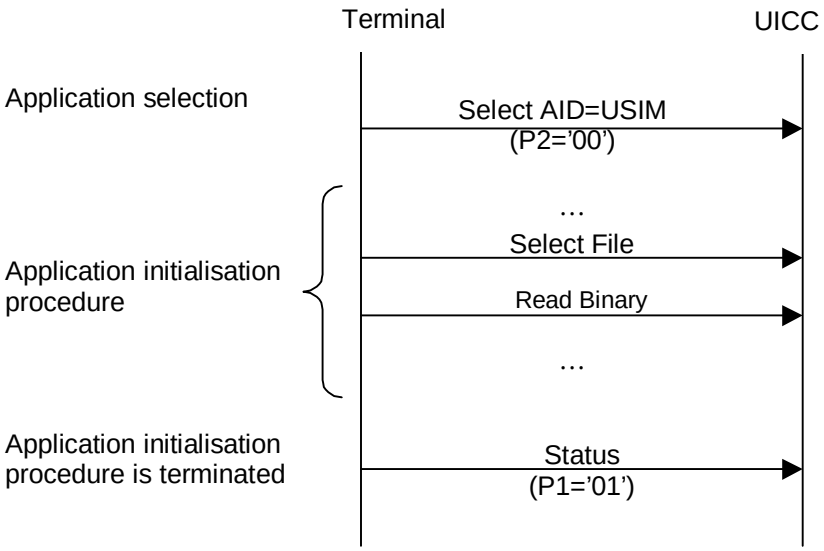


Figure I.1 USIM Application Session Activation procedure

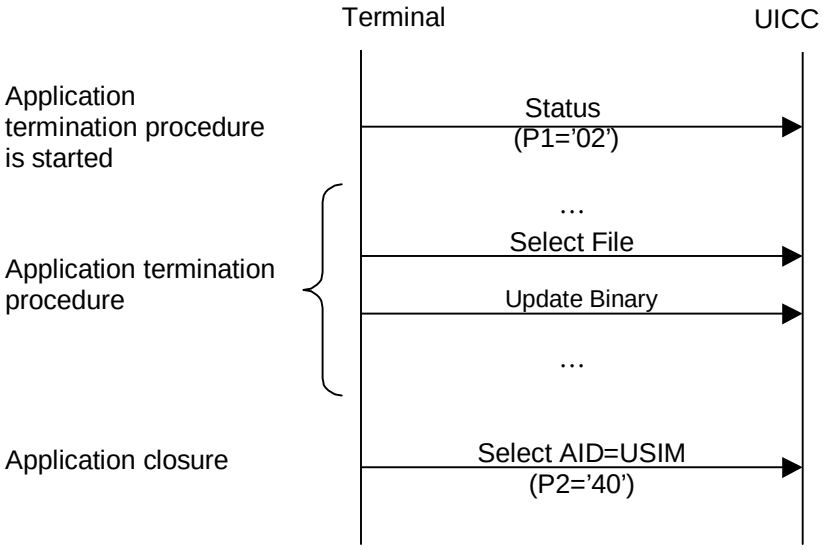


Figure I.2 USIM Application Session Termination procedure

Annex J (informative): Change history

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

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**Old**	**New**
2000-04	TP-07	TP-000014	001		F	Removal of EFappi	3.0.0	3.1.0
		TP-000014	002		F	Mandatory status for the EFs KcGPRS&LOCIGPRS		
		TP-000014	003		B	Implementation of FDN (Fixed Dialling Numbers)		
		TP-000014	004		B	Barred Dialling Numbers (BDN)		
		TP-000019	005	1	F	Emergency call codes		
		TP-000014	006		F	Mandatory status for the EF containing the Packet switched domain keys		
		TP-000014	007		F	Authentication		
		TP-000014	008		F	Alignment of terminology for authentication; addition of Kc-GPRS procedure		
		TP-000014	009		F	Correction to USIM specific FCP coding		
		TP-000014	011		F	Removal of SoLSA feature from Release 99		
		TP-000014	012		F	Alignment with 33.102 - AUTHENTICATE Command		
		TP-000014	014		B	Introduction of e-mail addresses in the Phone Book		
		TP-000014	015		C	APN control list		
		TP-000014	016		F	Phone book example		
		TP-000014	017		F	Alignment with GSM 11.11 R99		
		TP-000014	018		F	Alignment with 33.102 - Cipher key and integrity key lifetime		
		TP-000014	019		B	Operator controlled PLMN selection		
		TP-000014	020		C	Changes to 31.102 to align with 24.008		
		TP-000014	021		D	Collection of 31.102 editorial changes - part 1		
		TP-000014	023		F	Update to pre-personalisation values in Annex E		
		TP-000014	024		F	Update to "EF changes via Data Download or USAT applications" table in Annex A		
		TP-000014	025		B	Addition of security procedures		
		TP-000014	026		F	EF_LOCI access conditions		
2000-07	TP-08	TP-000095	028		F	removal of EUIC feature from R99	3.1.0	3.2.0
		TP-000095	029		F	Alignment with 33.102 Replace COUNT by START		
		TP-000095	031		F	Alignment to GSM 11.11 - Introduction of CPBCCH information and Investigation Scan indicator		
		TP-000095	032	2	B	HPLMN Length		
		TP-000095	033	1	F	LAI, RAI and CNL : alignment with GSM 04.08		
		TP-000095	034		F	Deletion of EF(LOCIGSM) and EF(LOCIGPRS)		
		TP-000095	035		F	Files to be read at USIM initialization		
		TP-000095	037		F	Alignment with 33.102 regarding key set identifier		
		TP-000095	038	2	F	Addition of SFI values to files read at initialisation of the USIM application		
		TP-000095	039		F	Support of voltage classes		
		TP-000110	040		B	Addition of files for MExE		
		TP-000095	041		F	Alignment with 33.102 regarding conversion functions		
		TP-000095	042		F	Addition of procedures for reading and updating the content of the Enabled Services Table.		
		TP-000095	043		F	Correction of the application activation termination procedures		
2000-10	TP-09	TP-000176	030		F	PLMN Selection additions	3.2.0	3.3.0
		TP-000176	036		F	Alignment to GSM 11.11 regarding Terminology		
		TP-000152	044	1	F	Correction to call information access conditions and correction of DF_GSM file IDs		
		TP-000152	045		F	Clarification of the type 3 links of the phonebook		
		TP-000152	046		F	Alignment of EF(CCP2) with EF(ECCP)		
		TP-000152	047	1	F	Correction of record length, editorial errors, missing FID		
		TP-000152	048		F	APN Control List coding		
		TP-000152	049		F	Alignment with TS 33.102 regarding authentication Sequence Numbers		
		TP-000152	050		F	Preferred language selection		
		TP-000152	051		F	Application Selection by partial AID		
		TP-000152	053		F	Phone book clarifications		
		TP-000182	054		F	Update condition for OPLMN Selector list		

Continued….

Change history (continued….)								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**Old**	**New**
2000-12	TP-10	TP-000203	055		F	Corrections and clarifications on Phonebook	3.3.0	3.4.0
		TP-000203	056		F	Miscellaneous clarifications and minor corrections		
		TP-000203	057		F	File-ID EFs of the phonebook		
		TP-000203	058		F	Correction of the phonebook example		
		TP-000203	059		F	Alignments with 3G TS 33.102 v3.6.0		
		TP-000203	062		F	Phonebook correction on CCPs		
		TP-000254	063		F	Storage of Network Parameters		
2001-03	TP-11	TP-010038	065	3	F	Correction and clarification of the APN Control feature	3.4.0	3.5.0
		TP-010038	066		F	Correction to default HPLMN RAT		
		TP-010038	067	2	F	Clarification on EF(ANR), EF(SNE) and EF(EMAIL)		
		TP-010038	068	1	F	Correction of the PROFILE download procedure		
		TP-010038	069		F	Clarification of EFARR access conditions		
		TP-010038	070		F	Indication of minimum clock frequency required by the USIM application		
		TP-010038	071		F	General corrections		
		TP-010038	072		F	Correction of the EF(UST) for Packet Domain		
		TP-010038	076		F	Usage of 'FF' in the EF(PBR)		
		TP-010038	077		F	Correction of EF_{ANR} (CR number changed from CR 076)		
		TP-010068	078		F	Correction of Tag values		

History

Document history		
V3.0.0	January 2000	Publication
V3.1.0	April 2000	Publication
V3.2.0	July 2000	Publication
V3.3.0	October 2000	Publication
V3.4.0	December 2000	Publication
V3.5.0	March 2001	Publication