ETSI TS 131 102 V3.0.0 (2000-01)

Technical Specification

Universal Mobile Telecommunications System (UMTS); Characteristics of the USIM Application (3G TS 31.102 version 3.0.0 Release 1999)

Reference

DTS/TSGT-0331102U

Keywords

UMTS

ETSI

Postal address

F-06921 Sophia Antipolis Cedex - FRANCE

Office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - 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

Internet

secretariat@etsi.fr
Individual copies of this ETSI deliverable
can be downloaded from
http://www.etsi.org
If you find errors in the present document, send your
comment to: editor@etsi.fr

Important notice

This ETSI deliverable may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2000.
All rights reserved.

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 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 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 or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables. The mapping of document identities is as follows:

For 3GPP documents:

3G TS | TR nn.nnn "<title>" (with or without the prefix 3G)

is equivalent to

ETSI TS | TR 1nn nnn "[Digital cellular telecommunications system (Phase 2+) (GSM);] Universal Mobile Telecommunications System; <title>

For GSM document identities of type "GSM xx.yy", e.g. GSM 01.04, the corresponding ETSI document identity may be found in the Cross Reference List on www.etsi.org/key

Contents

Foreword

This Technical Specification has been produced by the 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 this TS, 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:

0 working draft under the control of the relevant TSG Working Group

1 presented to TSG for information;

2 presented to TSG for approval;

3 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 specification;

Introduction

This specification 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 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.

This specification 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. This specification 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.

[1] 3G TS 21.111: "USIM and IC Card Requirements".

[2] 3G TS 22.011: "Service accessibility".

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

[4] 3G TS 22.030: "Man-Machine Interface (MMI) of the Mobile Station (MS)".

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

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

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

[8] 3G TS 23.073: "Support of Localised Service Area (SoLSA)".

[9] 3G TS 24.008: "Mobile Radio Interface Layer 3 specification".

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

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

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

[13] 3G TS 33.102: "3G Security Architecture".

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

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

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

[17] GSM 02.07: "Mobile Stations (MS) features".

[18] GSM 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".)

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

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
f6	Encryption function to encipher the IMSI

3.3 Abbreviations

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

3GPP	3rd Generation Partnership Project
AC	Access Condition
ADF	Application Dedicated File
AID	Application IDentifier
AK	Anonymity key
ALW	ALWays
AMF	Authentication Management Field
AoC	Advice of Charge
AuC	Authentication Centre
AUTN	Authentication token
BDN	Barred Dialling Number

CCP	Capability Configuration Parameter
CK	Cipher key
CS	Circuit switched
DF	Dedicated File
DO	Data Object
EF	Elementary File
EMUI	Encrypted Mobile User Identity
EUIC	Enhanced User Identity Confidentiality
FCI	File Control Information
FFS	For Further Study
GK	User group key
GMSI	Group Identity
GSM	Global System for Mobile communications
HE	Home Environment
ICC	Integrated Circuit Card
ID	IDentifier
IK	Integrity key
IMSI	International Mobile Subscriber Identity
K	USIM Individual key
KSI	Key Set Identifier
K_C	Cryptographic key used by the cipher A5
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
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
OFM	Operational Feature Monitor
PIN	Personal Identification Number
PS	Packet switched
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
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
XRES	Expected user RESponse

4 Contents of the Elementary Files (EF)

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; e.g. 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 three 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.

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 and for short message handling (e.g. screening of preferred languages in SMS-CB).

Identifier: '6F 05'	Structure: transparent	Optional	
File size: 2n bytes	Update activity: low		
Access Conditions: READ ALW UPDATE PIN DEACTIVATEDEACTIVATE 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 - 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

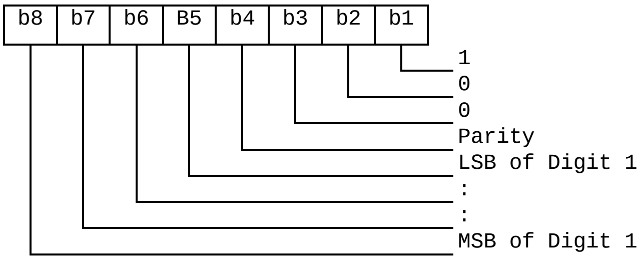
  Contents:

  International Mobile Subscriber Identity.

  Coding:

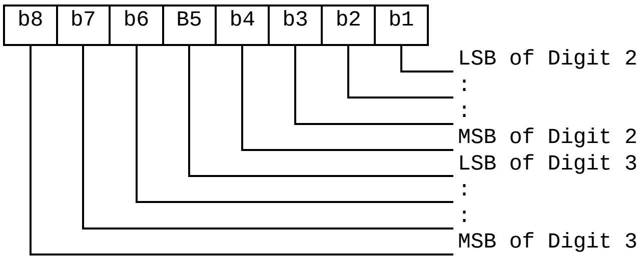
  this information element is of variable length. If a network operator chooses an IMSI of less than 15 digits, unused nibbles shall be set to 'F'.

Byte 2:



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

Byte 3:



etc.

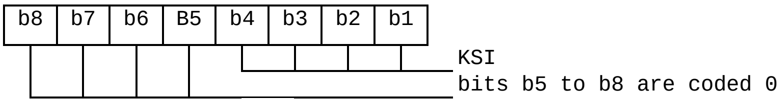
4.2.3 EF$_{Keys}$ (Ciphering and Integrity Keys)

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
2to17	Ciphering key CK	M	16 bytes
18to33	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.

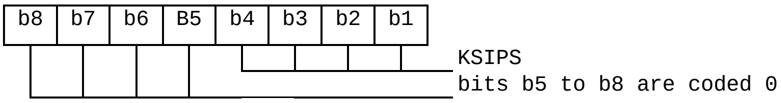
4.2.4 EF$_{KeysPS}$ (Ciphering and Integrity Keys for Packet Switched domain)

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	Optional
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
2to17	Ciphering key CKPS	M	16 bytes
18to33	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$_{PLMNsel}$ (PLMN selector)

This EF contains the coding for n PLMNs, where n is at least eight. This information determined by the user/operator defines the preferred PLMNs of the user in priority order.

Identifier: '6F30'	Structure: transparent	Optional
File size: 3n (n >= 8) bytes	Update activity: low	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 – 3	1st PLMN (highest priority)	M	3 bytes
22 to 24	8th PLMN	M	3 bytes
25 to 27	9th PLMN	O	3 bytes
(3n-2)-3n	Nth PLMN (lowest priority)	O	3 bytes

- PLMN
  Contents:
  Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).
  Coding:

according to 3G TS 24.008 [9];
if storage for fewer than the maximum possible number n is required, the excess bytes shall be set to 'FF'.
for instance, using 246 for the MCC and 81 for the MNC and if this is the first and only PLMN, the contents reads as follows:

Bytes 1-3: '42' 'F6' '18'
Bytes 4-6: 'FF' 'FF' 'FF'
etc.

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
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 - 3	Maximum value	M	3 bytes

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

First byte:

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

Second byte:

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

Third byte:

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 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.

<table>
<tr><td colspan="2">Identifier: '6F38'</td><td>Structure: transparent</td><td>Mandatory</td></tr>
<tr><td colspan="2">File size: X bytes, X >= 2</td><td colspan="2">Update activity: low</td></tr>
<tr><td colspan="4">Access Conditions:
READ PIN
UPDATE ADM
DEACTIVATE ADM
ACTIVATE ADM</td></tr>
<tr><td>Bytes</td><td>Description</td><td>M/O</td><td>Length</td></tr>
<tr><td>1</td><td>Services n°1 to n°8</td><td>M</td><td>1 byte</td></tr>
<tr><td>2</td><td>Services n°9 to n°16</td><td>O</td><td>1 byte</td></tr>
<tr><td>3</td><td>Services n°17 to n°24</td><td>O</td><td>1 byte</td></tr>
<tr><td>4</td><td>Services n°25 to n°32</td><td>O</td><td>1 byte</td></tr>
<tr><td>etc.</td><td></td><td></td><td></td></tr>
<tr><td>X</td><td>Services n°(4X-3) to n°(4X)</td><td>O</td><td>1 byte</td></tr>
</table>

-Services

Contents:	Service n°1 :	Local Phone Book
	Service n°2 :	Fixed Dialling Numbers (FDN): FFS
	Service n°3 :	Extension 2
	Service n°4 :	Service Dialling Numbers (SDN)
	Service n°5 :	Extension3
	Service n°6 :	Barred Dialling Numbers (BDN): FFS
	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:	PLMN selector
	Service n°21:	MSISDN
	Service n°22:	Image (IMG)
	Service n°23:	SoLSA (Support of Local Service Area)
	Service n°24:	Enhanced Multi-Level Precedence and Pre-emption Service
	Service n°25:	Automatic Answer for Emlpp
	Service n°26:	EUIC (Enhanced User Identity Confidentiality)
	Service n°27:	2G 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:	Packet Switched Domain

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 3G.

Coding:

1 bit is used to code each service:

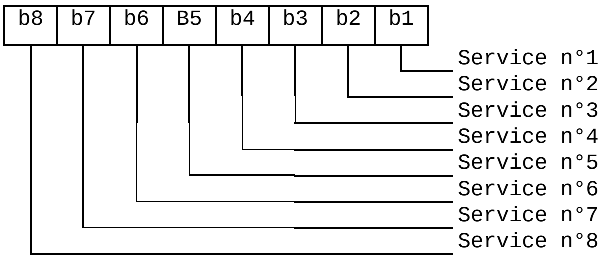
bit = 1: service available;

bit = 0: service not available.

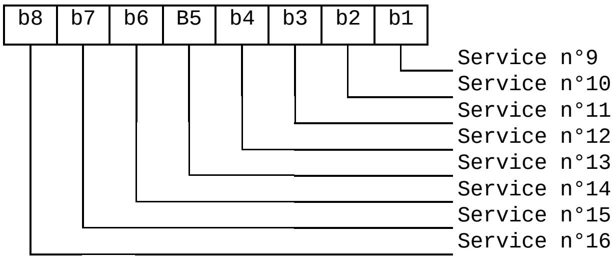
Service available means that the USIM has the capability to support the service and that the service is available for the user of the USIM.

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.

If the USIM supports the BDN feature (BDN available) and the ME does not support the BDN feature it shall stop operation immediately.

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]).

<table>
<tr><td colspan="2">Identifier: '6F39'</td><td colspan="2">Structure: cyclic</td><td>Optional</td></tr>
<tr><td colspan="3">SFI: Recommended</td><td colspan="2"></td></tr>
<tr><td colspan="3">Record length: 3 bytes</td><td colspan="2">Update activity: high</td></tr>
<tr><td colspan="5">Access Conditions:
READ PIN
UPDATE PIN/PIN2
(fixed during administrative management)
INCREASE PIN
DEACTIVATE ADM
ACTIVATE ADM</td></tr>
<tr><td>Bytes</td><td colspan="2">Description</td><td>M/O</td><td>Length</td></tr>
<tr><td>1 - 3</td><td colspan="2">Accumulated count of units</td><td>M</td><td>3 bytes</td></tr>
</table>

- 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.

<table>
<tr><td colspan="2">Identifier: '6F3E'</td><td colspan="2">Structure: transparent</td><td>Optional</td></tr>
<tr><td colspan="3">File size: 1-n bytes</td><td colspan="2">Update activity: low</td></tr>
<tr><td colspan="5">Access Conditions:
READ PIN
UPDATE ADM
DEACTIVATE ADM
ACTIVATE ADM</td></tr>
<tr><td>Bytes</td><td colspan="2">Description</td><td>M/O</td><td>Length</td></tr>
<tr><td>1 - n</td><td colspan="2">USIM group identifier(s)</td><td>O</td><td>n bytes</td></tr>
</table>

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 - n	USIM group identifier(s)	O	n bytes

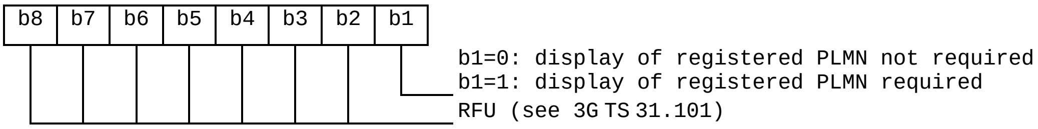
NOTE: The structure of EF_{GID1} and EF_{GID2} is identical. They are provided to allow the network operator to enforce different levels of security dependant on an application.

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 - 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:


b8
b7
b6
b5
b4
b3
b2
b1
b1=0: display of registered PLMN not required
b1=1: display of registered PLMN required
RFU (see 3G TS 31.101)

- 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)

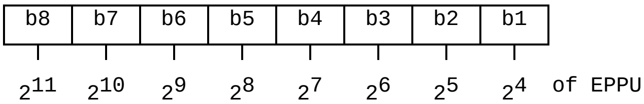
This EF contains the Price per Unit and Currency Table (PUCT). The PUCT is Advice of Charge related information which may be used by the ME in conjunction with EF$_{ACM}$ to compute the cost of calls in the currency chosen by the subscriber, as specified in 3G TS 22.024 [3]. This EF shall always be allocated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

<table>
<tr><td colspan="2">Identifier: '6F41'</td><td>Structure: transparent</td><td>Optional</td></tr>
<tr><td colspan="2">File size: 5 bytes</td><td colspan="2">Update activity: low</td></tr>
<tr><td colspan="4">Access Conditions:
READ PIN
UPDATE PIN/PIN2
(fixed during administrative management)
DEACTIVATE ADM
ACTIVATE ADM</td></tr>
<tr><td>Bytes</td><td>Description</td><td>M/O</td><td>Length</td></tr>
<tr><td>1 - 3</td><td>Currency code</td><td>M</td><td>3 bytes</td></tr>
<tr><td>4 - 5</td><td>Price per unit</td><td>M</td><td>2 bytes</td></tr>
</table>

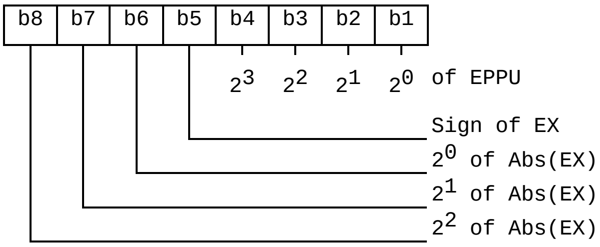
- Currency code
  Contents:
  the alpha-identifier of the currency code.
  Coding:
  bytes 1, 2 and 3 are the respective first, second and third character of the alpha identifier. This alpha-tagging shall use the SMS default 7-bit coded alphabet as defined in 3G TS 23.038 [5] with bit 8 set to 0.

- 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.

<table>
<tr><td colspan="2">Identifier: '6F45'</td><td colspan="3">Structure: transparent</td><td>Optional</td></tr>
<tr><td colspan="3">File size: 2 n bytes</td><td colspan="3">Update activity: low</td></tr>
<tr><td colspan="6">Access Conditions:
READ PIN
UPDATE PIN
DEACTIVATE ADM
ACTIVATE ADM</td></tr>
<tr><td>Bytes</td><td colspan="3">Description</td><td>M/O</td><td>Length</td></tr>
<tr><td>1 - 2</td><td colspan="3">CB Message Identifier 1</td><td>O</td><td>2 bytes</td></tr>
<tr><td>3 - 4</td><td colspan="3">CB Message Identifier 2</td><td>O</td><td>2 bytes</td></tr>
<tr><td></td><td colspan="3"></td><td></td><td></td></tr>
<tr><td>2n-1 - 2n</td><td colspan="3">CB Message Identifier n</td><td>O</td><td>2 bytes</td></tr>
</table>

- 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].

<table>
<tr><td colspan="2">Identifier: '6F78'</td><td colspan="3">Structure: transparent</td><td>Mandatory</td></tr>
<tr><td colspan="3">File size: 2 bytes</td><td colspan="3">Update activity: low</td></tr>
<tr><td colspan="6">Access Conditions:
READ PIN
UPDATE ADM
DEACTIVATE ADM
ACTIVATE ADM</td></tr>
<tr><td>Bytes</td><td colspan="3">Description</td><td>M/O</td><td>Length</td></tr>
<tr><td>1 - 2</td><td colspan="3">Access control classes</td><td>M</td><td>2 bytes</td></tr>
</table>

- 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:

```
b8  b7  b6  b5  b4  b3  b2  b1
 |   |   |   |   |   |   |   |
15  14  13  12  11  10  09  08  Number of the ACC (except for bit b3)
```

Byte 2:

```
b8  b7  b6  b5  b4  b3  b2  b1
 |   |   |   |   |   |   |   |
07  06  05  04  03  02  01  00  Number of the ACC
```

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 nth 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

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 - 3	PLMN 1	M	3 bytes
4 - 6	PLMN 2	M	3 bytes
7 - 9	PLMN 3	M	3 bytes
10 - 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:

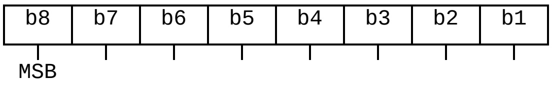
- Temporary Mobile Subscriber Identity (TMSI);
- Location Area Information (LAI);
- Location update status.

See clause 5.2.5 for special requirements when updating EF$_{LOCI}$.

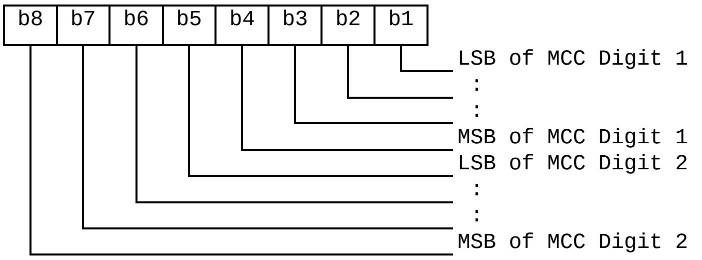
Identifier: '6F7E'	Structure: transparent	Mandatory
SFI: '30'		
File size: 11 bytes	Update activity: high	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE PIN		

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

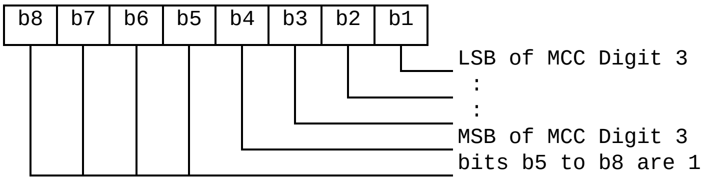
- TMSI
  Contents:
  Temporary Mobile Subscriber Identity.
  Coding:
  according to 3G TS 24.008 [9].



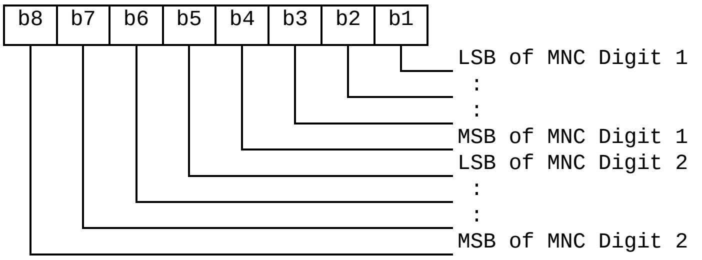
- LAI
  Contents:
  Location Area Information.
  Coding:
  according to 3G TS 24.008 [9].



Byte 6: second byte of LAI (MCC continued)



Byte 7: third byte of LAI (MNC)



Byte 8: fourth byte of LAI (LAC)
Byte 9: fifth byte of LAI (LAC continued)

- 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)

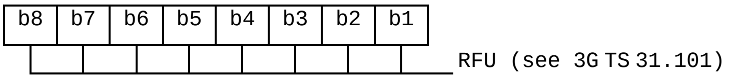
This EF contains information concerning the mode of operation according to the type of USIM, such as normal (to be used by PLMN subscribers for 3G operations), type approval (to allow specific use of the ME during type approval procedures of e.g. the radio equipment), cell testing (to allow testing of 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.

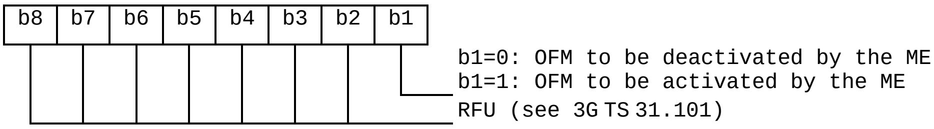
<table>
<tr><td colspan="2">Identifier: '6FAD'</td><td colspan="2">Structure: transparent</td><td>Mandatory</td></tr>
<tr><td colspan="3">File size: 3+X bytes</td><td colspan="2">Update activity: low</td></tr>
<tr><td colspan="5">Access Conditions:
READ ALW
UPDATE ADM
DEACTIVATE ADM
ACTIVATE ADM</td></tr>
<tr><td>Bytes</td><td colspan="2">Description</td><td>M/O</td><td>Length</td></tr>
<tr><td>1</td><td colspan="2">UE operation mode</td><td>M</td><td>1 byte</td></tr>
<tr><td>2 - 3</td><td colspan="2">Additional information</td><td>M</td><td>2 bytes</td></tr>
<tr><td>4 - 3+X</td><td colspan="2">RFU</td><td>O</td><td>X bytes</td></tr>
</table>

- 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:



b1=0: OFM to be deactivated by the ME
b1=1: OFM to be activated by the ME
RFU (see 3G TS 31.101)

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 EF$_{APPI}$ (Application Profile Indication)

This EF contains an indication concerning the application (USIM) profile.

Identifier: '6FAE'	Structure: transparent		Mandatory
File size: X byte		Update activity: low	
Access Conditions: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM			
Bytes	Description	M/O	Length
1 to 2	USIM Release	M	2 bytes
3	USIM Version	M	1 byte
4	Operator Indication	M	1 byte
5toX	RFU	O	X-4 bytes

All other codings are reserved for specification by 3GPP.

- USIM Release
  Contents:
  indicates the TSG-T approved release of the 3G TS 31.102 the USIM is based on.
  Coding:
  '19 99': Release 99
  All other codings are reserved for specification by 3GPP.

- USIM Version
  Contents:
  indicates the TSG-T approved version of the 31.102 within a Release the USIM is based on.
  Coding:
  according to the '31.102 Change Control Document'.
- Operator Indication
  Contents:
  for use by the operator to indicate different versions of operator-specific USIM applications.
  Coding:
  not within the scope of this specification.

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
File size: 2n bytes	Update activity: low	
Access Conditions: READ PIN UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

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

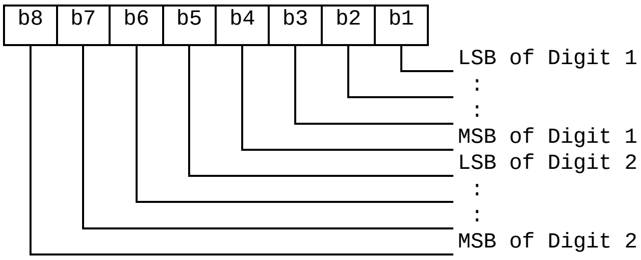
This EF contains up to 5 emergency call codes.

Identifier: '6FB7'	Structure: transparent	Optional
File size: 3n (n ≤ 5) bytes	Update activity: low	
Access Conditions: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

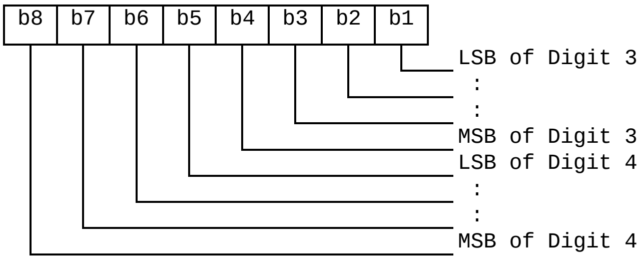
Bytes	Description	M/O	Length
1 - 3	Emergency Call Code 1	O	3 bytes
4 - 6	Emergency Call Code 2	O	3 bytes
(3n-2) - 3n	Emergency Call Code n	O	3 bytes

- 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'.

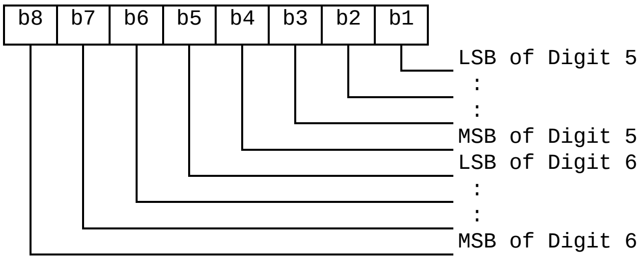
  Byte 1:



Byte 2:



Byte 3:



4.2.22 EF$_{\text{CBMIR}}$ (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 - 4	CB Message Identifier Range 1	O	4 bytes
5 - 8	CB Message Identifier Range 2	O	4 bytes
(4n-3) - 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$_{\text{PSLOCI}}$ (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: '6F53'		Structure: transparent		Optional
SFI: Recommended				
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

b8	b7	B6	B5	B4	b3	b2	b1
MSB							

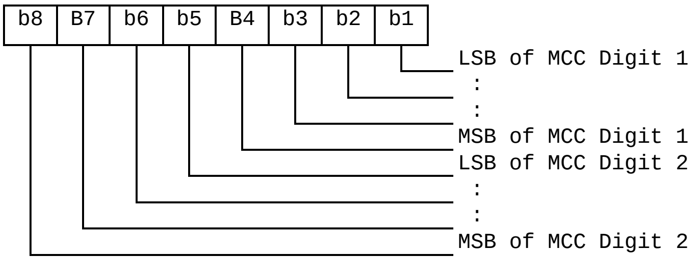
- P-TMSI signature value
  Contents:
    Packet Temporary Mobile Subscriber Identity signature value.
  Coding:
    according to 3G TS 24.008 [9].

  Byte 5: first byte of P-TMSI signature value

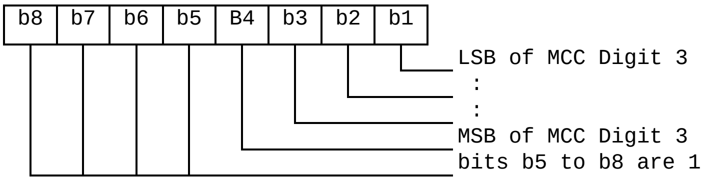
b8	b7	B6	B5	B4	b3	b2	b1
MSB							

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

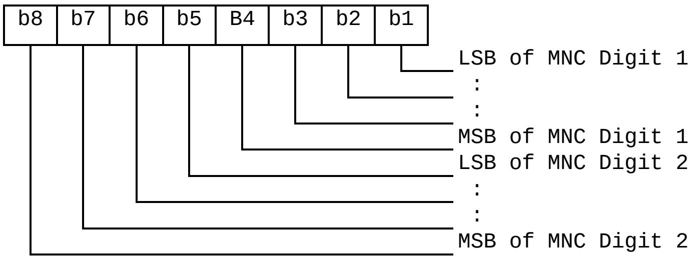
  Byte 8: first byte of RAI



Byte 9: second byte of RAI (MCC continued)



Byte 10: third byte of RAI (MNC)



Byte 11: fourth byte of RAI (LAC)
Byte 12: fifth byte of RAI (LAC continued)
Byte 13: sixth byte of RAI (RAC)

- Routing update status
  Contents:
  status of location 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.

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 4.4.3.3), with the exception that extension records are stored in the EF$_{EXT2}$.

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 4.4.3.3 (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-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 4.5.1), 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 4.5.2 (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 4.5.2 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 – 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
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'.

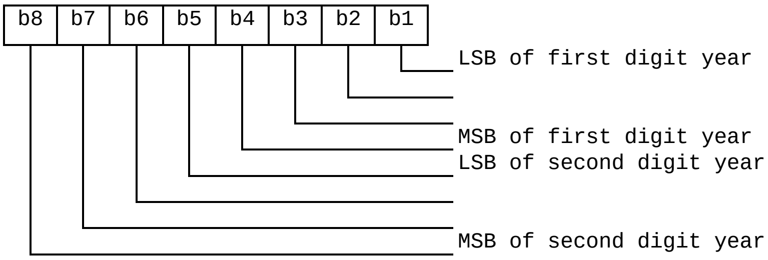
Detail 1 Coding of date and time

Content:

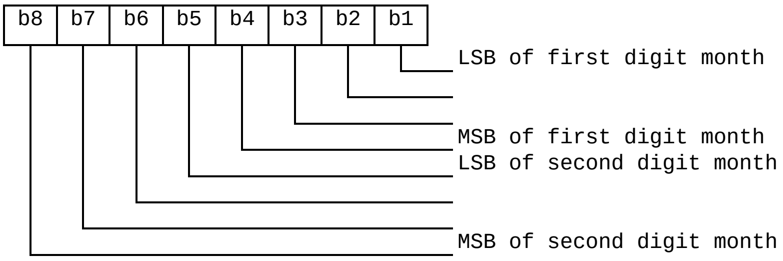
the date and time are defined by the ME.

Coding:

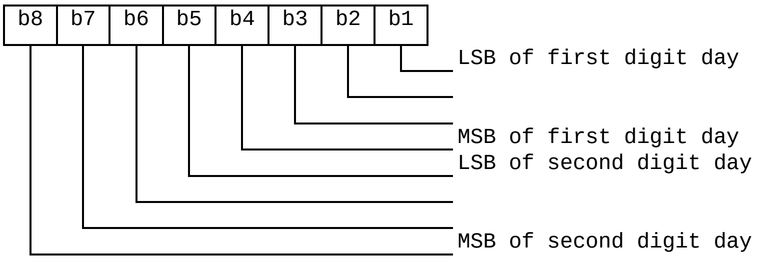
it is according to the extended BCD coding from Byte1 to Byte 7. The first 3 bytes show year, month and day (yy.mm.dd). The next 3 bytes show hour, minute and second (hh.mm.ss). The last Byte 7 is Time Zone. The Time Zone indicates the difference, expressed in quarters of an hour, between the local time 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 8 shall be "FF“. Byte X+15: Year



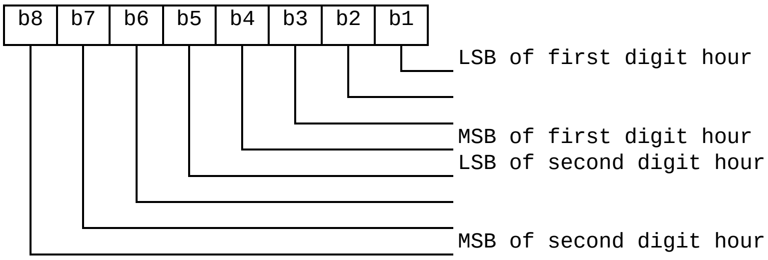
Byte X+16: Month



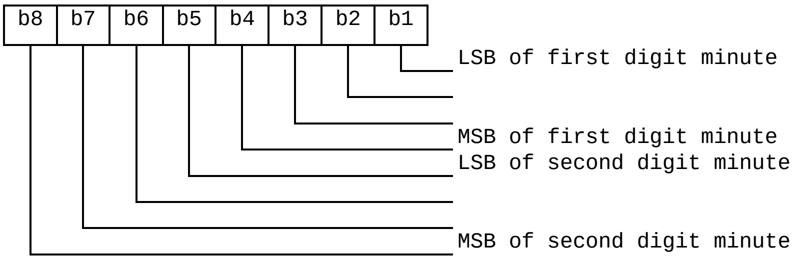
Byte X+17: Day



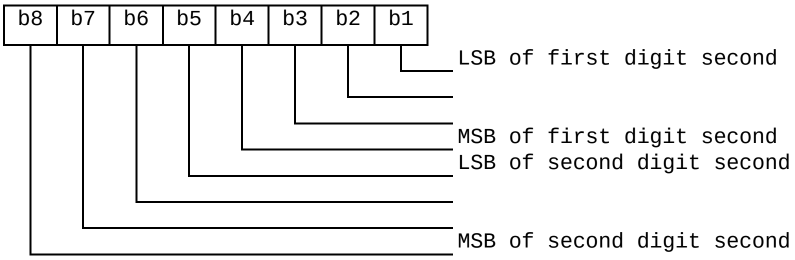
Byte X+18: Hour



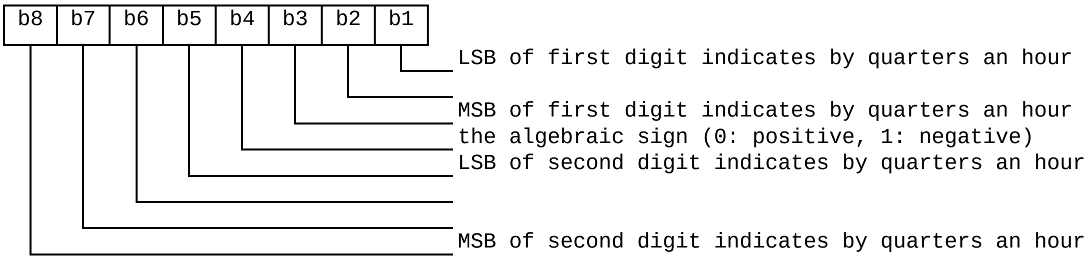
Byte X+19: Minute


b8
b7
b6
b5
b4
b3
b2
b1
LSB of first digit minute
MSB of first digit minute
LSB of second digit minute
MSB of second digit minute

Byte X+20: Second


b8
b7
b6
b5
b4
b3
b2
b1
LSB of first digit second
MSB of first digit second
LSB of second digit second
MSB of second digit second

Byte X+21: Time Zone



b8 b7 b6 b5 b4 b3 b2 b1
LSB of first digit indicates by quarters an hour
MSB of first digit indicates by quarters an hour
the algebraic sign (0: positive, 1: negative)
LSB of second digit indicates by quarters an hour
MSB of second digit indicates by quarters an hour

Detail 2 Coding of call duration

Call duration is indicated by second

Byte X+22:

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 X+23:

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

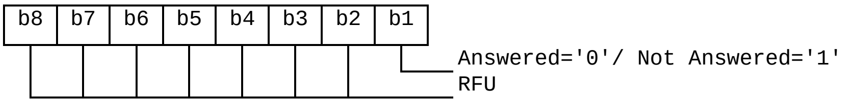
Byte X+24:

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

Detail 3 Coding of Call status

Byte X+25:

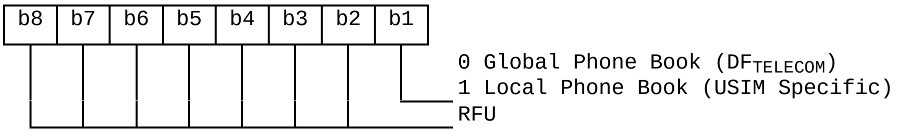


Detail 4 Link to phone book entry

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

- Phone book reference.

Byte X+26:



b8 b7 b6 b5 b4 b3 b2 b1
0 Global Phone Book (DF_{TELECOM})
1 Local Phone Book (USIM Specific)
RFU

- 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 application 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 aplha 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
Record length: X+26 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 - 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 - 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: optional			
Record length: 14 bytes		Update activity: low	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM			
Bytes	Description	M/O	Length
1 to 10	Bearer capability information element	M	10 bytes
11 to 14	Bytes reserved - see below	M	4 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.

- Bytes 11-14 shall be set to 'FF' and shall not be interpreted by the terminal.

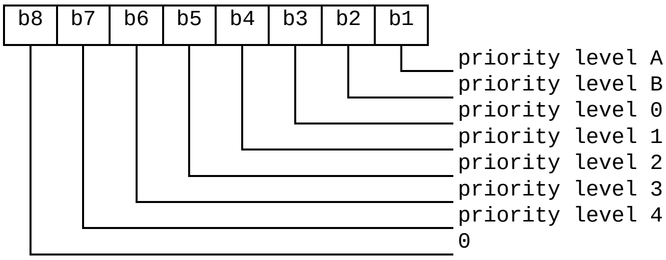
4.2.39 EF$_{eMLPP}$ (enhanced Multi Level Precedence and Pre-emption)

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:

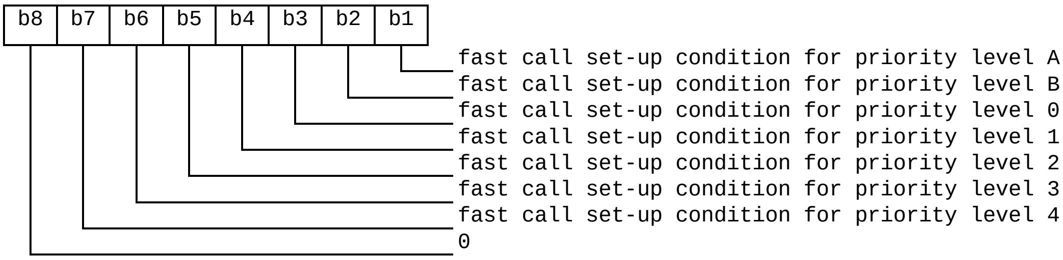


Example: If priority levels B and 2 are subscribed to, EF_{eMLPP} shall be coded '12'.

- 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:

`



b8
b7
b6
b5
b4
b3
b2
b1
fast call set-up condition for priority level A
fast call set-up condition for priority level B
fast call set-up condition for priority level 0
fast call set-up condition for priority level 1
fast call set-up condition for priority level 2
fast call set-up condition for priority level 3
fast call set-up condition for priority level 4
0

Example: If fast call set-up is allowed for priority levels B, 0 and 2, then byte 2 of EF_{eMLPP} is coded '16'.

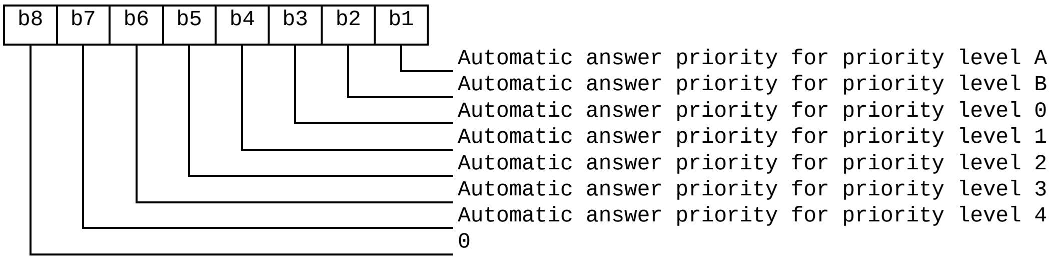
4.2.40 EF_{AAeM} (Automatic Answer for eMLPP Service)

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:


b8
b7
b6
b5
b4
b3
b2
b1
Automatic answer priority for priority level A
Automatic answer priority for priority level B
Automatic answer priority for priority level 0
Automatic answer priority for priority level 1
Automatic answer priority for priority level 2
Automatic answer priority for priority level 3
Automatic answer priority for priority level 4
0

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 EF contains the group identity of the mobile subscriber. This group identity references a group key GK, stored in the USIM, which is used for enhanced user identity confidentiality (enciphering of the IMSI).

Identifier: '6FC2'	Structure: transparent	Optional
File size: 4 bytes	Update activity: low	
Access Conditions: READ PIN UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to 4	Group Identity	M	4 bytes

- Group Identity GMSI
  Coding:
  the least significant bit of GMSI is the least significant bit of the 4th byte. The most significant bit of GMSI is the most significant bit of the first byte.

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 'FF'.

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 Files required for 2G Access

The EFs described in this chapter 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 2G access is indicated in the 'USIM Service Table' as service no. '27' being available.

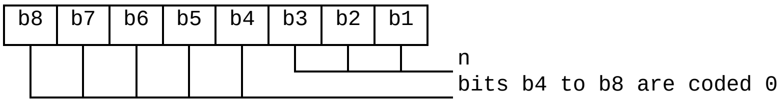
4.2.43.1 EF$_{Kc}$ (Ciphering key Kc)

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

Identifier: '6F20'	Structure: transparent		Optional
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.

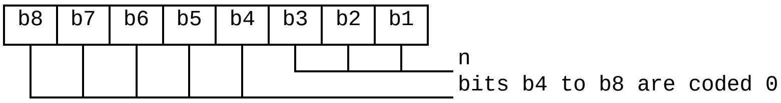
4.2.43.2 EF_{KcGPRS} (GPRS Ciphering key KcGPRS)

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

<table>
<tr><td colspan="2">Identifier: '6F52'</td><td colspan="2">Structure: transparent</td><td>Optional</td></tr>
<tr><td colspan="3">File size: 9 bytes</td><td colspan="2">Update activity: high</td></tr>
<tr><td colspan="5">Access Conditions:
READ PIN
UPDATE PIN
DEACTIVATE ADM
ACTIVATE ADM</td></tr>
<tr><td>Bytes</td><td colspan="2">Description</td><td>M/O</td><td>Length</td></tr>
<tr><td>1 - 8</td><td colspan="2">Ciphering key KcGPRS</td><td>M</td><td>8 bytes</td></tr>
<tr><td>9</td><td colspan="2">Ciphering key sequence number n for GPRS</td><td>M</td><td>1 byte</td></tr>
</table>

- 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.

4.2.43.3 $EF_{LOCIGPRS}$ (GPRS location information)

This EF contains the following Location Information:

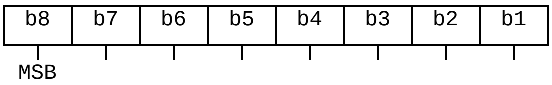
- Packet Temporary Mobile Subscriber Identity (P-TMSI);
- Packet Temporary Mobile Subscriber Identity signature value (P-TMSI signature value);
- Routing Area Information (RAI);
- Routing Area update status.

<table>
<tr><td colspan="2">Identifier: '6F53'</td><td colspan="2">Structure: transparent</td><td>Optional</td></tr>
<tr><td colspan="3">File size: 14 bytes</td><td colspan="2">Update activity: high</td></tr>
<tr><td colspan="5">Access Conditions:
READ PIN
UPDATE PIN
DEACTIVATE ADM
ACTIVATE ADM</td></tr>
<tr><td>Bytes</td><td colspan="2">Description</td><td>M/O</td><td>Length</td></tr>
<tr><td>1 - 4</td><td colspan="2">P-TMSI</td><td>M</td><td>4 bytes</td></tr>
<tr><td>5 to 7</td><td colspan="2">P-TMSI signature value</td><td>M</td><td>3 bytes</td></tr>
<tr><td>8 - 13</td><td colspan="2">RAI</td><td>M</td><td>6 bytes</td></tr>
<tr><td>14</td><td colspan="2">Routing Area update status</td><td>M</td><td>1 byte</td></tr>
</table>

- P-TMSI
  Contents:
  Packet Temporary Mobile Subscriber Identity.

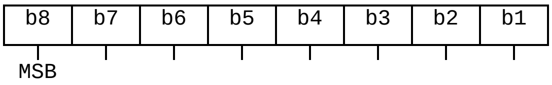
Coding:
according to TS 24.008 [9].

Byte 1: first byte of P-TMSI



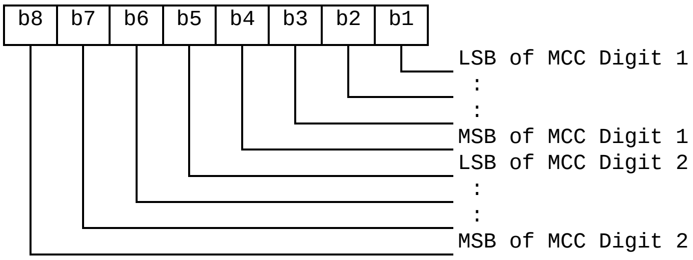
- P-TMSI signature value
  Contents:
  Packet Temporary Mobile Subscriber Identity signature value.
  Coding:
  according to TS 24.008 [9].

Byte 1: first byte of P-TMSI signature value

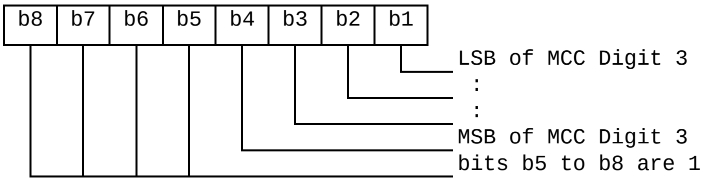


- RAI
  Contents:
  Routing Area Information.
  Coding:
  according to TS 24.008 [9].

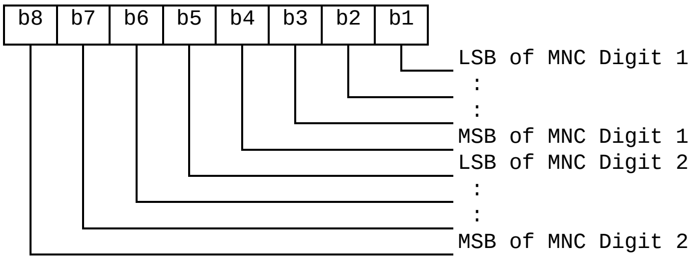
Byte 5: first byte of RAI



Byte 6: second byte of RAI (MCC continued)



Byte 7: third byte of RAI (MNC)



Byte 8: fourth byte of RAI (LAC)
Byte 9: fifth byte of RAI (LAC continued)
Byte 10: sixth byte of RAI (RAC)- Routing update status

Contents:
status of location update according to TS 24.008 [9].

Coding:

Byte 12:

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.

4.2.43.4 EF$_{LOCI2G}$ (Location Information for 2G access)

This EF contains the following Location Information:

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

See clause 5.2.5 for special requirements when updating EF$_{LOCI}$.

<table>
<tr><td colspan="2">Identifier: '6F7F'</td><td colspan="2">Structure: transparent</td><td>Mandatory</td></tr>
<tr><td colspan="3">File size: 11 bytes</td><td colspan="2">Update activity: high</td></tr>
<tr><td colspan="5">Access Conditions:
READ PIN
UPDATE PIN
DEACTIVATE ADM
ACTIVATE PIN</td></tr>
<tr><td>Bytes</td><td colspan="2">Description</td><td>M/O</td><td>Length</td></tr>
<tr><td>1 - 4</td><td colspan="2">TMSI</td><td>M</td><td>4 bytes</td></tr>
<tr><td>5 - 9</td><td colspan="2">LAI</td><td>M</td><td>5 bytes</td></tr>
<tr><td>10</td><td colspan="2">TMSI TIME</td><td>M</td><td>1 byte</td></tr>
<tr><td>11</td><td colspan="2">Location update status</td><td>M</td><td>1 byte</td></tr>
</table>

- TMSI

Contents:

Temporary Mobile Subscriber Identity.

Coding:

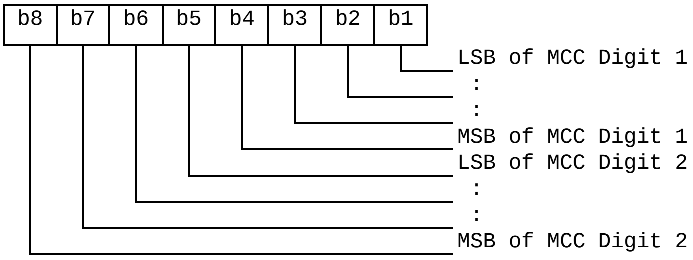
according to TS 24.008 [9].

Byte 1: first byte of TMSI

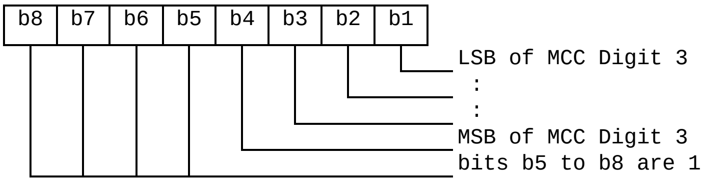
b8	b7	b6	b5	b4	b3	b2	b1
MSB							

- LAI
  Contents:
  Location Area Information.
  Coding:
  according to TS 24.008 [9].

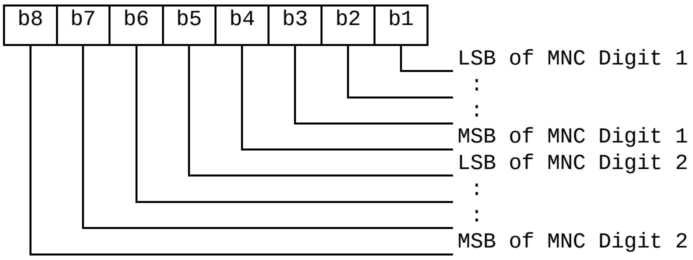
  Byte 5: first byte of LAI (MCC)



  Byte 6: second byte of LAI (MCC continued)



  Byte 7: third byte of LAI (MNC)



  Byte 8: fourth byte of LAI (LAC)

  Byte 9: fifth byte of LAI (LAC continued)

- TMSI TIME
  Contents:
  current value of Periodic Location Updating Timer (T3212).
  This byte is used by Phase 1 MEs, but it shall not be used by Phase 2 MEs.
- Location update status
  Contents:
  status of location update according to 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 GSM 11.11 [18]).

4.2.43.5 EF$_{BCCH}$ (Broadcast Control Channels)

This EF contains information concerning the BCCH according to TS 24.008 [9].

BCCH storage may reduce the extent of a User Equipment's search of BCCH carriers when selecting a cell. The BCCH carrier lists in an UE shall be in accordance with the procedures specified in TS 24.008 [9]. The UE shall only store BCCH information from the System Information 2 message and not the 2bis extension message.

Identifier: '6F74'	Structure: transparent		Optional
File size: 16 bytes		Update activity: high	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM			
Bytes	Description	M/O	Length
1 - 16	BCCH information	M	16 bytes

- BCCH information
  Coding:
  the information is coded as octets 2-17 of the "neighbour cells description information element" in TS 24.008 [9].

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_{SoLSA} '5F70'
- $DF_{PHONEBOOK}$ '5F3A'

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

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 specifies the EFs in the dedicated file DF_{SoLSA}. It only applies if the SoLSA feature is supported (see 3G TS 23.073 [8]).

The EFs contain information about the users subscribed local service areas.

4.4.1.1 EF_{SAI} (SoLSA Access Indicator)

This EF contains the 'LSA only access indicator'. This EF shall always be allocated if DF_{SoLSA} is present.

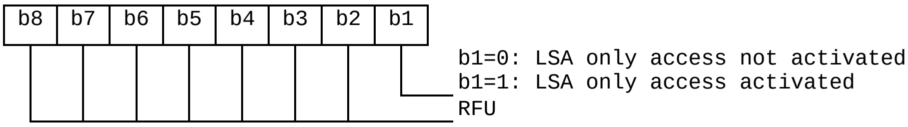
If the indicator is set, the network will prevent terminated and/or originated calls when the UE is camped in cells that are not included in the list of allowed LSAs in EF_{SLL}. Emergency calls are, however, always allowed.

The EF also contains a text string which may be displayed when the UE is out of the served area(s).

Identifier: '4F30'	Structure: transparent		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	LSA only access indicator	M	1 byte
2 to X+1	LSA only access indication text	M	X bytes

- LSA only access indicator
  Contents:
  indicates whether the UE is restricted to use LSA cells only or not.

  Coding:


b8
b7
b6
b5
b4
b3
b2
b1
b1=0: LSA only access not activated
b1=1: LSA only access activated
RFU

- LSA only access indication text
  Contents:
  text to be displayed by the ME when it's out of LSA area.
  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 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].

4.4.1.2 EF$_{SLL}$ (SoLSA LSA List)

This EF contains information describing the LSAs that the user is subscribed to. This EF shall always be allocated if DF$_{SoLSA}$ is present.

Each LSA is described by one record that is linked to a LSA Descriptor file. Each record contains information of the PLMN, priority of the LSA, information about the subscription and may also contain a text string and/or an icon that identifies the LSA to the user. The text string can be edited by the user.

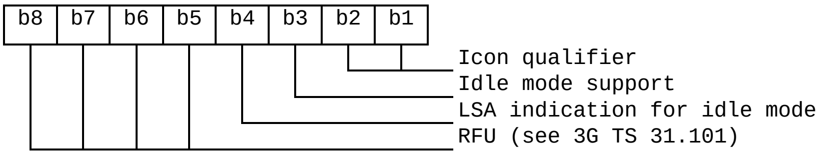
Identifier: '4F31'	Structure: linear fixed		Optional
Record length: X+10 bytes		Update activity: low	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM			
Bytes	Description	M/O	Length
1 to X	LSA name	O	X bytes
X+1	Configuration parameters	M	1 byte
X+2	RFU	M	1 byte
X+3	Icon Identifier	M	1 byte
X+4	Priority	M	1 byte
X+5 to X+7	PLMN code	M	3 bytes
X+8 to X+9	LSA Descriptor File Identifier	M	2 bytes
X+10	LSA Descriptor Record Identifier	M	1 byte

- LSA name
  Contents:
  LSA name string to be displayed when the ME is camped in the corresponding area, dependant on the contents of the LSA indication for idle mode field.
  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 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].

- Configuration parameters
  Contents:
  icon qualifier, control of idle mode support and control of LSA indication for idle mode.

Coding:



- Icon qualifier
  Contents:
  the icon qualifier indicates to the ME how the icon to be used.

  b1, b2: 00: icon is not to be used and may not be present.
  01: icon is self-explanatory, i.e. if displayed, it replace the LSA name
  10: icon is not self-explanatory, i.e. if displayed, it shall be displayed together with the LSA name
  11: RFU

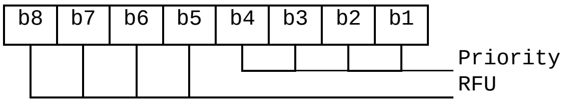
- Idle mode support
  Contents:
  the idle mode support is used to indicate whether the ME shall favour camping on the LSA cells in idle mode.
  b3 = 0 : Idle mode support disabled;
  b3 = 1 : Idle mode support enabled.

- LSA indication for idle mode
  Contents:
  the LSA indication for idle mode is used to indicate whether or not the ME shall display the LSA name when the ME is camped on a cell within the LSA.

  b4 = 0 : LSA indication for idle mode disabled
  b4 = 1 : LSA indication for idle mode enabled
  Bits b5 to b8 are RFU (see 3G TS 31.101 [11]).

- Icon Identifier
  Contents:
  the icon identifier addresses a record in EF_{IMG}.
  Coding:
  binary.

- Priority
  Contents:
  priority of the LSA which gives the ME the preference of this LSA relative to the other LSAs.
  Coding:



'0' is lowest priority 'F' is highest.

- PLMN code
  Contents:
  MCC + MNC for the LSA.
  Coding:
  according to 3G TS 24.008 [9] and EF_{LOCI}.

- LSA Descriptor File Identifier
  Contents:
  these bytes identity the EF which contains the LSA Descriptors forming the LSA.
  Coding:
  byte X+8: high byte of the LSA Descriptor file;
  byte X+9: low byte of the LSA Descriptor file.

- LSA Descriptor Record Identifier

Contents:
this byte identifies the number of the first record in the LSA Descriptor file forming the LSA.
Coding:
binary.

4.4.1.3 LSA Descriptor files

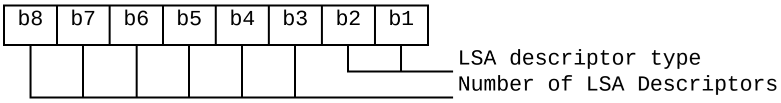
Residing under DF_{SoLSA}, there may be several LSA Descriptor files. These EFs contains one or more records again containing LSA Descriptors forming the LSAs. LSAs can be described in four different ways. As a list of LSA IDs, as a list of LAC + CIs, as a list of CIs or as a list of LACs. As the basic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

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

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

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

  Coding:



- LSA descriptor type
  Contents: Gives the format of the LSA Descriptors.
  b1, b2 : 00: LSA ID.
  01: LAC + CI
  10: CI
  11: LAC

- Number of LSA Descriptors
  Contents:
  the number of valid LSA Descriptors in the record.
  Coding:
  binary, with b8 as MSB and b3 as LSB leaving room for 64 LSA Descriptors per record.

- LSA Descriptor
  Contents:
  Dependant of the coding indicated in the LSA descriptor type:
  - in case of LSA ID the field length 'X' is 3 bytes,
  - in case of LAC + CI the field length 'X' is 4 bytes,
  - in case of CI the field length 'X' is 2 bytes,

- in case of LAC the field length 'X' is 2 bytes,

Coding:

according to 3G TS 24.008 [9].

- Record Identifier

  Contents:

  this byte identifies the number of the next record containing the LSA Descriptors forming the LSA.

  Coding:

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

This file utilises the concept of chaining as for EF$_{EXT1}$.

The identifier '4FXX' shall be different from one LSA Descriptor file to the other and different from the identifiers of EF$_{SAI}$ and EF$_{SLL}$. For the range of 'XX', see subclause tbd.

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$_{USIM}$. DF$_{PHONEBOOK}$ under DF$_{USIM}$ and under DF $_{TELECOM}$ have the same structure. 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.

The EF structure related to the public phone book is located under DF$_{PHONEBOOK}$ in DF$_{TELECOM}$. A USIM specific phone book may exist for application specific entries. The application specific phone book is protected by the application PIN. The application specific phone book is a copy of the file structure of 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. 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 TLV object in a record (Grouping information in EF$_{GAS}$)

Table 4.1: Phone Book Reference file Constructed Tags

Tag Value	Constructed TAG Description
'D8'	Indicating files where the amount of records equal to master EF, type 1
'D9'	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
'DA'	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 'D8' 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 'D8' 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 'D9' are mapped to the master EF (the file ID indicated as the first data object in the TLV object using Tag 'D8') 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 'D9'. 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 'D8'.

File IDs indicated using constructed Tag 'DA' 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.

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.

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

Phone Book Reference file EF_{PBR} structure

Identifier: '4F30'	Structure: linear fixed		Optional
SFI: Optional			
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

4.4.2.2 EF$_{IAP}$ (Index Administration Phone book)

This file is present if Tag 'D9' 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$_{ADN}$ (must 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 'D9' 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 'D9'.

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	Optional
SFI: mandatory		
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 xth object indicated after Tag 'D9'	M	1 byte

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.

This EF shall always be present if the DF$_{Phonebook}$ is present.

Identifier: '4F3A	Structure: linear fixed	Optional
SFI: mandatory		
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/Configuration Identifier	M	1 byte
X+14	Extension1 Record Identifier	M	1 byte

- 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

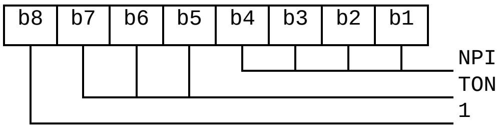
- one of the UCS2 coded options as defined in the annex of 3G TS 31.101 [11].

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 4.4.3.4).
  Coding:
  according to 3G TS 24.008 [9].

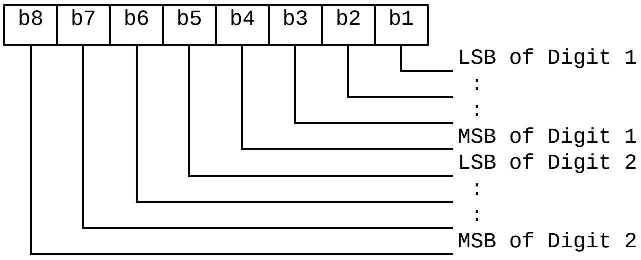
- TON and NPI
  Contents:
  Type of number (TON) and numbering plan identification (NPI).
  Coding:
  according to 3G TS 24.008 [9]. If the Dialling Number/SSC String does not contain a dialling number, e.g. a control string deactivating a service, the TON/NPI byte shall be set to 'FF' by the ME (see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

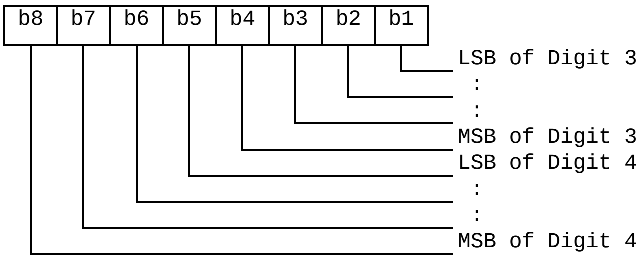


- Dialling Number/SSC String
  Contents:
  up to 20 digits of the telephone number and/or SSC information.
  Coding:
  according to 3G TS 24.008 [9] , 3G TS 22.030 [4] and the extended BCD-coding (see table 12). If the telephone number or SSC is longer than 20 digits, the first 20 digits are stored in 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/Configuration Identifier
  Contents:
  capability/configuration identification byte. This byte identifies the number of a record in the EF_{CCP} 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 4.4.3.4).
  Coding:
  binary.

NOTE 3: If EF_{ADN} is part of the public phone book in $DF_{TELECOM}$ it 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 4.3: 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, an MSISDN, an ICI or an OCI. This EF shall always be present if the DF$_{Phonebook}$ is present.

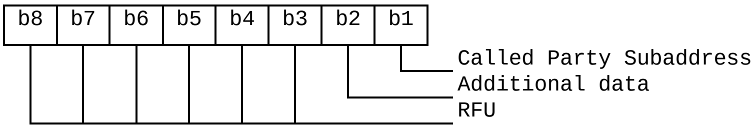
Extension data is caused by:

- an ADN/SSC (MSISDN, ICI, OCI) which is greater than the 20 digit capacity of the ADN/SSC (MSISDN, ICI, OCI) 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 (MSISDN, ICI, OCI) 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: Mandatory		
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":

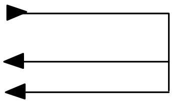
b8	b7	b6	b5	b4	b3	b2	b1
0	0	0	0	0	0	1	0

- 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 (respectively MSISDN, ICI, OCI). The coding of remaining bytes is BCD, according to the coding of ADN/SSC (MSISDN, ICI, OCI). Unused nibbles at the end have to 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
:	:	:	:	
:	:	:	:	
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 (must 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$_{PCB}$ and EF$_{ADN}$).

Structure of control file EF$_{PBC}$

<table>
<tr><td colspan="2">Identifier: '4FXX'</td><td colspan="3">Structure: linear fixed</td><td>Optional</td></tr>
<tr><td colspan="2">SFI: Mandatory</td><td colspan="4"></td></tr>
<tr><td colspan="3">Record length: 2 bytes</td><td colspan="3">Update activity: low</td></tr>
<tr><td colspan="6">Access Conditions:
READ PIN
UPDATE PIN
DEACTIVATE ADM
ACTIVATE ADM</td></tr>
<tr><td>Bytes</td><td colspan="3">Description</td><td>M/O</td><td>Length</td></tr>
<tr><td>1</td><td colspan="3">Entry Control Information</td><td>M</td><td>1 byte</td></tr>
<tr><td>2</td><td colspan="3">Hidden Information</td><td>M</td><td>1 byte</td></tr>
</table>

- Entry Control Information
  Contents:
  provides some characteristics about the phone book entry (eg modification by a 2G mobile).
  Coding:

```
b8 | B7 | b6 | B5 | b4 | B3 | b2 | B1
                                  |___ Modified by 2G phone '1', no change '0'
 |____|____|____|____|____|____|______ RFU (see 3G TS 31.101)
```

- Hidden Information
  Contents:
  indicates to which USIM/GSM application of the UICC this phone book entry belongs, so that the corresponding secret code can be verified to display the phone book entry, other wise the phone book entry is hidden.
  Coding:
  '00' – the phone book entry is not hidden;
  'xx' – 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 to which the entry belongs.

Structure of grouping file EF$_{GRP}$

<table>
<tr><td colspan="2">Identifier: '4FXX'</td><td colspan="3">Structure: linear fixed</td><td>Optional</td></tr>
<tr><td colspan="2">SFI: Mandatory</td><td colspan="4"></td></tr>
<tr><td colspan="3">Record Length: X bytes (1 ≤ X ≤10)</td><td colspan="3">Update activity: high</td></tr>
<tr><td colspan="6">Access Conditions:
READ PIN
UPDATE PIN
DEACTIVATE ADM
ACTIVATE ADM</td></tr>
<tr><td>Bytes</td><td colspan="3">Description</td><td>M/O</td><td>Length</td></tr>
<tr><td>1</td><td colspan="3">Group Name Identifier 1</td><td>M</td><td>1 byte</td></tr>
<tr><td>2</td><td colspan="3">Group Name Identifier 2</td><td>O</td><td>1 byte</td></tr>
<tr><td>X</td><td colspan="3">Group Name Identifier X</td><td>O</td><td>1 byte</td></tr>
</table>

- 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' – the phone book entry is not part of a group;
'XX' – record number in $EF_{GAS.}$

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: Recommended			
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		Optional
SFI: Recommended			
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:
  group names.
  Coding:
  same as the alpha identifier in EF_{ADN}.

4.4.2.9 EF_{ANR} (Additional Number)

Several phone numbers 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. 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.

Structure of EF_{ANR}

Identifier: '4FXX'		Structure: linear fixed		Optional
SFI: mandatory				
Record length: X+11 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
2to11	Additional number	M	10 bytes
12	ADN file SFI	M/O	1 byte
13	ADN file Record Identifier	M/O	1 byte

- 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.

- Additional number
  Content:
    additional phone number linked to the phone book entry.
  Coding:
    same than the dialling number /SSC string in 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

In case of a one-to-one mapping, i.e. there is one ANR entry for each ADN entry, the ADN file SFI and the ADN file Record Identifier should not be present. In all other cases these two bytes shall be present.

4.4.2.10 EF_{SNE} (Second Name Entry)

The phone book also contains the option of a second name entry. The second name entry is associated with the ADN record through the pointer in the index administration file. The amount of second name entries may be less than or equal to the amount of records in EF_{ADN}.

Structure of EF_{SNE}

Identifier: '4FXX'	Structure: linear fixed		Optional
SFI: mandatory			
Record length: 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	M/O	1 byte
X+2	ADN file Record Identifier	M/O	1 byte

- 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.

In case of a one-to-one mapping, i.e. there is one SNE entry for each ADN entry, the ADN file SFI and the ADN file Record Identifier should not be present. In all other cases these two bytes shall be present.

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.

Identifier: '4F3D'	Structure: linear fixed		Optional
SFI: optional			
Record length: 14 bytes		Update activity: low	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM			

Bytes	Description	M/O	Length
1 to 10	Bearer capability information element	M	10 bytes
11 to 14	Bytes reserved - see below	M	4 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_{CCP} record shall be Length of the bearer capability contents.

- Bytes 11-14 shall be set to 'FF' and shall not be interpreted by the ME.

4.4.2.12 Phone Book Synchronisation

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

When the 3G UICC has been inserted into a 2G terminal and a record in the phone book has been updated, a flag in the entry control information in the EF_{PBC} is set from 0 to 1 by the card. When/if the UICC later is inserted into a 3G terminal again, the terminal shall check the flag in EF_{PBC} and if this flag is set update the CC. A set flag in EF_{PBC} results in a full synchronisation of the phone book (if synchronisation is requested).

4.4.2.12.1 EF_{UID} (Unique Identifier)

The UID is used to uniquely identify a record and to be able to keep track of the records in the phonebook.. 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 PID remains the same. The UID shall remain on the UICC, in EF_{UID}, until the PID is regenerated. This means that when a record is deleted from the phonebook, the content of the linked information (eg ADN, E-MAIL,..) are set to the personalisation value 'FF…FF'. But the UID-value of the deleted record shall not be used when a new record is added to the phonebook until the PID is regenerated, but it shall be set to a new value.

If/when the PID is regenerated, all UIDs for the records in the phonebook shall be assigned new values starting from 1. The new value of the UID for each record shall then be kept until the PID is regenerated again.

Structure of EF_{UID}

Identifier: '4F21'	Structure: linear fixed	Optional
SFI: optional		
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

- Unique Identifier of Phone Book Entry
  Content:
  number to unambiguously identify the phone book entry for synchronisation purposes.
  Coding:
  hexadecimal. At initialisation all UIDs are personalised to 0000 Hex (e.g. 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 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 phonebook residing in a USIM-application). If the PSC is unknown, a full synchronisation of the phonebook 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		Optional
SFI: 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	Phone book synchronisation counter (PSC)		M	4 bytes

- PSC: Unique synchronisation counter of Phone Book
  Content:
  number to unambiguously identify the status of the phone book for synchronisation purposes
  Coding:
  hexadecimal.

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

- For a phone book residing in DF-telecom:
  - Phone book identifier = ICCid (10bytes) "fixed part" + 4 bytes (in EF_{PSC}) "variable part"
- For a phone book residing in an USIM application:
  - Phone book identifier = 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 must 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 = FFFF then
    {Increment PSC mod FFFFFFFF ; }
```

- Each time the terminal has to increment the value of CC the following test is needed:

```
If CC = FFFF then
    {Increment PSC mod FFFFFFFF ; 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 CC. The concept of having a CC makes it possible to update the phonebook 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		Optional
SFI: Mandatory			
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

- Change Counter of Phone Book
  Content:
  indicates recent change(s) to phone book entries for synchronisation purposes.
  Coding:
  hexadecimal. at initialisation, CC shall be personalised to 0000Hex (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 than be stored in the PUID.

Structure of EF$_{PUID}$

Identifier: '4F24'	Structure: transparent		Optional
SFI: Mandatory			
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 Change Counter (CC) of Phone Book	M	2 bytes

- Previously unique Identifier of Phone Book Entry
  Content:
  previous number that was used to unambiguously identify the phone book entry for synchronisation purposes.

4.5 Contents of files 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 to DF$_{TELECOM}$ to ensure backwards compatibility.

A 3G ME shall not access this file. The information is accessible for a 3G ME under 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 $\text{DF}_{\text{PHONEBOOK}}$ is mapped to $\text{DF}_{\text{TELECOM}}$ to ensure backwards compatibility.

4.5.3 EF_{CCP} (Capability Configuration Parameter)

In case of a present GSM application on the UICC the first EF_{CCP} (i.e. reflected by the first record in EF_{PBR}) of the $\text{DF}_{\text{PHONEBOOK}}$ is mapped to $\text{DF}_{\text{TELECOM}}$ to ensure backwards compatibility.

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 - X	Title Alpha Identifier	M	X bytes
1+X - 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'.

4.6 Contents of DFs at the TELECOM level

DFs may be present as child directories of $\text{DF}_{\text{TELECOM}}$. The following DFs have been defined:

- $\text{DF}_{\text{GRAPHICS}}$ '5F50'

- $\text{DF}_{\text{PHONEBOOK}}$ '5F3A'

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

4.6.1 Contents of files at the $\text{DF}_{\text{GRAPHICS}}$ level

The EFs in the Dedicated File $\text{DF}_{\text{GRAPHICS}}$ 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 $\text{DF}_{\text{GRAPHICS}}$, there may be several image instance data files. These EFs containing image instance data shall have the following attributes:

<table>
<tr><td colspan="2">Identifier: '4FXX'</td><td>Structure: transparent</td><td>Optional</td></tr>
<tr><td colspan="2">Record length: Y bytes</td><td colspan="2">Update activity: low</td></tr>
<tr><td colspan="4">Access Conditions:
READ PIN
UPDATE ADM
DEACTIVATE ADM
ACTIVATE ADM</td></tr>
<tr><td>Bytes</td><td>Description</td><td>M/O</td><td>Length</td></tr>
<tr><td>1 to Y</td><td>Image Instance Data</td><td>M</td><td>Y bytes</td></tr>
</table>

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', see subclause ??. The length Y may be different from one image instance data file to the other.

4.6.2 Contents of files at the $\text{DF}_{\text{PHONEBOOK}}$ under the $\text{DF}_{\text{TELECOM}}$

4.6.3 EF_{CCP} (Capability Configuration Parameters)

This EF contains parameters of required GSM network and GSM bearer capabilities and terminal configurations associated with a call established using an abbreviated dialling number, a fixed dialling number, an MSISDN, a last number dialled, a service dialling number or a barred dialling number. This EF can be referred to by EFs at the $\text{DF}_{\text{PHONEBOOK}}$ under $\text{DF}_{\text{TELECOM}}$.

Identifier: '4F3D'	Structure: linear fixed	Optional
SFI: optional		
Record length: 14 bytes	Update activity: low	
Access Conditions: READ PIN UPDATE PIN DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to 10	Bearer capability information element	M	10 bytes
11 to 14	Bytes reserved – see below	M	4 bytes

- Bearer capability information element
  Contents and Coding:
  see 3G TS 24.008 and GSM 24.008 [9]. The Information Element Identity (IEI) shall be excluded. i.e. the first byte of the EF$_{CCP}$ record shall be Length of the bearer capability contents.

- Bytes 11-14 shall be set to 'FF' and shall not be interpreted by the ME.

4.7 Files of USIM

This subclause contains a figure depicting the file structure of the UICC and the ADF$_{USIM}$. ADF$_{USIM}$ shall be selected using the AID and information in EF$_{DIR}$.

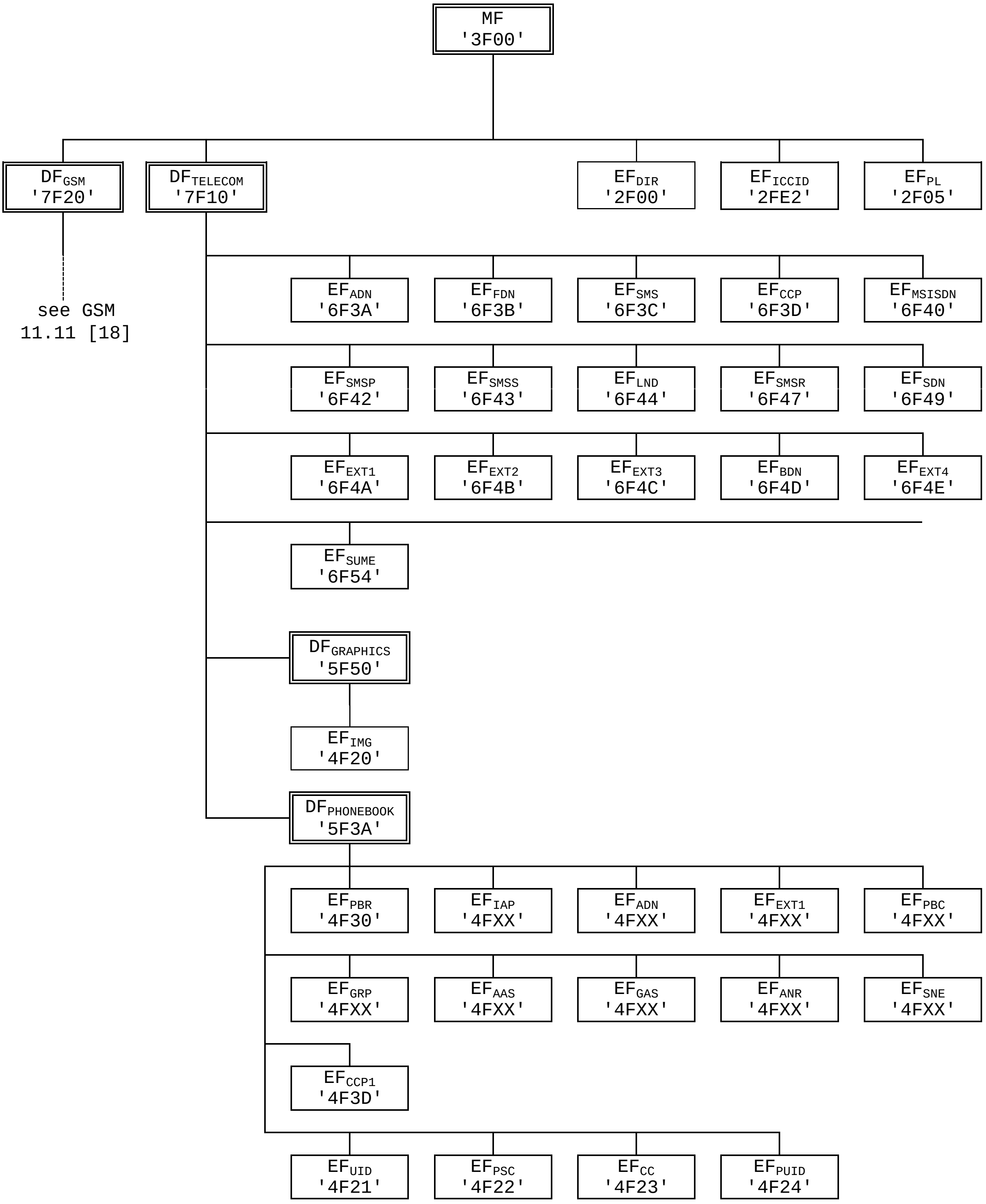


Figure 4.1: File identifiers and directory structures of UICC

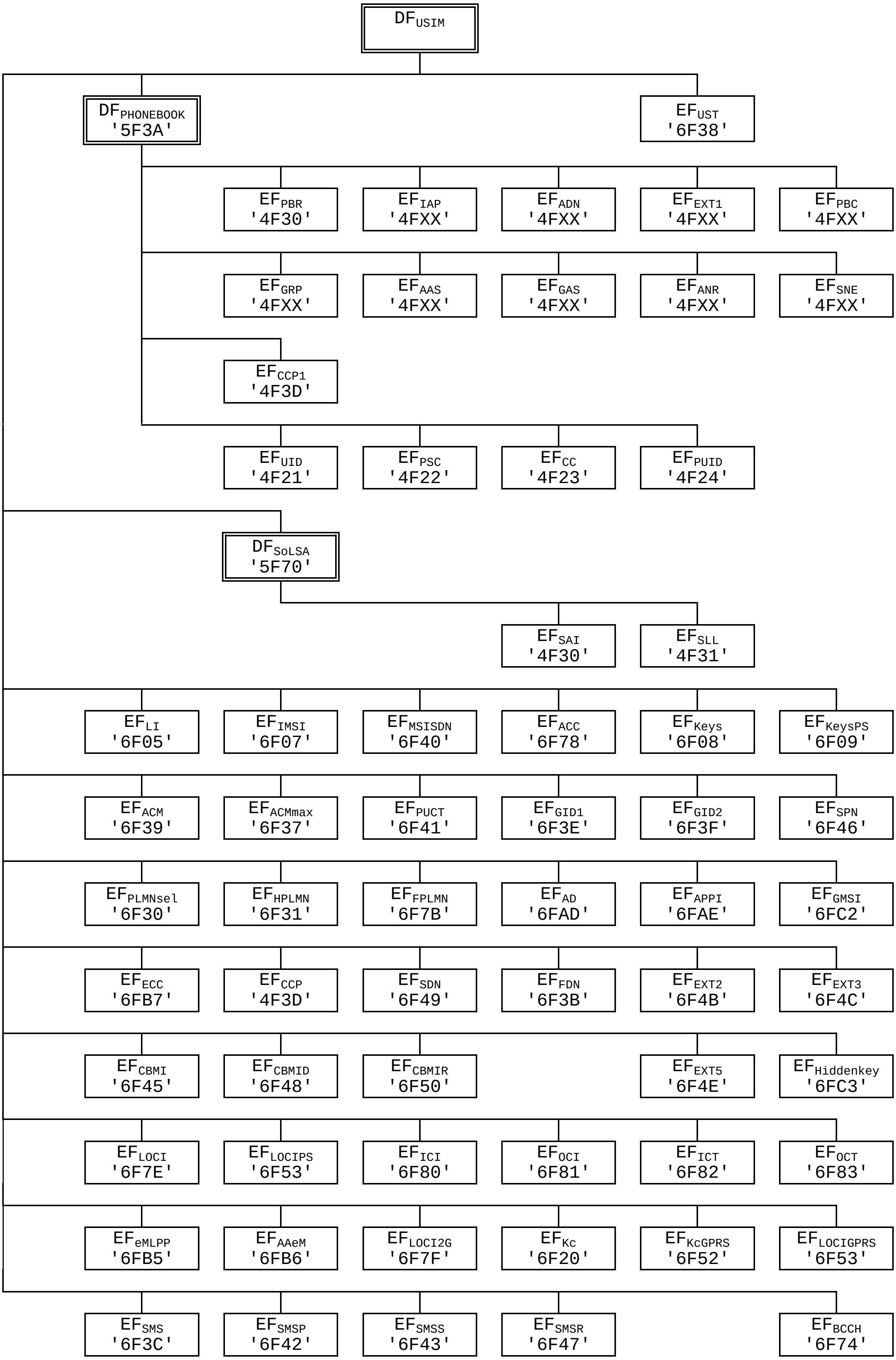


Figure 4.2: File identifiers and directory structures of USIM

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 USIM initialisation

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].

The ME optionally attempts to select EF_{ECC}. If EF_{ECC} is available, the ME requests the emergency call codes.

The ME requests the Language Indication. The ME keeps using the language selected during UICC activation by means of EF_{PL} (see 3G TS 31.101 [11]) if at least one of the following conditions holds:

- EF_{LI} is not available;
- EF_{LI} does not contain an entry corresponding to a language specified in ISO 639[19];
- the ME does not support any of the languages in EF_{LI}.

If none of the languages in the EFs is supported then the ME selects a default language.

The ME then runs the PIN verification procedure. If the PIN verification procedure is performed successfully, the ME then runs the application profile indication request procedure.

The ME performs the administrative information request.

The ME performs the USIM Service Table request.

For a USIM application requiring PROFILE DOWNLOAD, the ME shall perform the PROFILE DOWNLOAD procedure in accordance with 3G TS 31.111 [12].

If the FDN service is available the ME shall perform the following procedure. The procedure is tbd.

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:

- IMSI request;
- Access control information request;
- HPLMN search period request;
- PLMN selector request;
- Location Information request;
- Cipher key and integrity key request;
- Forbidden PLMN request;
- LSA information 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 indicates this to the USIM be sending a particular STATUS command.

5.1.2 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 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.

As soon as the USIM indicates that these procedures are completed, the ME sends a particular STATUS command indicating the termination of the 3G session.

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.

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 Application profile indication request

The ME performs the reading procedure with EF$_{APPI}$.

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 INTERNAL 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 '92 40' (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

Request: The ME performs the reading procedure with EF_{SAI}, EF_{SLL} and its associated LSA Descriptor files.
Update: The ME performs the updating procedure with EF_{SLL}.

5.2.9 User Identity Request

The ME selects a USIM and checks service no. 26 (Enhanced user identity confidentiality). If service no. 26 is not available then the ME performs the reading procedure with EF_{IMSI}.

Otherwise the ME uses the Encipher IMSI function (see 7.2.1). The response is received by the ME (in case of the T=0 protocol when requested by a subsequent GET RESPONSE command). Then the ME reads the group identity out of EF_{GMSI}. The ME concatenates the HE-id, the group identity GMSI and the enciphered IMSI and sends that to the network.

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}.

5.3 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 'D8' the ME reads the content of EF_{IAP} in order to establish the relation ship between the content in the files indicated using tag 'D9' and files indicated by tag 'D8'. 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 diplayed 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_{CCP} and EF_{EXT1} as described in the procedures below, but also to EF_{FDN}, EF_{MSISDN}, EF_{LND}, EF_{BDN} and EF_{SDN} 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°2 "allocated and activated"
(Service n°3 for FDN,
Service n°9 for MSISDN,
Service n°13 for LND,
Service n°18 for SDN),
Service n°31 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°10 "allocated and activated"
(Service n°10 applies also for MSISDN and LND;
Service n°11 for FDN;
Service n°19 for SDN;
Service n°32 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°10 "allocated and activated"
(Service n°10 applies also for MSISDN and LND;
Service n°11 for FDN;
Service n°19 for SDN;
Service n°32 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 recognie 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 (LND, MSISDN). 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 2: 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°3 (FDN).

FDN capability request. The ME has to check the state of service n°2, i.e. if FDN is "available". BDN capability request. The ME has to check the state of service n°7, i.e. if BDN is "available ".

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 PLMN selector

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

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}.

5.4 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.

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 describes 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 SEQ_{MS} and SEQ_{HE} respectively to support network authentication.

When the SN/VLR initiates an authentication and key agreement, it selects the next authentication vector from the array 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 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);
- f6: the user identity encryption function to encrypt the IMSI (optional).

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 C1 and C2. These functions derive the required GSM parameters (RAND_G, SRES, cipher key Kc) from available 3G parameters.

6.4 File access conditions

Every file has its own specific access condition for each command. The relevant access condition of the last selected file shall be fulfilled before the requested action can take place.

For each file:

- the access conditions for the commands READ and SEARCH RECORD are identical;
- the access conditions for the commands SELECT and STATUS are ALWays.

TBD: No file access conditions are currently assigned by 3G to the MF and the DFs.

The access condition levels are defined in the following table:

Table 6.1: Access condition level coding

Level	Access Condition
0	ALWays
1	PIN
2	PIN2
3	RFU
4 to 14	ADM
15	NEVer

The meaning of the file access conditions is as follows:

ALWAYS: The action can be performed without any restriction.

PIN (Personal Identification Number): The action shall only be possible if one of the following three conditions is fulfilled:
- a correct PIN value has already been presented to the USIM during the current session;
- TBD: the PIN enabled/disabled indicator is set to "disabled";

- UNBLOCK PIN has been successfully performed during the current session.

PIN2: The action shall only be possible if one of the following two conditions is fulfilled:
- a correct PIN2 value has already been presented to the USIM during the current session;
- UNBLOCK PIN2 has been successfully performed during the current session.

ADM: Allocation of these levels and the respective requirements for their fulfilment are the responsibility of the appropriate administrative authority.

The definition of access condition ADM does not preclude the administrative authority from using ALW, PIN, PIN2 and NEV if required.

NEVER: The action cannot be performed over the USIM(UICC)/ME interface. The USIM may perform the action internally.

Condition levels are not hierarchical. For instance, correct presentation of PIN2 does not allow actions to be performed which require presentation of PIN. A condition level which has been satisfied remains valid until the end of the USIM session as long as the corresponding secret code remains unblocked, i.e. after three consecutive wrong attempts, not necessarily in the same application session, the access rights previously granted by this secret code are lost immediately. A satisfied PIN condition level applies to both ADF_{USIM} and $DF_{TELECOM}$.

TBD if applicable: The ME shall determine whether PIN2 is available by using the response to the STATUS command. If PIN2 is "not initialised" then PIN2 commands, e.g. VERIFY PIN2, shall not be executable.

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

7.1.1.1 UMTS 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 in the correct range. This is described in annex C.If the USIM detects the sequence numbers to be not in the correct range, this is considered as a synchronisation failure and the USIM abandons the function. In this case the command response is AUTS, where:
$AUTS = Conc(SEQ_{MS}) \| MACS;$
$Conc(SEQ_{MS}) = SEQ_{MS} \oplus f5_K(MACS)$ is the concealed value of the counter SEQ_{MS} in the USIM; and.
$MACS = f1^*_K(SEQ_{MS} \| RAND \| AMF)$ 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 be used for support of multiple algorithms or keys, for changing the size of windows or lists, or for discriminating authentication vectors from separate CS/PS domains, see 3G TS 33.102 [13].

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, AUTN (AUTN := SQN ⊕ AK || AMF || MAC).

Output:
- RES, CK, IK, SRES, K_C
  or
  AUTS.

7.1.1.2 GSM security context

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	See below

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 UMTS 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 UMTS 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, UMTS security context, command successful:

Byte(s)	Description	Length
1	"Successful UMTS 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 SRES (= 4)	1
(L3+L4+L5+6) to (L3+L4+L5+10)	SRES	4
(L3+L4+L5+11)	Length of K_C (= 8)	1
(L3+L4+L5+12) to (L3+L4+L5+19)	K_C	8

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, UMTS 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 Encipher IMSI

7.2.1 Command description

The function is used during the procedure for identification of the user via the radio access path by means of the enciphered permanent user identity (IMSI).

For the execution of the command the USIM uses the group key GK and the sequence number $SEQ_{UIC/UE}$ which are stored internally in the USIM.

The USIM increments the internal sequence number $SEQ_{UIC/UE}$ that holds the value from the last execution of 'Encipher IMSI'.

Next the USIM computes the enciphered IMSI as $f6_{GK}$ ($SEQ_{UIC/UE}$ || IMSI) which is then returned in the command response.

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).

Input:
- none

Output:
- enciphered IMSI.

7.2.2 Command parameters and data

Code	Value
CLA	As defined in 3G TS 31.101
INS	'2A'
P1	'00'
P2	'00'
Lc	not present
Data	not present
Le	Length of EMSI (L1)

Parameter Le specifies the expected length of the response. This is depending on the further specification of function f6.

Command parameters/data:

none

Response parameters/data:

Byte(s)	Description	Length
1	Length of encrypted IMSI (L1)	1
2 to (L1+1)	Encrypted IMSI	L1

The most significant bit of the encrypted IMSI is coded on bit 8 of byte 2.

7.3 Status Conditions Returned by the UICC

Status of the card after processing of the command is coded in the status bytes SW1 and SW2. This subclause specifies coding of the status bytes in the following tables.

7.3.1 Security management

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

7.3.2 Status Words of the Commands

The following table shows for each command the possible status conditions returned (marked by an asterisk *). Status conditions of GSM and USIM applications are on the left and right sides of the table, respectively.

Commands and status words

AUTHENTICATE	ENCIPHER IMSI	
		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
*	*	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

Annex A (normative): Coding of USIM Specific Data

A.1 SELECT Response Information

Table A.1 and A.2 of this annex describe how the response information of the SELECT command is coded in case of MF, DF, ADF and EF selection, respectively.

Table A.1: SELECT Response Information in case of MF, ADF or DF

Byte(s)	Description	Length
1 to 2	Total amount of memory of the selected directory which is not allocated to any of the DFs or EFs under the selected directory	2
3 to 4	File ID	2
5	Type of file (see subclause C.2)	1
6 to 10	RFU	5
11	Length of the following data (byte 12 to the end)	1
12 to X	USIM specific data – see table A.2	21

Table A.2: USIM Specific Data

Byte(s)	Description	Length
12	File characteristics (see detail 1)	1
13	Number of DFs which are a direct child of the current directory	1
14	Number of EFs which are a direct child of the current directory	1
15	Number of PINs, UNBLOCK PINs and administrative codes	1
16	Application power consumption (see chapter C.2)	1
17	PIN status (see detail 2)	1
18	UNBLOCK PIN status (see detail 2)	1
19	PIN2 status (see detail 2)	1
20	UNBLOCK PIN2 status (see detail 2)	1
21	RFU	1
22 - 32	Reserved for the administrative management	0 ≤ lgth ≤ 11

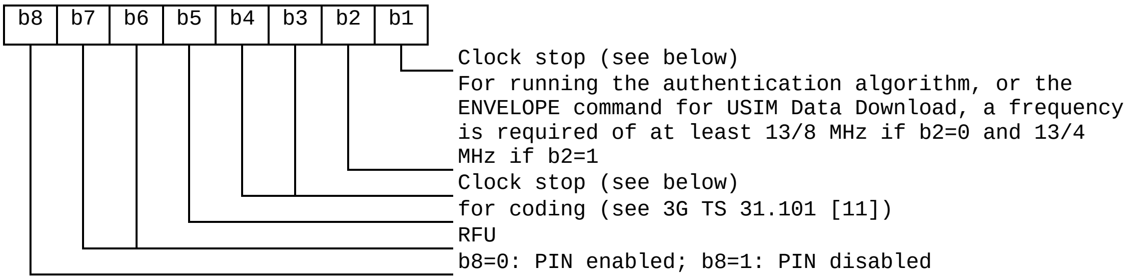
Bytes 1 to 20 are mandatory and shall be returned by a GSM application. Bytes 21 and following are optional and may not be returned by a GSM application.

NOTE 1: Byte 33 and following are RFU.

NOTE 2: The STATUS information of the MF, DF_{GSM} and $DF_{TELECOM}$ provide some identical application specific data, e.g. PIN status. On a multi-application card the MF should not contain any application specific data. Such data is obtained by MEs from the specific application directories. ME manufacturers should take this into account and therefore not use application specific data which may exist in the MF of a mono-application UICC.

Similarly, the VERIFY PIN command should not be executed in the MF but in the relevant application directory (e.g. DF_{GSM}).

Detail 1: File characteristics


b8
b7
b6
b5
b4
b3
b2
b1
Clock stop (see below)
For running the authentication algorithm, or the ENVELOPE command for USIM Data Download, a frequency is required of at least 13/8 MHz if b2=0 and 13/4 MHz if b2=1
Clock stop (see below)
for coding (see 3G TS 31.101 [11])
RFU
b8=0: PIN enabled; b8=1: PIN disabled

The coding of the conditions for stopping the clock is as follows:

Bit b1	Bit b3	Bit b4	
1	0	0	clock stop allowed, no preferred level
1	1	0	clock stop allowed, high level preferred
1	0	1	clock stop allowed, low level preferred
0	0	0	clock stop not allowed
0	1	0	clock stop not allowed, unless at high level
0	0	1	clock stop not allowed, unless at low level

If bit b1 (column 1) is coded 1, stopping the clock is allowed at high or low level. In this case columns 2 (bit b3) and 3 (bit b4) give information about the preferred level (high or low, respectively) at which the clock may be stopped.

If bit b1 is coded 0, the clock may be stopped only if the mandatory condition in column 2 (b3=1, i.e. stop at high level) or column 3 (b4=1, i.e. stop at low level) is fulfilled. If all 3 bits are coded 0, then the clock shall not be stopped.

Detail 2: Status byte of a secret code

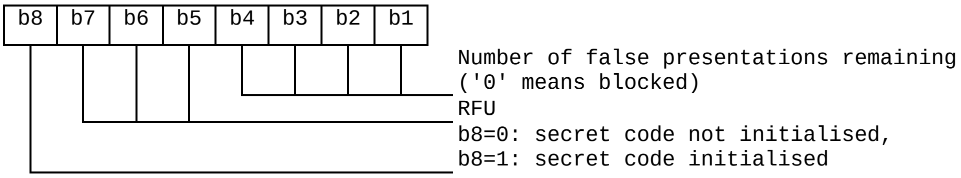

b8
b7
b6
b5
b4
b3
b2
b1
Number of false presentations remaining ('0' means blocked)
RFU
b8=0: secret code not initialised,
b8=1: secret code initialised

Table A.3: SELECT Response Information in case of an EF

Byte(s)	Description	Length
1 to 2	File size (for transparent EF: the length of the body part of the EF) (for linear fixed or cyclic EF: record length multiplied by the number of records of the EF)	2
3 - 4	File ID	2
5	Type of file (see C.2)	1
6	See detail 3	1
7 to 9	Access conditions (see C.2)	3
10	File status (see C.2)	1
11	Length of the following data (byte 14 to the end)	1
12	Structure of EF (see C.2)	1
13	Length of a record (see detail 4)	1
14 and following	RFU	-

Bytes 1-12 are mandatory and shall be returned by a USIM application.
Byte 13 is mandatory in case of linear fixed or cyclic EFs and shall be returned by a USIM application.
Byte 13 is optional in case of transparent EFs and may not be returned by a USIM application.
Byte 14 and following (when defined) are optional and may not be returned by a USIM application.

Detail 3: Byte 6

For transparent and linear fixed EFs this byte is RFU. For a cyclic EF all bits except bit 7 are RFU; b7=1 indicates that the INCREASE command is allowed on the selected cyclic file.

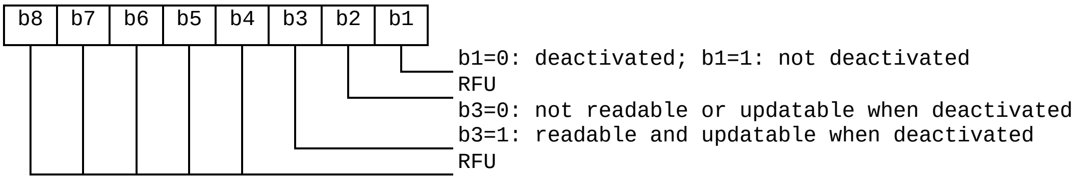
Detail 4: Byte 13

For cyclic and linear fixed EFs this byte denotes the length of a record. For a transparent EF, this byte shall be coded '00', if this byte is sent by a USIM application. If the file is of type variable then the information returned is the number of records.

A.2 Coding of telecom specific EF response data

The following response coding applies for telecom applications and are used in the response to SELECT command when an EF has been selected.

File status:


b8
b7
b6
b5
b4
b3
b2
b1
b1=0: deactivated; b1=1: not deactivated
RFU
b3=0: not readable or updatable when deactivated
b3=1: readable and updatable when deactivated
RFU

Bit b3 may be set to 1 in special circumstances when it is required that the EF can be read and updated even if the EF is deactivated, e.g. reading and updating the EF_{ADN} when the FDN feature is enabled, or reading and updating the EF_{BDN} when the BDN feature is deactivated.

Structure of file:

- '00' transparent;
- '01' linear fixed;
- '02'linear variable;
- '03' cyclic.

Type of File:

- '00' RFU;
- '01' MF;
- '02' DF;
- '04' EF.

Coding of PINs and UNBLOCK PINs

A PIN is 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.

Coding of Access Conditions:

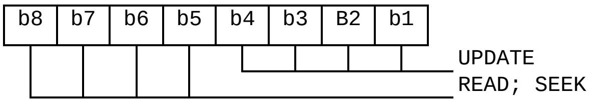
The access conditions for the commands are coded on bytes 9, 10 and 11 of the response data of the SELECT command. Each condition is coded on 4 bits as shown in table A.4.

Table A.4: Access conditions

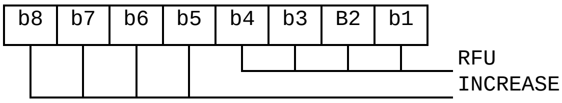
ALW	'0' *
PIN	'1' *
Second PIN	'2' *
RFU	'3'
ADM	'4'
.....	..
ADM	'E'
NEV	'F' *

Entries marked "*" in the table above, are also available for use as administrative codes in addition to the ADM access levels '4' to 'E' (refer to subclause 7.3 ?) if required by the appropriate administrative authority. If any of these access conditions are used, the code returned in the Access Condition bytes in the response data shall be the code applicable to that particular level.

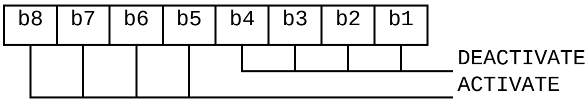
Byte 9:



Byte 10:



Byte 11:



A.3 Application Related Electrical Parameters

The power consumption of a UICC is depending upon the supply voltage class and the application it is running. The power consumption of the UICC is restricted to the values specified in 3G TS 31.101 [11] until an application is selected. An application is considered to be selected when the access condition is successfully verified. If no access condition is required for the application, the application is considered to be selected when an application related command is executed within the selected application. Selecting the application and performing a STATUS command is not an execution of an application command.

The ME retrieves the application power consumption information by selecting the application and performing a STATUS command. The power consumption parameters are returned by the card in the response to the STATUS command at a DF level in the application. In case of a multiapplication UICC, where the application selection according to ISO/IEC 7816-5 [21] is used, the application power consumption is to be indicated in the information elements of the application identifier stored in EF_{DIR} as defined in ISO/IEC 7816-4 [20].

If no power consumption indication is available in the card, the ME shall assume the application power consumption as specified in 3G TS 31.101 [11].

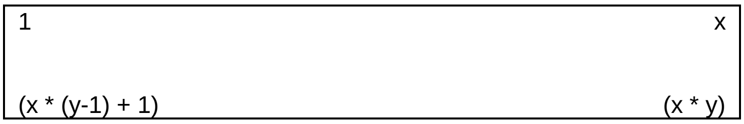
Table A.5: Power Consumption during the Application Session

Symbol	Voltage Class	Maximum	Unit	Remark
Icc	A	60	mA	
Icc	A	10	mA	GSM Application
Icc	B	50	mA	
Icc	B	6	mA	GSM Application
Icc	C	20	mA	
Icc	C	4	mA	GSM Application
Icc	D	RFU	mA	
Icc	E	RFU	mA	

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

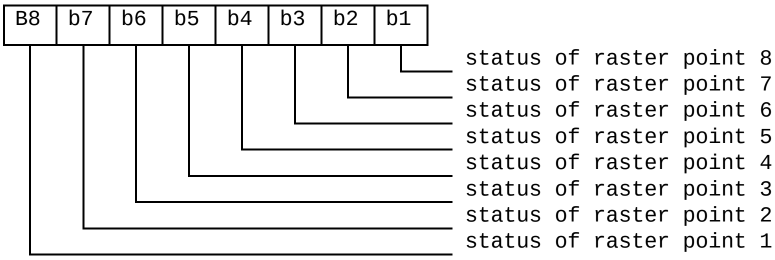
This coding scheme applies to rectangular raster images made up of raster points that are either set or not set. This coding scheme does not support any notion of colour. Image data are coded as follows:

Byte(s)	Description	Length
1	image width = X	1
2	image height = Y	1
3 to K+2	image body	K

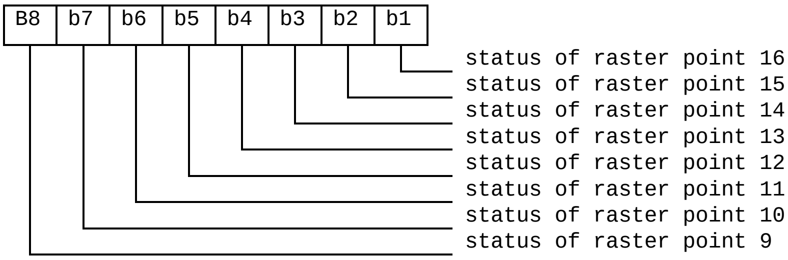
Coding of image body:

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:


B8
b7
b6
b5
b4
b3
b2
b1
status of raster point 16
status of raster point 15
status of raster point 14
status of raster point 13
status of raster point 12
status of raster point 11
status of raster point 10
status of raster point 9

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

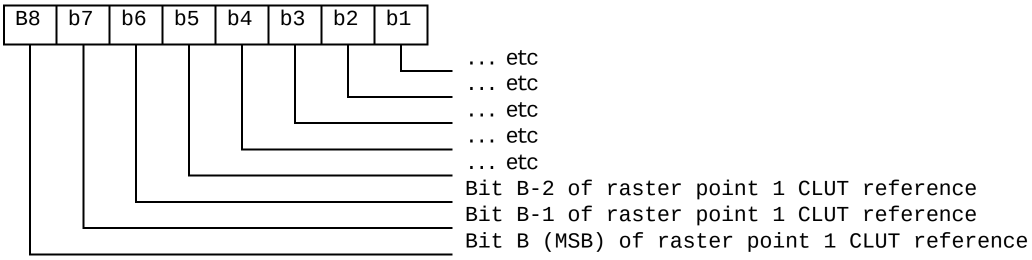
- Bits per raster image point:
    Contents:
        the number B of bits used to encode references into the CLUT, thus defining a raster image point's colour. B shall have a value between 1 and 8.
    Coding:
        binary.

- 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:


B8
b7
b6
b5
b4
b3
b2
b1
... etc
... etc
... etc
... etc
... etc
Bit B-2 of raster point 1 CLUT reference
Bit B-1 of raster point 1 CLUT reference
Bit B (MSB) of raster point 1 CLUT reference

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 (normative): Management of Sequence Numbers

For efficiency reasons, it is taken into account that authentication vectors may be generated in batches (such that all authentication vectors in one batch are sent to the same SN/VLR).

In its binary representation, the sequence number consists of two concatenated parts $SQN = SEQ \| IND$. *SEQ* is the batch number, and *IND* is an index numbering the authentication vectors within one batch. *IND* represents the least significant bits of *SQN*. If the concept of batches is not supported then the parameter *IND* is not used and $SQN = SEQ$.

The USIM keeps track internally of an ordered list of the *b* highest batch number values it has accepted. In addition, for each batch number *SEQ* in the list, the USIM stores internally the highest *IND* value *IND(SEQ)* it has accepted associated with that batch number. Let SEQ_{LO} denote the lowest and SEQ_{MS} denote the highest batch number in the list.

C.1 Acceptance rule

When a user authentication request arrives, the USIM checks whether the sequence number is acceptable. The sequence number $SQN = SEQ \| IND$ is accepted by the USIM if and only if a) and either b) or c) hold:

a) $SEQ - SEQ_{MS} < \Delta$;

b) *SEQ* is in the list and $IND > IND(SEQ)$;

c) *SEQ* is not in the list and $SEQ > SEQ_{LO}$.

NOTE: The purpose of condition (i) is to protect against wrap around of the counter in the USIM.

The USIM shall also be able to put a limit *L* on the difference between SEQ_{MS} and an accepted batch number *SEQ*. If such a limit is applied then, in addition to the above conditions, the sequence number shall only be accepted by the USIM if $SEQ_{MS} - SEQ < L$.

NOTE: This allows for a memory-efficient storage of batch numbers: With the exception of SEQ_{MS} , the batch numbers in the list need not be stored in full length, if those entries in the list which would cause the limit *L* to be exceeded are removed from the list after a new sequence number has been accepted.

C.2 List update

After a sequence number $SQN = SEQ \| IND$ received in a user authentication request has been accepted by the USIM, the USIM proceeds as follows:

a) Case 1: the batch number *SEQ* is not in the list.

Then the list entry corresponding to SEQ_{LO} is deleted, *SEQ* is included in the list, *IND(SEQ)* is set to *IND* and SEQ_{LO} and SEQ_{MS} are updated;

b) Case 2: the batch number *SEQ* is in the list.

Then *IND(SEQ)* is set to *IND*. If a sequence number received in a user authentication request is rejected the list remains unaltered.

A USIM shall support a list size of at least xx entries (*FFS*).

Annex D (informative): Tags defined in 31.102

Tag	Name of Data Element	Usage
'D8'	Indicator for type 1 EFs (amount of records equal to master EF)	Phone Book Reference File (EF_{PBR})
'D9'	Indicator for type 2 EFs (EFs linked via the index administration file)	Phone Book Reference File (EF_{PBR})
'DA'	Indicator for type 3 EFs (EFs addressed inside a TLV object) The following are encapsulated under 'XZ': 'C0' EF_{ADN} data object 'C1' EF_{IAP} data object 'C2' EF_{ECT1} 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	Phone Book Reference File (EF_{PBR})
'DC'	Synchronisation failure	Response to AUTHENTICATE
'DB'	Successful UMTS authentication	Response to AUTHENTICATE

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
'2F E2'	ICC identification	operator dependant
'6F 05'	Language indication	'FF'
'6F 07'	IMSI	operator dependant
'6F 20'	Ciphering key Kc	'FF...FF07'
'6F 30'	PLMN selector	'FF...FF'
'6F 31'	HPLMN search period	'FF'
'6F 37'	ACM maximum value	'000000' (see note 1)
'6F 38'	USIM service table	operator dependant
'6F 39'	Accumulated call meter	'000000'
'6F 3E'	Group identifier level 1	operator dependant
'6F 3F'	Group identifier level 2	operator dependant
'6F 41'	PUCT	'FFFFFF0000'
'6F 45'	CBMI	'FF...FF'
'6F 46'	Service provider name	'FF...FF'
'6F 48'	CBMID	'FF...FF'
'6F 49'	Service Dialling Numbers	'FF...FF'
'6F 74'	BCCH	'FF...FF'
'6F 78'	Access control class	operator dependant
'6F 7B'	Forbidden PLMNs	'FF...FF'
'6F 7E	Location information	'FFFFFFFF xxFxxx 0000 FF 01' (see note 2)
'6F AD'	Administrative data	operator dependant
'6F AE'	Application profile identification	see 10.3.16
'4F XX'	Abbreviated dialling numbers	'FF...FF'
'6F 3B'	Fixed dialling numbers	'FF...FF'
'6F 3C'	Short messages	'00FF...FF'
'6F 3D'	Capability configuration parameters	'FF...FF'
'6F 40'	MSISDN storage	'FF...FF'
'6F 42'	SMS parameters	'FF...FF'
'6F 43'	SMS status	'FF...FF'
'6F 47'	Short message status reports	'00FF…FF'
'4F XX'	Extension 1	'FF...FF'
'6F 4B'	Extension 2	'FF...FF'
'6F 4C'	Extension 3	'FF...FF'
'6F 52'	GPRS Ciphering key KcGPRS	'FF...FF07'
'6F 53'	GPRS Location Information	'FFFFFFFF FFFFFF xxFxxx 0000 FF 01'
‘6F 54’	SetUpMenu Elements	operator dependent
'4F 20'	Image data	'00FF...FF'
'4F 30'	SoLSA Access Indicator)	'00FF...FF'
'4F 31'	SoLSA LSA List	'FF...FF'

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

NOTE 2: xxFxxx 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

The length of all the records is determined by the LSA descriptor containing the largest number of bytes. Combinations containing different numbers of LSA IDs, LAC+ CI and CI or LAC can therefore be done. Various examples are show. Due to the OTA management of the records it is recommended that the record length is maximum 100 bytes in order to leave room for command descriptor and signature information in the SMS.

This first example contains two LSAs, one described by two LSA IDs and another described by three Cell IDs, giving a record length of 8 bytes.

1st record:	LSA descriptor type = LSA ID and number = 2 (1 byte)	LSA ID (3 bytes)	LSA ID (3 bytes)	Identifier (1 byte)

2nd record:	LSA descriptor type = CI and number = 3 (1 byte)	CI (2 bytes)	CI (2 bytes)	CI (2 bytes)	Identifier (1 byte)

The second example contains two LSAs, one described by one LSA ID and one described by two Cell Ids, giving a record length of 6 bytes.

1st record:	LSA descriptor type = LSA ID and number = 1 (1 byte)	LSA ID (3 bytes)	'FF'	Identifier (1 byte)

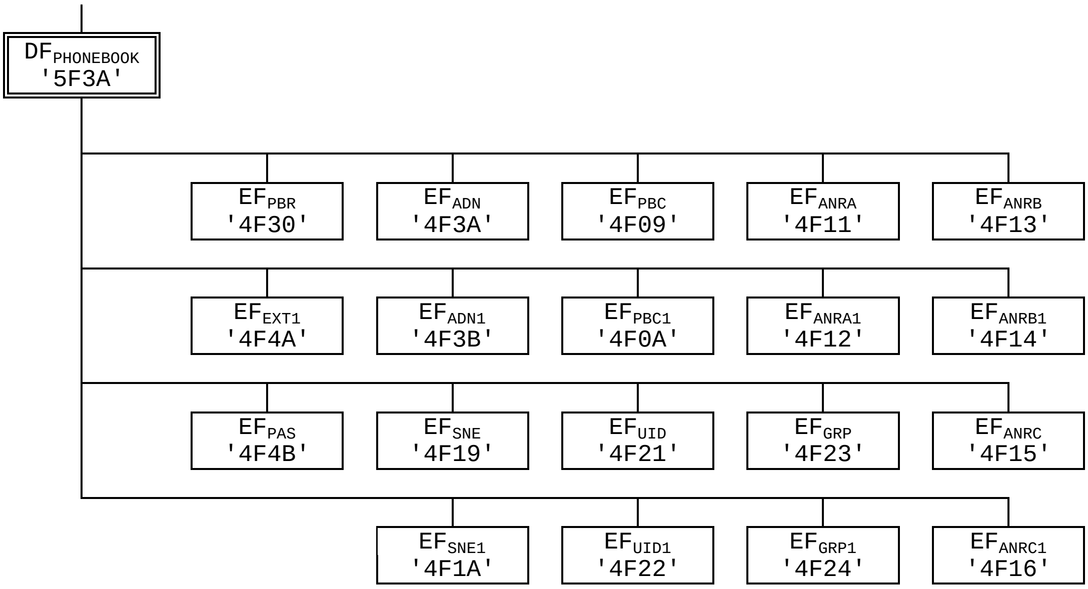
2nd record:	LSA descriptor type = CI and number = 2 (1 byte)	CI (2 bytes)	CI (2 bytes)	Identifier (1 byte)

Annex G (informative): Phonebook Example

The phonebook has more than 254 entries. Additional number (3 additional numbers) information and second name 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 two files that are shared EF$_{\text{EXT1}}$ and EF$_{\text{PAS}}$. These files are addressed from inside a file. EF$_{\text{EXT1}}$ is addressed via EF$_{\text{ADN,}}$ EF$_{\text{ADN1}}$ and EF$_{\text{PAS}}$ is addressed via EF$_{\text{PBC,}}$ EF$_{\text{PBC1}}$. The phonebook supports two levels of grouping and hidden entries in EF$_{\text{PBC.}}$

Two records are needed in the reference file PBR '4F30' for supporting more than 254 entries. The reference file PBR '4F30' record structure is as shown in table 1x. The structure of the DF$_{\text{PHONEBOOK}}$ for Case 1 is shown in table 1y.

Table G.1: Structure of EFs inside DF$_{\text{PHONEBOOK}}$



The content of a phonebook entry in the range from 1-508 is described in table 1d and 1e.

Table G.2: Contents of EF$_{\text{PBR}}$

Rec 1	Tag'XX'	L='12'	Tag'X0'	L='02'	'4F3A'	Tag'X6'	L='02'	'4F09'	Tag'X4'	L='02'	'4F11'	Tag'X4'	L='02'	'4F13'
	Tag'X4'	L='02'	'4F15'	Tag'X3'	L='02'	'4F19'	Tag'X9'	L='02'	'4F21'	Tag'XZ'	L='08'	Tag'X1'	L='02'	'4F4A'
	Tag'X8'	L='02'	'4F4B'	'FF'										
Rec 2	Tag'XX'	L='12'	Tag'X0'	L='02'	'4F3B'	Tag'X6'	L='02'	'4F0A'	Tag'X4'	L='02'	'4F12'	Tag'X4'	L='02'	'4F14'
	Tag'X4'	L='02'	'4F16'	Tag'X3'	L='02'	'4F1A'	Tag'X9'	L='02'	'4F22'	Tag'XZ'	L='08'	Tag'X1'	L='02'	'4F4A'
	Tag'X8'	L='02'	'4F4B'	'FF'										

Table G.3: Structure of the 254 first entries in the phonebook

ADN '4F3A'			PBC '4F09'	GRP '4F23'	ANR '4F11'	ANR '4F13'	ANR '4F15'	SNE '4F19'	UID '4F21'	EXT1 '4F4A'	PAS '4F4B'
Rec 1	ADN Cont (1-(X+13))	EXT1 Rec '02'	Hidden AID rec N° 3	Rec n°1 Rec n°3 '00'	ANR1 Rec n°1	ANR2 Rec n°2	ANR3 Rec n°3	Second Name Alpha String	UID	Rec '02'	Record numbers as defined in PBC/ANR
Rec 2	ADN Cont (1-(X+13))	EXT1 Rec '2A'	Not Hidden	Rec n°2 Rec n°1 Rec n°3	ANR1 Rec n°1	ANR2 Rec n°2	ANR3 Rec n°3	Second Name Alpha String	UID	Rec '2A*	Record numbers as defined in PBC/ANR
Rec 3											
:											
:											
:											
Rec 254											

Table G.4: Structure of phone book entries 255-508 (Rec 1-254)

ADN '4F3B'			PBC '4F0A'	GRP '4F24'	ANR '4F12'	ANR '4F14'	ANR '4F16'	SNE '4F1A'	UID '4F22'	EXT1 '4F4A'	PAS '4F4B'
Rec 1	ADN Cont (1-(X+13))	EXT1 Rec '02'	Hidden AID Rec n° 3	Rec n°1 Rec n°3 '00'	ANR1 Rec n°2	ANR2 Rec n°2	ANR3 Rec n°3	Second Name Alpha String	UID	Rec '02'	Record numbers as defined in PBC/ANR
Rec 2	ADN Cont (1-(X+13))	EXT1 Rec '2A'	Not Hidden	Rec n°2 Rec n°1 Rec n°3	ANR1 Rec n°2	ANR2 Rec n°2	ANR3 Rec n°3	Second Name Alpha String	UID	Rec '2A*	Record numbers as defined in PBC/ANR
Rec 3											
:											
:											
:											
Rec 254											

Annex H (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
'2F 05'	Extended Language preference	Yes
'2F E2'	ICC identification	No
'4F 20'	Image data	Yes
'4F xx'	Image Instance data Files	Yes
'6F 05'	Language preference	Yes
'6F 07'	IMSI	Caution (Note 1)
'6F 20'	Ciphering key Kc	No
'6F 2C'	De-personalization Control Keys	Caution
'6F 30'	PLMN selector	Caution
'6F 31'	HPLMN search period	Caution
'6F 32'	Co-operative network	Caution
'6F 37'	ACM maximum value	Yes
'6F 38'	SIM service table	Caution
'6F 39'	Accumulated call meter	Yes
'6F 3A'	Abbreviated dialling numbers	Yes
'6F 3B'	Fixed dialling numbers	Yes
'6F 3C'	Short messages	Yes
'6F 3D'	Capability configuration parameters	Yes
'6F 3E'	Group identifier level 1	Yes
'6F 3F'	Group identifier level 2	Yes
'6F 40'	MSISDN storage	Yes
'6F 41'	PUCT	Yes
'6F 42'	SMS parameters	Yes
'6F 43'	SMS status	Yes
'6F 44'	Last number dialled	Yes
'6F 45'	CBMI	Caution
'6F 46'	Service provider name	Yes
'6F 47'	Short message status reports	Yes
'6F 48'	CBMID	Yes
'6F 49'	Service Dialling Numbers	Yes
'6F 4A'	Extension 1	Yes
'6F 4B'	Extension 2	Yes
'6F 4C'	Extension 3	Yes
'6F 4D'	Barred dialling numbers	Yes
'6F 4E'	Extension 4	Yes
'6F 50'	CBMIR	Yes
'6F 51'	Network's indication of alerting	Caution
'6F 52'	GPRS Ciphering key KcGPRS	No
'6F 53'	GPRS Location Information	Caution
'6F 54'	SetUpMenu Elements	Yes
'6F 74'	BCCH	No
'6F 78'	Access control class	Caution
'6F 7B'	Forbidden PLMNs	Caution
'6F 7E'	Location information	No (Note 1)
'6F AD'	Administrative data	Caution
'6F AE'	Phase identification	Caution
'6F B1'	Voice Group Call Service	Yes
'6F B2'	Voice Group Call Service Status	Yes
'6F B3'	Voice Broadcast Service	Yes
'6F B4'	Voice Broadcast Service Status	Yes
'6F B5'	Enhanced Multi Level Pre-emption and Priority	Yes
'6F B6'	Automatic Answer for eMLPP Service	Yes
'6F B7'	Emergency Call Codes	Caution
NOTE1: If EF_{IMSI} is changed, the UICC should issue REFRESH as defined in TS 31.111 and update EF_{LOCI} accordingly.		

History

Document history		
V3.0.0	January 2000	Publication